

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

**№ 2(29)/2019**

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 11.07.16 р. № 820 (додаток 12),  
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.

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 RIGHT**

**SCIENTIFIC PROFESSIONAL JOURNAL**

**№ 2(29)/2019**

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 11.07.16 № 820 (Annex 12), the journal can publish materials related to thesis works aimed on the receipt of scientific degrees of candidate of sciences (Doctor of Philosophy-Ph.D.) and Doctor of Sciences in the area of Juridical Science.

The printed journal INFORMATION AND LAW is included in the international database of journal, in accordance with relevant ISSN number.

Kyiv

УДК 002:340+316.4+338.46

**Р е д а к ц і й н а   к о л е г і я**

**ПИЛИПЧУК Володимир Григорович**, доктор юридичних наук, професор, член-кореспондент  
НАПрН України – *голова редакційної колегії,*  
*головний редактор;*

**БРИЖКО Валерій Михайлович**, доктор філософії (Ph.D.) з юридичних наук, с.н.с.  
– *зас. голови редакційної колегії,*  
*зас. головного редактора;*

**ПОПИК Володимир Іванович**, доктор історичних наук, професор,  
член-кореспондент НАН України – *зас. голови редакційної колегії;*

**БЕБИК Валерій Михайлович**, доктор політичних наук, професор – *зас. голови редакційної колегії;*

**АРІСТОВА Ірина Василівна**, доктор юридичних наук, професор;

**БАРАНОВ Олександр Андрійович**, доктор юридичних наук, с.н.с.;

**БЄЛЯКОВ Костянтин Іванович**, доктор юридичних наук, професор;

**ДЗЬОБАНЬ Олександр Петрович**, доктор філософських наук, професор;

**ДОВГАНЬ Олександр Дмитрович**, доктор юридичних наук, с.н.с.;

**КОПАН Олексій Володимирович**, доктор юридичних наук, професор;

**КОРЖ Ігор Федорович**, доктор юридичних наук, с.н.с.;

**КУЙБИДА Василь Степанович**, доктор наук з державного управління, професор;

**ЛАНДЕ Дмитро Володимирович**, доктор технічних наук, професор;

**МАРУЩАК Анатолій Іванович**, доктор юридичних наук, професор;

**НАСТЮК Василь Якович**, доктор юридичних наук, професор,  
член-кореспондент НАПрН України;

**НОР Василь Тимофійович**, доктор юридичних наук, професор,  
академік НАПрН України;

**ОНИЩЕНКО Олексій Семенович**, доктор філософських наук, професор,  
академік НАН України;

**ПЕТРИШИН Олександр Віталійович**, доктор юридичних наук, професор,  
академік НАПрН України;

**ПОКУТНИЙ Сергій Іванович**, доктор фізико-математичних наук, професор;

**САВІНОВА Наталія Андріївна**, доктор юридичних наук, с.н.с.;

**СКУЛИШ Євген Деонізієвич**, доктор юридичних наук, професор;

**ТАЛАНЧУК Петро Михайлович**, доктор технічних наук, професор;

**ТИХИЙ Володимир Павлович**, доктор юридичних наук, професор,  
академік НАПрН України;

**ФУРАШЕВ Володимир Миколайович**, кандидат технічних наук, доцент, с.н.с.;

**ШЕМШУЧЕНКО Юрій Сергійович**, доктор юридичних наук, професор,  
академік НАН України.

\* \* \* \* \*

UDC 002:340+316.4+338.46

**E d i t o r i a l   B o a r d**

**PYLYPCHUK Volodymyr**, Doctor of Juridical Science, Professor,  
Corresponding Member NALS of Ukraine – *Chairman of Editorial Board,*  
– *Editor in Chief;*

**BRYZHKO Valerii**, Doctor of Philosophy (Ph.D.) of Juridical Science, Senior researcher fellow  
– *Vice-chairman of Editorial Board,*  
– *Vice-editor;*

**POPYK Volodymyr**, Doctor of Historical Sciences, Corresponding Member NAN of Ukraine  
– *Vice-chairman of Editorial Board.*

**BEBYK Valerii**, Doctor of Political Sciences, Professor – *Vice-chairman of Editorial Board;*

**ARISTOVA Iryna**, Doctor of Juridical Science, Professor;

**BARANOV Oleksandr**, Doctor of Juridical Science, Senior researcher fellow;

**BIELIAKOV Konstantyn**, Doctor of Juridical Science, Professor;

**DZ'OBAN Oleksandr**, Doctor of Philosophical Science, Professor;

**DOVGAN Oleksandr**, Doctor of Juridical Science, Senior researcher fellow;

**KOPAN Oleksii**, Doctor of Juridical Science, Professor;

**KORZH Ihor**, Doctor of Juridical Science, Senior researcher fellow;

**KUIBIDA Vasyl**, Doctor of Administration Science, Professor;

**LANDE Dmytro**, Doctor of Engineering Sciences, Professor;

**MARUSHCHAK Anatolii**, Doctor of Juridical Science, Professor;

**NASTIUK Vasyl**, Doctor of Juridical Science, Professor,  
Corresponding Member NALS of Ukraine;

**NOR Vasyl**, Doctor of Juridical Science, Professor,  
Academician NALS of Ukraine;

**ONISHCHENKO Oleksii**, Doctor of Philosophical Science, Professor;  
Academician NALS of Ukraine;

**PETRYSHIN Oleksandr**, Doctor of Juridical Science, Professor,  
Academician NALS of Ukraine;

**POKUTNYI Serhii**, Doctor of Physics and Mathematics Sciences, Professor;

**SAVINOVA Nataliia**, Doctor of Juridical Science, Senior researcher fellow;

**SKULYSH Ievhen**, Doctor of Juridical Science, Professor;

**TALANCHUK Petro**, Doctor of Engineering Sciences, Professor;

**TYKHYI Volodymyr**, Doctor of Juridical Science, Professor,  
Academician NALS of Ukraine;

**FURASHEV Volodymyr**, Candidate of Engineering Sciences, Associate Professor,  
Senior researcher fellow;

**SHEMSHUCHENKO Yurii**, Doctor of Juridical Science, Professor,  
Academician NAN of Ukraine.

\* \* \* \* \*

## З М І С Т

**Інформаційне право**

<b>КОРЖ І.Ф.</b> Національна інтегрована система нормативно-правових актів: реальність і можливості.....	<b>9</b>
<b>ДОВГАНЬ О.Д., ЯЩЕНКО В.А.</b> Сутність і зміст законодавства у секторі оборони та його реалізації: інформаційно-правове дослідження.....	<b>17</b>

**Правова інформатика**

<b>ЛАНДЕ Д.В., ЛІНЕНКО Ю.О.</b> Мережева модель правових обмежень доступу до Інтернету у світі.....	<b>26</b>
<b>БРАЙЧЕВСКИЙ С.М.</b> Зворотні зв'язки в системах Інтернету речей з елементами штучного інтелекту.....	<b>32</b>
<b>РАДУТНИЙ О.Е.</b> Юридична освіта та сфера надання правових послуг в контексті штучного інтелекту.....	<b>40</b>
<b>ДОРОГИХ С.О.</b> Електронний парламент як базис побудови національної системи нормативно-правових актів.....	<b>55</b>

**Інформаційна і національна безпека**

<b>ДЗЬОБАНЬ О.П., ЖДАНЕНКО С.Б.</b> Від “інформаційного суспільства до “інформаційної безпеки”: до проблеми концептуалізації сутності понять.....	<b>60</b>
<b>ДОРОНІН І.М.</b> Правові проблеми суверенізації Інтернету.....	<b>74</b>
<b>ГРЕБЕНЮК М.В., ЛЕОНОВ Б.Д.</b> Проблеми протидії поширенню деструктивної пропаганди та дезінформації напередодні виборів: аналіз досвіду ЄС.....	<b>82</b>
<b>ГУЦАЛЮК М.В.</b> Оцінка реалізації стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик.....	<b>90</b>
<b>ПЕТРОВ С.Г.</b> Повноваження СБ України як суб'єкта національної системи кібербезпеки.....	<b>100</b>
<b>КРАВЧЕНКО Р.М.</b> Щодо деяких підходів до вдосконалення контррозвідального пошуку органів військової контррозвідки СБ України з урахуванням аналізу законодавства США.....	<b>106</b>
<b>КУЛЕШОВ М.В.</b> Сутність та зміст розслідування кіберінцидентів та кібератак підрозділами СБ України.....	<b>115</b>
<b>САНДУЛ В.С.</b> Удосконалення законодавства та навчальної програми викладання предмета “Захист Вітчизни” в середніх загальноосвітніх закладах.....	<b>123</b>

## Інформація за іншими предметними напрямками досліджень за спеціалізаціями в галузі знань 08 – “Право”

<b>БЕЛАНЮК М.В., ВРОНСЬКА Т.В.</b> Перші кроки відновлення роботи органів юстиції на визволеній від нацистів території України (1943 – 1944 рр.).....	<b>129</b>
<b>НИЖНИК А.І.</b> Недоторканність народного депутата України – конституційно-правова гарантія незалежного парламентського контролю: інформаційно-правовий аспект.....	<b>141</b>
<b>УХАНОВА Н.С.</b> Правова культура молоді в Україні.....	<b>156</b>
<b>БЄЛЄВЦЕВА В.В.</b> Міграційний режим перебування іноземних громадян і осіб без громадянства на території України: стан і перспективи.....	<b>167</b>
<b>ДЕНИСОВ А.І.</b> Перспективи створення спеціальних правових режимів для трудових мігрантів.....	<b>172</b>
<b>КОСИЦЯ О.</b> Публічний контроль за забезпеченням прав викривачів.....	<b>179</b>
<b>ЛИМАРЬ І.В.</b> Дискусійні питання місця виконавчого провадження в системі права України.....	<b>186</b>
<b>До відома авторів.....</b>	<b>194</b>

Наукове редагування, створення оригінал-макета та дизайн – Брижко В.М.

Граматичне коректування – Майстренко І.А. (укр., англ.).

Формат 70 x 108/16. Спосіб друку – різнографія. Ум. друк. арк. 17.75. Тираж 100 прим.

Виготовлено з оригінал-макета в друкарні ТОВ “Видавничий дім “АртЕк”.

04050, м. Київ, вул. Мельникова, буд. 63.

Свідectво 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 НДПП НАПрН України, протокол № 4 від 12.06.19 р.

## TABLE OF CONTENTS

### Informative Law

<b>KORZH I.</b> National integrated system of regulatory and legal acts: reality and possibilities.....	9
<b>DOVGAN O., YASCHENKO V.</b> Essence and content of legislation in the defense sector and its implementation: informational and legal research.....	17

### Legal Informatics

<b>LANDE D., LINENCO Y.</b> Network model of legal access restrictions for the Internet access in the world.....	26
<b>BRAYCHEVSKYY S.</b> Feedback in the internet of things systems with elements of artificial intelligence.....	32
<b>RADUTNIY O.</b> Legal education and the provision of legal services in the context of artificial intelligence.....	40
<b>DOROHYKH S.</b> Electronic parliament as the base of the construction of the national system of regulatory legal acts.....	55

### Informative and National Safety

<b>DZ'OBAN O., ZDANENKO S.</b> From “information society“ to “information security”: on the problem of conceptualizing the essence of concepts.....	60
<b>DORONIN I.</b> Legal problems of Internet sovereignty.....	74
<b>HREBENIUK M., LEONOV B.</b> The problems of countering dissemination of destructive propaganda and disinformation ahead of elections: analysis of the EU experience.....	82
<b>GUTSALYUK M.</b> Assessment of implementation of the cybersecurity strategy of Ukraine taking into account the experience of European and world practices...	90
<b>PETROV S.</b> Authority of the Security Service of Ukraine as a subject of national cybersecurity system.....	99
<b>KRAVCHENKO R.</b> Improving the effectiveness of counterintelligence search by military counterintelligence bodies of the Security Service of Ukraine with analysis of US law.....	106
<b>KULESHOV M.</b> The essence and content of the investigation of cyber incidents and cyberattacks by the Security Service of Ukraine units .....	115
<b>SANDUL V.</b> Improvement of the legislation and the curriculum of teaching the subject “Defense of the Motherland” in secondary schools.....	123

### **Information on other subject research directions by specializations in the field of knowledge 08 – “Right”**

<b>BELANYK M, VRONSKA T.</b> The first steps in the restoration of the work of the justice bodies on the Ukrainian territory liberated from the nazis (1943 – 1944).....	<b>129</b>
<b>NIZHNIK A.</b> Immunity of People's Deputy of Ukraine – constitutional and legal guarantee of the independent parliamentary control: information and legal aspect.....	<b>141</b>
<b>UHANOVA N.</b> The legal culture of youth in Ukraine.....	<b>156</b>
<b>BELEVSEVA V.</b> Migration regime for the stay of foreign citizens and stateless persons on the territory of Ukraine: the state and prospects.....	<b>167</b>
<b>DENYSOV A.I.</b> Perspectives of the establishment of special legal regimes of labor migrants.....	<b>172</b>
<b>KOSYTSIA O.</b> Public control for the protection of the rights of whistleblowers.....	<b>179</b>
<b>LYMAR I.</b> Discussion issues of the place of enforcement proceedings in the system of law of Ukraine.....	<b>186</b>
<b>For the consideration of authors.....</b>	<b>194</b>



## Інформаційне право

УДК 342.72/.73

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

### НАЦІОНАЛЬНА ІНТЕГРОВАНА СИСТЕМА НОРМАТИВНО-ПРАВОВИХ АКТІВ: РЕАЛЬНІСТЬ І МОЖЛИВОСТІ

**Анотація.** В даній статті досліджуються питання стану функціонування веб-сайтів органів державної влади та органів місцевого самоврядування в Україні; правове регулювання їхнього наповнення інформацією та їхньої структури; стан передумов для створення в Україні національної інтегрованої системи нормативно-правових актів; перспективи на майбутнє.

**Ключові слова:** веб-сайти, національна інтегрована система, нормативно-правові акти, органи державної влади, органи місцевого самоврядування, право.

**Summary.** This article examines the state of the functioning of websites of state authorities and local governments in Ukraine; legal regulation of their filling with information and their structure; the condition of the prerequisites for the creation of a national integrated system of legal acts in Ukraine; future prospects.

**Keywords:** web sites, national integrated system, regulatory and legal acts, state authorities, local authorities, right.

**Аннотация.** В данной статье исследуются вопросы состояния функционирования веб-сайтов органов государственной власти и органов местного самоуправления в Украине; правового регулирования их наполнения информацией и их структуры; состояние предпосылок для создания в Украине национальной интегрированной системы нормативно-правовых актов; перспективы на будущее.

**Ключевые слова:** веб-сайты, национальная интегрированная система, нормативно-правовые акты, органы государственной власти, органы местного самоуправления, право.

**Постановка проблеми.** В науці інформаційного права дослідники аналізують та здійснюють наукові розвідки щодо питання доступу до інформації та захисту даних в цілому, а також до правової інформації та до нормативно-правових актів держави, розкривають нинішні здобутки у цій царині та визначають проблеми, які необхідно вирішити. Так такі науковці як: О. Баранов, В. Белевцева, К. Беляков, В. Брижко, М. Демкова, О. Довгань, І. Доронін, О. Золотар, А. Марущак, В. Пилипчук, Н. Савінова та інші, у своїх працях розкривають зазначені та суміжні питання, аналізують існуючі проблеми та напрацьовують відповідні механізми їх вирішення. Однак поза увагою поки що залишається така загальнодержавна проблема, як створення та функціонування загальної системи нормативно-правових актів органів державної влади та органів місцевого самоврядування, або інакше – національної інтегрованої системи нормативно-правових актів.

**Метою статті** є дослідження питання нинішнього стану функціонування можливих складових згаданої системи, виявлення проблем в їхніх інтеграційних механізмах та напрацювання пропозицій щодо шляхів їх вирішення.

**Виклад основного матеріалу.** Отримання доступу до правової інформації, до змісту нормативно-правових актів, до управлінських рішень органів державної влади та органів місцевого самоврядування – це реальний здобуток українського суспільства в сучасних, демократичних умовах функціонування незалежної України. Щоб мати зазначені демократичні здобутки, Український народ здолав багато перешкод на цьому тернистому шляху до здобуття незалежності, до економічних, соціальних та правових перетворень, до можливості брати участь в управлінні державними справами зокрема, та управління державою – в цілому.

Доступ до інформації, до управлінських рішень держави має суттєве суспільне значення, і це стало своєрідним європейським і світовим трендом. За цих умов особливої ваги питання забезпечення доступу до правової інформації набувають для регіонального та місцевого рівнів публічного управління. Адже, незважаючи на напрацьований протягом останніх років досвід, публічні службовці нині мають розв'язувати нові комплексні та складні проблеми за цим напрямом діяльності, у тому числі з використанням сучасних інформаційно-комунікаційних технологій (далі – ІКТ). В умовах здійснення всебічних реформ в Україні, постійне удосконалення чинної нормативно-правової бази та організаційної структури органів влади спонукає запроваджувати та використовувати у практиці публічного управління та адміністрування нові технологічні інструменти, спрямовані на поліпшення інформаційних обмінів між органами влади та суспільством.

Сучасний етап суспільного розвитку та розвитку держави позначений динамічним проникненням ІКТ в усі сфери людської діяльності. За таких умов недостатня увага органів публічної влади до характеру, змісту інформаційних обмінів з громадськістю, більше того – їх недооцінка, можуть зумовити дисбаланс у відносинах влади й громадськості. З одного боку, це може спричинити збільшення кількості прийнятих нерезультативних і неефективних рішень, з іншого – зниження ступеня підтримки органів публічної влади суспільством, а то й відкритим протистоянням. Унаслідок такого стану справ значна кількість суспільно важливих проблем можуть залишитися невирішеними, належним чином не будуть прогнозовані та попереджені нові проблемні ситуації.

Як зазначають науковці, для нормального функціонування описаної системи взаємовідносин важливо досягти такого стану речей, коли потоки даних між органами публічної влади та громадськістю циркулюють максимально безперешкодно. Така модель може бути реалізована, коли кожен громадянин матиме реальну можливість отримання гарантованої законом повної, достовірної та всебічної інформації про функціонування органів влади, про їх плани, прийняті рішення, можливі напрями дій, стан окремих сфер суспільного життя, використання державних та комунальних ресурсів тощо [1, с. 7].

Окрім зазначеного, важливого значення набуває адаптація законодавства України, яке включає в себе окрім законів та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України [2] підзаконні акти органів державної влади та органів місцевого самоврядування. Зазначені підзаконні акти фактично є результатом прийняття управлінських рішень відповідно до прийнятих законів. Тому відповідність їхніх положень положенням законів, а останніх – відповідність законодавству Європейського Союзу, тобто їх адаптація, і визначає механізм досягнення Україною відповідності третьому Копенгагенському та Мадридському критеріям набуття членства в Європейському Союзі. Копенгагенські критерії були схвалені на засіданні Європейської Ради у Копенгагені у червні 1993 р. і включають в себе:

I) стабільність інститутів, що гарантують демократію, верховенство права, повагу до прав людини, повагу і захист національних меншин (політичні критерії);

II) наявність дієвої ринкової економіки і здатність витримувати конкурентний тиск і дію ринкових сил у межах ЄС (економічні критерії);

III) здатність узяти на себе зобов'язання, що випливають з членства в ЄС, включаючи суворе дотримання цілей політичного, економічного, валютного союзу (інші критерії) [3].

Мадридські критерії вимагають створення належних управлінських інституцій та судових органів, підсилення їх адміністративної спроможності, що має не тільки прискорити адаптацію національного законодавства до норм і правил ЄС, але й гарантуватиме впровадження і дотримання законів і надасть новим членам ЄС можливість скористатися перевагами членства (наприклад, отримати фінансову допомогу від Структурних фондів) [4].

Саме із зазначеною метою в Україні була напрацьована загальнодержавна програма адаптації законодавства України до законодавства Європейського Союзу, і яка була затверджена Законом [5], як механізму досягнення Україною відповідності згаданим критеріям і передбачає утворення відповідних інституцій та інші додаткові заходи, необхідні для ефективного правотворення та правозастосування.

Метою адаптації законодавства України до законодавства Європейського Союзу є досягнення відповідності правової системи України *acquis communautaire* з урахуванням критеріїв, що висунуті ЄС до держав, які мають намір вступити до нього. Під *acquis communautaire* (*acquis*) розуміється правова система ЄС, прийняті в рамках Європейського співтовариства, Спільної зовнішньої політики та політики безпеки і Співпраці у сфері юстиції та внутрішніх справ. Тому адаптація законодавства України до законодавства ЄС є пріоритетною складовою процесу інтеграції України до ЄС, що в свою чергу є пріоритетним напрямом української зовнішньої політики.

Необхідно зазначити, що нинішнє життя українського суспільства позначено динамічним застосуванням ІКТ в усіх сферах людської діяльності. Насамперед можна виділити електронні системи нормативно-правових актів. А тому, якщо буде проявлена недостатня увага органів публічної влади до характеру, змісту інформаційних обмінів з громадськістю, або щодо їх недооцінки, то це може зумовити певний дисбаланс у відносинах влади і громадськості. З одного боку, це може загрожувати збільшенням кількості нерезультативних і неефективних рішень, з іншого – зниженням ступеня підтримки органів публічної влади суспільством, або й відкритим протистоянням. Унаслідок такого стану справ значна кількість суспільно важливих проблем залишаться невирішеними, належним чином не будуть прогнозовані та попереджені нові проблемні ситуації. Для нормального функціонування описаної системи взаємовідносин важливо досягти такого стану речей, коли інформаційні потоки між органами публічної влади та громадськістю циркулюють максимально безперешкодно.

З огляду на зазначене та враховуючи здійснювані в Україні реформи (децентралізація, освітня, медична тощо), що передбачають зміщення акценту суспільного та бізнесового життя з умовного центру на периферію, тобто переведення повноважень та бюджетних надходжень від державних органів до органів місцевого самоврядування, забезпечення спроможності місцевого самоврядування самостійно, за рахунок власних ресурсів, вирішувати питання місцевого значення, що, у свою чергу, потребує активної участі в даних процесах громадськості, окремих громадян, яким не байдуже стан справ в регіоні. Громадяни мають займати активну життєву позицію, контролювати публічну владу та прийняті нею рішення, впливати на прийняття нею

рішень у різних сферах життєдіяльності не лише держави, а й регіону та місцевого рівня. Реалізувати зазначене громадяни можуть шляхом наявності вільного доступу до веб-сайтів органів публічної влади, на яких публікуються прийняті цими органами рішення, насамперед у вигляді прийнятих нормативно-правових актів.

На сьогоднішній день в Україні сформувалася наступна структура комунікації між публічною владою і громадянами, за якої громадяни можуть отримати інформацію про нормативно-правові акти та ухвалені органами різнобічні рішення:

- державний ресурс, який включає в себе інформаційно-комунікаційні системи: законодавчої влади; виконавчої влади; Президента України; судової влади; державних органів, які не відносяться до жодної гілки державної влади;

- регіональні ресурси, які включають в себе інформаційно-комунікаційні системи обласних рад;

- місцевий ресурс, який включає в себе інформаційно-комунікаційні системи міських та районних рад;

- інформаційно-комунікаційні системи приватного ресурсу різного рівня.

В Україні існує багато інформаційних ресурсів, що характеризуються різноманітними формами представлення інформації, організаційними та технологічними рішеннями, кількість яких збільшується одночасно із стрімким розвитком ІКТ. Під час цих процесів виникає багато проблем, до яких можна віднести:

- переважно галузевий принцип інформатизації органів державної влади та органів місцевого самоврядування, що призводить до обмеженості використання певних видів ресурсів;

- недостатня правова урегульованість механізму доступу громадян до державних електронних ресурсів, а також порядку надання і використання інформації про діяльність органів публічної влади та інших державних органів;

- недостатня правова урегульованість суспільних відносин, пов'язаних із формуванням, використанням та захистом згаданих ресурсів, у тому числі щодо комерційного використання державних ресурсів;

- необхідність приведення згаданих ресурсів у відповідність до єдиних державних стандартів на базі новітніх ІКТ, міжнародних стандартів, уніфікованих систем класифікації і кодування інформації;

- недостатня ефективність операційних, пошукових, геоінформаційних та навігаційних систем згаданих ресурсів;

- неопрацьованість загальних вимог до змісту згаданих ресурсів та обмежень щодо їх використання;

- відносно висока вартість користування ресурсами;

- недостатня розгалуженість згаданих систем.

Необхідно зазначити, що державний ресурс має значно менше недоліків. Так основні інформаційні ресурси веб-сайту Верховної Ради України містять інформацію про:

- законопроекти;

- закони України, постанови Верховної Ради України, міжнародні договори України;

- пленарні засідання Верховної Ради України та парламентські слухання;

- структуру Верховної Ради України;

- керівництво Верховної Ради України;

- депутатський корпус Верховної Ради України (всі скликання);

- депутатські фракції і групи;

- комітети та комісії Верховної Ради України;

- діяльність комітетів Верховної Ради України;
- діяльність тимчасових спеціальних і тимчасових слідчих комісій Верховної Ради України;
- міжпарламентські зв'язки;
- проведення перевірки відповідно до Закону України “Про очищення влади”;
- господарсько-фінансову діяльність Верховної Ради України;
- доступ до публічної інформації;
- порядок доступу громадян до відкритих пленарних засідань Верховної Ради України;
- висвітлення діяльності Верховної Ради України у ЗМІ;
- бібліотечно-бібліографічні ресурси Верховної Ради України;
- діяльність Апарату Верховної Ради України, а також посилення на веб-ресурси інших органів державної влади, органів влади інших держав та фото-, аудіо- та відеоматеріали, що висвітлюють діяльність Верховної Ради України. Реально ж веб-ресурс Верховної Ради України через базу даних нормативно-правових актів “Законодавство України” надає інформацію про нормативно-правові та інші акти більш широкого кола суб'єктів, включаючи міжнародних [6, с. 11]. Однак, інформація, розміщена на веб-порталі Верховної Ради України не носить офіційного характеру.

На нашу думку, доцільним було б запровадити на порталі Верховної Ради України, як вищого представницького органу держави, систему посилань на веб-сайти регіональних (обласних) представницьких органів місцевого самоврядування, що забезпечило б функціонування завершеного механізму єдиної системи представницьких органів в державі, оскільки, у свою чергу, веб-сайти регіональних органів місцевого самоврядування мають систему посилання на веб-сайти районних рад та веб-сайти міст районного порядкування.

У певному відношенні позитивно відрізняється від усіх веб-порталів публічної влади офіційне Інтернет-представництво Президента України, яке, окрім загальної та конкретної поточної інформації про Президента та його Адміністрацію, наявності механізму зворотного зв'язку з громадянами України, їхніх звернень, містить офіційні правові акти Президента України в електронному вигляді. Зазначене дозволяє громадянину мати доступ до офіційних актів Президента України.

Водночас, даний портал не містить посилання на веб-ресурси інших державних органів, фактично є локальним.

Найбільш розгалуженою, на нашу думку, Інтернет-мережею на сьогоднішній день є Урядовий портал, що становить єдиний веб-портал органів виконавчої влади України. Він містить посилання на веб-сайти Президента України, Верховної Ради України, Конституційного Суду України, Ради національної безпеки і оборони України, центральних та місцевих органів виконавчої влади. Представлено варіант порталу для людей з порушенням зору. Портал містить обширну інформацію діяльності Уряду та органів виконавчої влади, механізми зворотного зв'язку з громадянами через електронне звернення та подання ними петицій, а також через пряму телефонну лінію та урядову гарячу лінію, прийняті рішення та правові акти, електронні та адміністративні послуги. І уся зазначена інформація подається українською та англійською мовами.

Цікавими відповідно до досліджуваної нами тематики є мапи веб-сайтів з корисними посиланнями таких обласних рад, як: Житомирська, Харківська, Чернівецька та Чернігівська. Окрім загальної та конкретної інформації про діяльність рад, а також корисних посилань на інші веб-сайти, насамперед районних та міських рад, веб-сайти згаданих обласних рад мають посилання на веб-сайти інших обласних рад, утворюючи

своєрідну мікроінтегровану систему веб-сайтів представницьких органів України. Тобто, громадянин України, зайшовши на веб-сайт одного з цих чотирьох веб-сайтів, спроможний далі, по ланці, зайти на веб-сайт будь-якого регіонального чи місцевого представницького органу України і отримати інформацію про його діяльність чи видані ним правові акти. Це – своєрідний прообраз національної інтегрованої системи нормативно-правових актів України.

Веб-сайти органів державної влади (законодавчої, виконавчої, Президента України) створювалися та їхній зміст наповнюється відповідно до положень відповідних нормативно-правових актів [7; 8], тобто затверджується його внутрішній Порядок інформаційного наповнення з визначенням конкретних структурних підрозділів та посадових осіб, відповідальних за своєчасну підготовку і подання інформації та її зміст за кожним тематичним напрямом, веб-сайти органів місцевого самоврядування наповнюються лише відповідно до рекомендацій, висловлених у відповідних розпорядчих документах органів державної влади та самостійного підходу органу самоврядування до створення мапи веб-сайту та інформаційного його наповнення. Крім того, в них запроваджується система керування інформаційним вмістом веб-сайту яка має універсальну модульну архітектуру та включає: модуль адаптації інформації на веб-сайті для користувачів з вадами зору та слуху, модуль системи обліку публічної інформації, модуль пошукової теми, модуль адміністративних послуг, модуль електронних звернень громадян, модуль резервного копіювання даних веб-сайту на випадок непередбаченого збою тощо. Інформація на веб-сайтах є доступною для перегляду за допомогою різних браузерів. А матеріали, що складають інформаційне наповнення веб-сайтів, за своїм характером розподілені на три категорії: статичні матеріали; динамічні матеріали; потокові.

У свою чергу, веб-сайти органів місцевого самоврядування функціонують не у відповідності з відповідним керівним засадничим документом, яким би регулювалося питання напруцювання змісту веб-сайту та забезпечувалася б універсальність його мапи, а також наповнювався його контент, що сприяло б загалом універсалізації та консолідації веб-сайтів органів самоврядування, спростило б механізм його використання.

Аналіз веб-сайтів судової гілки влади нами не здійснюється, оскільки судові органи видають нормативно-правові акти для внутрішнього використання і на громадян вони не поширюються. Що ж до інших державних органів, які не відносяться до жодної гілки державної влади, такі як: Центральна виборча комісія; Уповноважений Верховної Ради України з прав людини; Рахункова палата України; Антимонопольний комітет України; Прокуратура України тощо, то вони мають власні веб-сайти, в яких громадяни мають можливість отримати інформацію про їхню діяльність і видані ними нормативно-правові акти. В них є посилання на веб-сайти вищих органів державної влади та окремих інших органів, які наповнюються і функціонують як і веб-сайти органів державної влади.

### **Висновки.**

Підсумовуючи викладене вище, можна зробити наступні висновки.

Питання державної політики у сфері Інтернет тісно пов'язані з темою права на інформацію. Регулювання відносин у глобальній мережі має опиратися, насамперед, на національне законодавство, яке, у свою чергу, має базуватися на міжнародному праві. Такими є, наприклад, такі міжнародні акти як: Окінавська хартія глобального інформаційного суспільства [9], Резолюція Генеральної Асамблеї ООН 60/45 “Досягнення у галузі інформатизації та телекомунікацій в контексті міжнародної безпеки” [10] тощо.

Загалом в умовах розвитку ІКТ можливості доступу до інформації значно виросли, що створює умови для вільного кругообігу значних обсягів інформації, знань. Виникають нові суспільні відносини, які потребують правової регламентації [11, с. 318].

В загальній системі нормативних правових актів, які регламентують організацію роботи органів публічної влади, лівову частку становлять підзаконні акти. На жаль, багато з них офіційно не оприлюднюються, оскільки, як вважається, не стосуються безпосередньо основних прав і свобод громадян. Це ускладнює доступ широких кіл громадськості до цих актів і породжує значну кількість перешкод у налагодженні взаємодії органів публічної влади з населенням. На сьогодні найбільш повне уявлення про цей нормативно-правовий масив дають комп'ютерні бази даних, зокрема "Законодавство України", "Ліга", "Нормативні акти України" та інші [12].

Аналіз зазначених та інших проблем сфери інформаційних ресурсів свідчить про необхідність вдосконалення державної політики у цій сфері. Нинішній стан порталів органів державної влади сприяє належному доступу громадян до нормативно-правової інформації, що не можна сказати про портали органів місцевого самоврядування. Тому на порядку денному державної політики нині стоїть питання напрацювання нормативно-правового акту, яким би визначалися засадничі положення щодо механізму наповнення інформацією та функціонування веб-сайтів органів місцевого самоврядування, єдиного підходу до структури мапи веб-сайту, напрацювання спроможності їхньої інтеграції для створення передумов формування національної інтегрованої системи нормативно-правових актів, базовими для якої мають стати портал Верховної Ради України або Урядовий портал. Тим самим, внаслідок реалізації даних пропозицій, в подальшому існуватимуть передумови для інтеграції створеної національної інтегрованої системи нормативно-правових актів з веб-сайтом Ради Європи, на якому можна знайти прийняті нормативні акти РЄ, що сприятиме інтеграції України до інформаційного і правового простору Європейського Союзу.

### Використана література

1. Пігарев Ю.Б., Дрешпак В.М., Куспльак І.С. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. Київ, 2017. Ч. 11: Доступ до публічної інформації. Київ: ФОП Москаленко О. М., 2017. 60 с.
2. Конституція України від 28.06.1996 р. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
3. Копенгагенські критерії членства в Європейському Союзі (інформаційно-аналітична довідка). URL: <https://mfa.gov.ua/ua/page/open/id/774> (дата звернення: 30.04.2019).
4. Оцінка та розвиток інституційної спроможності органів державної влади Європейського Союзу та його країн-членів щодо виконання покладених на них завдань. URL: [http://www.cpk.org.ua/index.php?option=com\\_content&view=article&id=866&Itemid=34](http://www.cpk.org.ua/index.php?option=com_content&view=article&id=866&Itemid=34) (дата звернення: 30.04.2019).
5. Про Загальнодержавну програму адаптації законодавства України до законодавства Європейського Союзу: Закон України від 18.03.04 р. № 1629-IV. *Відомості Верховної Рад України*. 2004. № 29. Ст. 367.
6. Корж І.Ф. Веб-сайти органів державної влади та органів місцевого самоврядування: механізми доступу до публічної інформації. *Інформація і право*. № 2(25)/2018. С. 9-16.
7. Про порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади: Постанова Кабінету Міністрів України від 04.01.02 р. № 3. *Урядовий кур'єр*. 2002. № 11.

8. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні: Указ Президента України від 31.07.00 р. № 928/2000. *Офіційний вісник України*. 2000. № 31. Ст. 1300.

9. Окинавская хартия глобального информационного общества от 22 червня 2000 г. URL: [https://zakon.rada.gov.ua/laws/show/998\\_163](https://zakon.rada.gov.ua/laws/show/998_163) (дата звернення: 06.05.2019).

10. Резолюция 60/45, принятая Генеральной Ассамблеей Организации Объединенных Наций, “Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности” (по докладу Первого комитета (A/60/452) от 08 грудня 2005 г.) URL: [https://zakon.rada.gov.ua/laws/show/995\\_e45](https://zakon.rada.gov.ua/laws/show/995_e45) (дата звернення: 06.05.2019).

11. Марущак А.І. Інформаційне право: доступ до інформації: навчальний посібник. Київ: КНТ, 2007. 532 с.

12. Багмет М.О. Історія та практика державного управління і місцевого самоврядування в Україні. Т. 2. Миколаїв: МДГУ, 2006. 292 с.

~~~~~ \* \* \* ~~~~~



УДК 355/359:342.9

ДОВГАНЬ О.Д., доктор юридичних наук, старший науковий співробітник,  
НДІ інформатики і права НАПрН України  
ЯЩЕНКО В.А., доктор юридичних наук, професор,  
НДІ інформатики і права НАПрН України

## СУТНІСТЬ І ЗМІСТ ЗАКОНОДАВСТВА У СЕКТОРІ ОБОРОНИ ТА ЙОГО РЕАЛІЗАЦІЇ: ІНФОРМАЦІЙНО-ПРАВОВЕ ДОСЛІДЖЕННЯ

**Анотація.** У статті досліджується система законодавства оборонного сектору, питання, пов'язані з процесом подальшого удосконалення правового регулювання безпеково-оборонного комплексу, які потребують наукового аналізу змін, що відбуваються. Зокрема, зроблено висновок, що військове право є окремим явищем у правовій системі, національній чи міжнародній, синтезуючи в собі основні риси загального права і специфічні особливості військово-професійного регулятора суспільних відносин. А реалізація військового права як його чільна конструктивна функція є однією з найактуальніших парадигм забезпечення оборони України.

**Ключові слова:** законодавство, військове право, оборонний комплекс, правове регулювання.

**Summary.** The article examines the system of legislation of the defense sector, issues related to the process of further improving the legal regulation of security and defense complex, which require a scientific analysis of the changes that take place. In particular, it was concluded that military law is a separate phenomenon in the legal system, national or international, by synthesizing the basic features of the general law and the specific features of the military-professional regulator of social relations. And the realization of military law as its main constructive function is one of the most urgent paradigms of the defense of Ukraine.

**Keywords:** legislation, military law, defense complex, legal regulation.

**Аннотация.** В статье исследуется система законодательства оборонного сектора, вопросы, связанные с процессом дальнейшего совершенствования правового регулирования безопасности оборонного комплекса, требующих научного анализа происходящего. В частности, сделан вывод, что военное право является отдельным явлением в правовой системе, национальной или международной, синтезируя в себе основные черты общего права и специфические особенности военно-профессионального регулятора общественных отношений. А реализация военного права как его главенствующая конструктивная функция является одной из самых актуальных парадигм обеспечения обороны Украины.

**Ключевые слова:** законодательство, военное право, оборонный комплекс, правовое регулирование.

**Постановка проблеми.** Розгляд у статті відповідного питання пов'язаний з процесом подальшого удосконалення правового регулювання безпеково-оборонного комплексу і потребою наукового аналізу змін, які відбуваються. Зокрема, у Законі України “Про національну безпеку України” замість словосполучення “військова організація держави” вжито новий термін “сектор безпеки та оборони”, який вимагає ґрунтовного висвітлення. Тим більш, коли мова йде про систему законодавства оборонного сектору, яка під кутом зору реалізації практично не розглядалась.

Це, безперечно, дасть можливість більш предметно і науково зважено втілювати його в життя Збройних Сил України.

Сфера оборони, в силу притаманних їй особливостей, вимагає в ході її висвітлення і відповідного теоретико-практичного осягнення. Виходячи з цього пропонується розпочати це дослідження з розведення понять об'єкту і предмету. Ця операція – обов'язкова умова застосування однієї з стратегічних методологій наукового пошуку – аналітико-синтетичної. Поняття об'єкту та предмету дослідження розводяться для того, щоб розглядати потім їх в єдності, тобто синтезувати нове знання.

Зазначаємо це тому, що аналітико-синтетичний підхід лежатиме в основі нашого подальшого дослідження. При цьому об'єктом дослідження є все те, на що спрямований наш науковий інтерес, предметом же виступає та складова об'єкту, яка, власне, надає нашому пошуку суттєвості, необхідності, цілеспрямованості.

У нашому випадку об'єктом дослідження виступає реалізація законодавства, як обов'язкового регулятора функціонування Збройних Сил України і оборони України в цілому. На нашу думку, саме феномен реалізації найбільш адекватно відображує проблему в її цілісності і багатоманітності, у чому, вважаємо, полягає сутність реалізації законодавства у сфері оборони.

Предметом же є діяльність владно-управлінських військових структур, як суб'єктів реалізації законодавства у сфері оборони. Разом з тим, оскільки оборона країни охоплює досить широку палітру сфер, суб'єктів, засобів здійснення і т.п., виходячи з мети дослідження пропонується зосередити увагу на об'єктно-предметній визначеності військового права і військового законодавства як регулятора військово-оборонних реалій.

**Результати аналізу наукових публікацій** – В основу написання даної статті покладено аналіз чинного законодавства, яке стосується предмету дослідження, а також творчий доробок відомих вітчизняних вчених та зарубіжних науковців, зокрема П. Богуцького [5], В. Брижка [9], В. Дяченка, М. Цюрупи, П. Шумського [8], О. Скакун [1], М. Кельмана [4], І. Коропатнік, І. Шопіна [2], В. Бачиніна [6], Л. Попова, Ю. Мигачева, С. Дихомирова [3] та ін. Проте, незважаючи на значний рівень наукового осмислення проблем реалізації законодавства, як обов'язкового регулятора функціонування оборонного сектора, пізнання сутності реалізації військового законодавства потребує і надалі, шляхом його поглиблення, тобто, розкриття більш глибоких його сутнісних характеристик. Тим більш, коли мова йде про систему законодавства оборонного сектору, яка під кутом зору реалізації практично не розглядалась.

**Метою статті** є удосконалення правового регулювання безпеково-оборонного комплексу України.

**Виклад основного матеріалу.** У довідково-енциклопедичній літературі термін “реалізація” у перекладі з пізньо-латинської (зречовлений, дійсний), означає здійснення, виконання.

Тут методологічно важливим є застосування діалектики можливості та дійсності, за якою будь-яке явище, існуюче потенційно, проблематично, набуває за певних умов статусу дійсності, реальності. Ось чому, вважаємо, має рацію О.Ф. Скакун, яка визначає термін реалізація як “втілення правових норм” [1, с. 579]. Правда, у неї мова йде про право взагалі. Але враховуючи, що законодавство – важлива складова правової сфери, термін “втілення” наближує нас до розкриття проблеми реалізації законодавства як втілення в дійсність його норм, що є, на нашу думку, його сутністю першого порядку.

Звичайно, реалізація законодавства не зводиться лише до його втілення в дійсність (здійснення). Але є найбільш суттєвим його атрибутом, бо як зазначалось вище, будь-яке наукове пізнання є процесом руху мислення від сутності першого порядку до сутності другого і так далі порядку, від менш глибокої до більш глибокої сутності...

Тож цей гносеологічний момент розшифровується ще й як зречовленість, тобто, опредмечування, набуття статусу предметності, інакше кажучи, нової конструктивної якості. Ця істина особливо важлива стосовно законодавства військового, конструктивними якостями якого, на думку авторів інноваційного з підручника з військового права є провідними, домінуючий метод його здійснення – імперативний (весільно-наказовий) та якості ординарного та складного механізмів реалізації військового права [2, с. 58-59].

Отже, сутністю реалізації військового законодавства є його втілення у військову сферу, у військову дійсність, тобто набуття цим законодавством опредмечення, статусів посюсторонності, принципу і правила правової поведінки.

Немає сумніву, що процес пізнання сутності реалізації військового законодавства буде продовжуватись і надалі шляхом його поглиблення, тобто, розкриття більш глибоких його сутнісних характеристик. Але це зовсім не означає, що у об'єкта пізнання, у даному випадку реалізації військового законодавства, є декілька різних сутностей.

Насправді ж сутність об'єкту пізнання завжди одна. Завдяки їй він, власне, і існує як даний об'єкт, а не щось інше. Предмети, речі, явища дійсності, як пізнавальні об'єкти, відрізняються один від одного перш за все своєю гносеологічною сутністю.

Таким чином, ще раз підкреслимо, сутністю процесу реалізації військового законодавства є його опредмечення, що здійснюється суб'єктами влади та військового управління у багатоманітній діяльності Збройних Сил України, її обороні.

Слід зазначити, що гносеологічна категорія сутності не є самодостатньою. В процесі пізнання вона так чи інакше тяжіє до поняття змісту. Зміст означає сукупність елементів даного пізнавального об'єкту та функцій, які ці елементи виконують. Справа в тому, що сутність предмета чи явища завжди одна, стабільна, незмінна. Вона – парадигма статичності. Зміст же – навпаки, параметр динаміки, рухомості, змінності. Фактично зміст – це діяльність конструктивна, цілеспрямована, перетворююча людська практика.

Ці теоретичні положення є для нас відправними, методологічними у подальшому аналізі змістовно-функціональних складових процесу реалізації законодавства у сфері оборони.

Перш за все викликає сумнів зведення процесу реалізації права і, відповідно, реалізації законодавства, в тому числі і військового законодавства лише до правозастосовної діяльності [1, с. 581]. На нашу думку, таке тлумачення дещо звужує, а отже, збіднює сам феномен реалізації законодавства. Адже правозастосовна – лише одна із функцій права, в якій реалізується законодавство. Але ця реалізація здійснюється в рівній мірі і в правотворчій, і в оборонній сферах, в яких не здійснюватися вона не може. Реалізація законодавства не зводиться лише до його застосування.

Разом з тим, реалізація законодавства і його правозастосовна функція органічно пов'язані між собою. Але це, на нашу думку, не тип зв'язку тотожності чи протилежності, а саме, правозастосовна функція законодавства є способом його реалізації. Фактично в дійсності має місце не феномен реалізації законодавства взагалі, а конкретний спосіб його опредмечення.

Адміністративне, військове, цивільне, адміністративне право тощо відрізняються одне від одного не лише належністю до тієї чи іншої сфери (галузі) відносин, – це більшою мірою в даному випадку зовнішня їх ознака, – а відрізняються тим, як, яким способом здійснюється їх реалізація.

Що стосується власне, правозастосування, то воно, на відміну від інших, пасивних способів реалізації права, є суто практичним, активним його опредмеченням. У зв'язку з

цим підлягає критичному аналізу кваліфікація військового права як комплексного правового феномену, що роблять сьогодні більшість дослідників.

Зокрема, на думку П.П. Богуцького “...Військове право є комплексною галуззю права – системою загальнообов’язкових норм, формально визначених правил поведінки у військово-публічній сфері, які встановлені, охороняються та забезпечуються державою, здійснюють регулювання суспільних відносин, пов’язаних з діяльністю Воєнної організації суспільства, і мають за мету забезпечення захисту держави, її суверенітету, територіальної цілісності” [5, с. 60].

Автори підручника з військового права теж вважають, що “Військове право – це комплексна галузь права, яка регулює суспільні відносини, пов’язані з організацією функціонування військових формувань та захистом держави у разі збройної агресії або збройного конфлікту” [2, с. 8].

Зрозуміти це можна, тому що дійсно, військове право начебто вбирає в себе риси різних галузей права: адміністративного, цивільного, господарського тощо. Тому вважаємо, що дана точка зору має право на існування. Але атрибутивно військове право є монополією на спосіб його здійснення, про який більш детально мова йтиме нижче.

Протилежною точкою зору є віднесення військового права до чисто галузевого, скажімо, адміністративного, з чим також навряд чи можна погодитися. І перша, і друга позиції, на нашу думку, є крайнощами, які дещо суперечать об’єктивній істині.

Правила формальної логіки щодо визначення понять передбачають перш за все, встановлення родової належності феномену, поняття про яке йде мова. Що стосується військового права, постає питання, до якого більш широкого класу чи роду воно належить.

У більшості випадків військове право розглядається як складова правової реальності взагалі, з чим, в принципі, слід погодитися. Військове право дійсно є одним із елементів більш широкого правового і законодавчого комплексу країни, нації, держави. Але в чинній теорії держави та права, військове право розглядається як частина цілого, тобто, права взагалі.

Але такий підхід, вважаємо, є помилковим, бо частина і ціле не є діалектичними категоріями, хоча б тому, що частина не завжди несе в собі риси цілого. Сепаратизм, наприклад, який спровокований зовні, на жаль, має місце в українському сьогоденні, є частиною умонастрою окремих груп населення. Але заявляти, що він є втіленням інтересів всього українського суспільства, було б невірним.

Не має рації, вважаємо, і кваліфікація родової належності військового права як лише суто національного фактору, як це робиться сьогодні в російських підручниках з військового права [3, с. 25]. На нашу думку, така позиція теоретично хибна і соціально небезпечна, оскільки є нічим іншим, як безпідставною спробою включити невичерпний зміст військового права в “прокрустове ложе” російського державного шовінізму.

Насправді ж діалектика військового права і права взагалі – це діалектика загального і одиничного, окремого. Військове право є окремим явищем у правовій системі, національній чи міжнародній, синтезуючи в собі основні риси загального права і специфічні особливості військово-професійного регулятора суспільних відносин.

Тут мова йде вже не про родову його належність, його комплексність чи галузевість, а про його видову сутнісну визначеність. Фахівці справедливо зазначають, що вона, ця сутність, пов’язана з військовою діяльністю. Саме належність до війни, як особливої форми насилля, є тим, що відрізняє військове право від усіх інших правових явищ. “Війна є продовження політики іншими, насильницькими методами”. Ця крилата фраза Клаузевіца залишається методологічно визначальною для розкриття сутності військового права.

І справа тут, вважаємо, не в галузевості, – якраз це суто зовнішня риса військового права, – а в способі регулювання: як, яким чином регулюються відносини у військовій сфері. Це в першу чергу стосується насилля, яке діалектично пов'язане з поняттям примусовості. Саме примус по відношенню до насилля є його родовим явищем. Категорія примусу і визначається в юридичній літературі як “соціальна практика впливу одних суб'єктів на інших, з метою змусити їх робити те, чого вони за власною волею здійснювати не бажають” [6, с. 644].

Що ж стосується родової, сутнісної визначеності насилля, то головною його ознакою є застосування примусу у формі сили. Оскільки сила – явище багатоманітне, звідси багатство різновидів насилля, його способів, прийомів, відтінків тощо, від мирного до військового і т.п. Можливо, саме абстрактний підхід до оцінки цього явища не дав можливості належною мірою своєчасно здійснити адекватну відповідь насильницьким діям РФ щодо України.

Особливістю насилля, у тому числі військового насилля, є те, що воно змінюється історично, як змінюється і сам характер війни. Сучасна війна набуває рис, які в ній були відсутні в минулому.

Невипадково сьогодні у вжитку терміни “військовий конфлікт”, “гібридна війна” і т.п., а сутнісний атрибут насилля в них не є однозначним, тобто, лише військовим насиллям. У зв'язку з цим військовий конфлікт між державами, як форму військового насилля, доцільно розглядати в межах співвідношення інших категорій: мирного та немирного насилля. І вже на цій діалектиці робити висновок про справедливість чи несправедливість військового насилля.

Виходячи з цих філософсько-правових, етичних міркувань, зазначимо, що парадигма волевиявлення, яка відносить військове право до родового правового чинника, відзначається підвищеною мірою і ступінню прояву волі в регулюванні військових відносин, на відміну від інших сфер чи галузей права.

Військове право, таким чином, є феноменом унікальним, воно синтезує в собі не лише властивості загального та окремого, а й свої специфічні, особливі закономірності. Таким унікальним завжди була і залишається військова діяльність і перш за все військові дії, як головний об'єкт правового регулювання.

Отже, військове право і, відповідно, військове законодавство є важливим компонентом правової системи держави, нації, соціальної спільноти, сутністю якого є підвищений насильницько-вольовий інгредієнт регулятивної діяльності. Цей інгредієнт має включати два компоненти насилля: мирного і суто військового (немирного), і їх співвідношення по лінії пріоритетності військового вольового чинника.

Всі ці теоретичні зауваження щодо об'єкту аналізу як процесу реалізації права і законодавства принципово важливі і в ході висвітлення предмету пошуку. Як вище зазначалось, предметом є діяльність владно-управлінських військових структур як суб'єктів реалізації, тобто, опредмечення законодавства в сфері оборони країни.

Поверхово ми уже торкнулися питання співвідношення права та законодавства, але у найбільш загальному вигляді. Діалектика ж їх більш глибока. Розглянемо її. Законодавство виступає важливою складовою права. Але яке їх концептуальне співвідношення? Як конкретно пов'язані між собою законодавство і право?

У відповідях на ці запитання в юридичній літературі однозначного розуміння немає. Зокрема, О.Ф. Скакун законодавство трактується як чисто зовнішня, тобто, несуттєва канва права. Вона пише наступне: “законодавство є зовнішнім результатом законотворчості” [1, с. 173]. М.С. Кельман, вказуючи на зв'язок системи права з системою законодавства і вбачає цей зв'язок в тому, що “система законодавства є зовнішньою формою права” [4,

с. 398]. Головна вада цих міркувань – неврахування діалектики зовнішнього та внутрішнього, за якою зовнішнє, (тобто, поверхове, несуттєве, випадкове) не існує без внутрішнього, того, що характеризує власну природу і зміст, своєрідність того, чи іншого явища, речі, події.

Діалектика зовнішнього і внутрішнього ще й така, що вони єдині, і в цій єдності “визначальним є внутрішнє, бо будь-який розвиток має своїм джерелом саморух, тобто, внутрішню суперечливість, протиріччя. Врахування діалектики внутрішнього та зовнішнього в законодавстві дає нам уявлення про його сутнісно-змістовну визначеність. Взагалі ж найбільш адекватним у визначенні поняття законодавства і розкриття його співвідношення з правом ми вважаємо есенційно-діяльнісний методологічний підхід. “Есенційний (сутнісний) аналіз дає змогу з’ясувати найбільш глибоку атрибутивну характеристику законодавства і його однопорядковість з категорією закону, який є необхідним, суттєвим, постійним, об’єктивним співвідношенням між явищами природи та суспільства”.

Це стосується і закону як юридичної категорії, атрибутивними характеристиками якого на думку вчених є суще та необхідне [6, с. 310]. Оскільки закони суспільства, тим більш у юридичному статусі, суб’єктивні за формою, бо діють лише через свідомість, то вони не виникають самі по собі, хоча за змістом і об’єктивні.

Їх необхідно відкрити, видати, розповсюдити і забезпечити реалізацію. Все це – параметри діяльнісного підходу. У нашому випадку мова йде про діяльність оборонних суб’єктів із забезпечення реалізації законодавства. Ця діяльність – головна змістовна складова предмету нашого дослідження. Отже, законодавство – це та складова правових відносин (не частина, а сфера), яка полягає у створенні, виданні та реалізації законів як правової парадигми регулювання суспільного життя.

Саме в контексті єдності сущого та необхідного спостерігається, на нашу думку, і співпадіння (звичайно, не тотожне, а діалектичне) законодавства та права. У зв’язку з цим ми не можемо не нагадати про свою точку зору щодо природи права, яку оприлюднили свого часу.

Мова йде про залучення екзистенційного підходу до з’ясування сутності та походження феномену права як чисто гуманістичного явища. Цей підхід дозволив нам визначити право як волю людини до самоіснування (що юридичною мовою трактується як суще). Але це суще не є чисто суб’єктивною категорією відокремленого індивіда. Воно не є й синонімом протилежного, так би мовити, стадійного існування, моральної поведінки.

Суще в даному випадку слугує для характеристики автономії існування, в основі якої лежить необхідність комунікації. Закон і є однією з форм цієї необхідності. Право і закон мають, таким чином, атрибутивну спорідненість. Саме вона лежить в основі співпадіння цих двох феноменів. Комунікативна природа діяльності з забезпечення реалізації законодавства у сфері оборони не викликає ніякого сумніву.

Все вищесказане переконує, що законодавство є не формою права, законодавство є способом його існування, що поєднує в собі зміст і форму права. Таким чином, військове законодавство є змістовним втіленням військового права, його реалізацією.

Постульований діяльнісний підхід зумовлює реалізацію військового законодавства у сфері оборони в єдності трьох взаємопов’язаних змістовно-функціональних складових: дотримання чинного військового законодавства, його практичного застосування і подальшого його конструктивного удосконалення. Зупинимось на аналізі цих різновидів опредмечення військового законодавства.

Перша складова – дотримання законодавства. Мова йде про забезпечення такого стану функціонування Збройних Сил України, який адекватно відповідає вимогам чинного військового законодавства. Що стосується військовослужбовців, то це стан їх

зразкової, правомірної поведінки. Забезпечення цієї правомірності – першочергове завдання владно-військових управлінських структур.

Отже, дотримання як форма реалізації права у військовому законодавстві має особливе значення. Не стільки в утриманні від негативних, протиправних вчинків, про що пишуть О.Ф. Скаун та інші автори [1, с. 580], а навпаки, що дотримання військового законодавства дозволяє його суб'єктам зануритись у чинну військово-правову реальність і досягнути її змістовну визначеність і узгодити свою власну поведінку з вимогами законодавства. Власне, дотримання є своєрідною передумовою подальшої їх поведінки як суб'єктів права, на чому і будується процес реалізації законодавства.

Наприклад, дотримання норм міжнародного гуманітарного права (далі – МГП), які передбачають чітке розмежування військових і цивільних об'єктів в ході ведення бойових дій. Зокрема, Додатковий Протокол 1 до Женевських Конвенцій 1949 р. передбачає, що “цивільні об'єкти не повинні бути об'єктом нападу або репресій.... Напади повинні суворо обмежуватися воєнними об'єктами”. При цьому мова йде не лише про утримання від нападу на цивільні об'єкти, а й захисту культурних цінностей, об'єктів, необхідних для виживання цивільного населення тощо [7, с. 238-239]. Таким чином, дотримання виступає не лише пасивною формою реалізації права, а й тяжіє до функцій виконання і використання норм права.

Оскільки в теорії права, крім дотримання, безпосередніми формами реалізації права називаються “виконання” та “використання” зазначимо, що феномен дотримання певною мірою включає ці дві складові реалізації, тому в ході характеристики поняття “дотримання” військового законодавства вважаємо їх його атрибутивними якостями.

Друга складова реалізації – це застосування військового права, яка є суто практичною його парадигмою. Про це, зокрема, свідчать і визначення сутності правозастосовної діяльності, що наведені в числених працях.

М.С. Кельман, наприклад, визначає правозастосовну діяльність як організаційну, що здійснюється владними державними органами з реалізації правових норм [4, с. 438]. О.Ф. Скаун розглядає правозастосовну діяльність як “здійснювану у процедурно-процесуальному порядку владно-організуючу діяльність уповноважених державних органів організацій і посадових осіб, яка полягає у реалізації ними правових норм стосовно конкретних суб'єктів і конкретних життєвих випадків, через винесення індивідуально правових рішень” [1, с. 581]. Відповідно до таких підходів, правозастосовна діяльність виступає формою реалізації норм права.

З цим навряд чи можна погодитися, оскільки це відриває норму права від її змісту. Таким чином правозастосування є не формою, а особливим способом реалізації законодавства. І цю особливість, зокрема, відображає практична багатоаспектність і поліфункціональність правозастосування.

Рівною мірою це стосується і такого важливого правового компоненту, як військове право. Про це свідчить те, що застосування військового права має ті ж ознаки, які притаманні правозастосуванню взагалі. Це перш за все владний характер застосування військового права, оскільки здійснюється органами військового управління, які мають владно-організаційні повноваження, є процесом – офіційним порядком дій, що складається з низки послідовних стадій і прерогативою при цьому виступає військова необхідність, як регулятивна норма – принцип.

Саме ця необхідність виступає ключовим елементом застосування військового права, що відрізняє його від інших форм регулювання суспільних відносин. Навіть заборона МГП нападу на цивільні об'єкти припиняється, “якщо такий напад є єдиним

практично можливим способом припинити використання цього об'єкту для регулярної, суттєвої, безпосередньої підтримки воєнних операцій" [7, с. 240].

За своїм змістом застосування військового права є досить складним, поліфункціональним процесом: це і визначення правових основ оборони; і військового будівництва; і організації застосування Збройних Сил, у тому числі при правових режимах особливого періоду та воєнного стану; і забезпечення правових основ військової служби; і визначення правового статусу військовослужбовців та ін.

Але ця поліфункціональність не повинна відволікати від головного цілеспрямованого розкриття особливостей атрибутивної специфіки саме військово-бойового чинника функціонування Збройних Сил України. Як зазначають В.І. Дяченко, М.В. Цюрупа, П.В. Шумський: "...важко долається інерція воєнно-теоретичного мислення, згідно з якою вважалось, що праву не слід втручатися в теорію і практику військового мистецтва, інакше норми та правила унеможливають ініціативу, творчість, активність військового керівника, тобто принципово заперечують воєнному мистецтву" [8, с. 113].

Всупереч цьому зазначимо, що в сучасних умовах військове мистецтво не є самодостатнім, воно органічно вплетене в правове поле, інформаційну реальність, психологію сучасного збройного конфлікту. Тому синтез військового мистецтва і військової правотворчості має бути закономірним явищем в комплексі реалізації військового права і військового законодавства.

Оскільки правозастосовна діяльність – це діяльність організаційна, провідним принципом її організації є принцип стадійності, який регулює також застосування й військового права. Виділяються, як правило, три основних стадії процесу застосування права: встановлення та аналіз фактичних обставин справи, вибір норми права та її аналіз (тлумачення), прийняття рішення у справі.

Що стосується останніх постульованих нами складових правозастосування: ідеології, функціональності та стадійності, то вони набувають особливої ваги у застосуванні військового права. Зокрема, реалізація Міжнародного гуманітарного права в Україні здійснюється поетапно: ратифікація Конвенцій і додаткових Протоколів до них Верховною Радою України, інтеграція норм МГП в діяльність Збройних Сил України спочатку за окремими наказами, наступний крок – розширення впровадження даних норм у всі конкретні сфери військової діяльності.

При цьому ідеологічний і функціональний аспекти пов'язані з євроатлантичною інтеграцією Збройних Сил України і долученням їх до цивілізаційних досягнень.

### **Висновки.**

Військове право посідає особливе місце в правовій системі України. Ця особливість полягає в тому, що військове право не є однозначно комплексним чи чинно галузевим феноменом, а унікальним правовим явищем зі своїми власними атрибутивними закономірностями, що втілюють все багатство військово-професійної сфери і виступає відносно самостійним чинником регулювання військових відносин.

Реалізація військового права як його чільна конструктивна функція є однією з найактуальніших парадигм забезпечення оборони України.

### **Використана література**

1. Скакун О.Ф. Теорія держави і права (Енциклопедичний курс): підручник. Харків: Еспада, 2006. 776с.
2. Військове право: підручник/ за ред. І.М. Коропаткіна, І.М. Шопіної. Київ: Алерта, 2019. 648 с.



3. Попов Л.Л., Мигачев Ю.И., Дихомиров СВ. Военное право: учебник/ под ред. Ю.И. Мигачева. Москва: Юристъ, 2008. 576 с.
4. Кельман М.С. Загальна теорія держави і права: підручник. Київ: Вид. Кондор, 2016. 716 с.
5. Богущкий П.П. Військове право України: джерела, структура та розвиток: монографія. Одеса: Фенікс, 2008. 188 с.
6. Бачинин В. Энциклопедия философии и социологии права. СПб.: Издательство Р. Асланова “Юридический центр Пресс”, 2006. 1093 с.
7. Женевские Конвенции от 12 августа 1949 года и Дополнительные протоколы к ним. Изд. 5-е, доп. Москва: Международный Комитет Красного Креста, 2011. 302 с.
8. Дяченко В.І., Цюрупа М.В., Шумський П.В. Міжнародне гуманітарне право: філософсько-правова доктрина регулювання збройних конфліктів. Ч.І. Історія становлення. Київ: Сфера, 1999. 128 с.
9. Брижко В. До гносеології категорії “право”. *Правова інформатика*. № 3(15)/2007. С. 24-32; Домінанта праворозуміння та основ понятійно-категоріального апарату інформаційного права. *Інформація і право*. № 3(3)/2011. С. 5-17.

~~~~~ \* \* \* ~~~~~

## Правова інформатика

УДК 004.773

ЛАНДЕ Д.В., доктор технічних наук, професор,  
керівник наукового центру НДІ інформатики і права НАПрН України  
ЛІНЕНКО Ю.О., магістрант НТУУ “КПІ ім. Ігоря Сікорського”

### МЕРЕЖЕВА МОДЕЛЬ ПРАВОВИХ ОБМЕЖЕНЬ ДОСТУПУ ДО ІНТЕРНЕТУ У СВІТІ

**Анотація.** У ряді країн сучасного світу доступ користувачів до мережі Інтернет підлягає суттєвим правовим обмеженням. У статті викладено підхід до вивчення цього явища. Представлено метод формування і дослідження відповідної мережевої моделі Інтернет-обмежень. Змістовне пояснення обмеження доступу до соціальних мереж та інших Інтернет-ресурсів ґрунтується на правових актах окремих держав.

**Ключові слова:** Інтернет-обмеження, міжнародне право, мережева модель, соціальні мережі, таблиця обмежень.

**Summary.** At this time, in a number of countries, users' access to the Internet is subject to significant legal constraints. The article describes the approach to studying this phenomenon. The method of formation and research of the corresponding network model of Internet restrictions is presented. A meaningful explanation for restricting access to social networks and other Internet resources is based on legal acts of individual countries.

**Keywords:** Internet restrictions, international law, network model, social networks, table of restrictions.

**Аннотация.** В ряде стран современного мира доступ пользователей к сети Интернет имеет существенные правовые ограничения. В статье изложены подход к изучению этого явления. Представлен метод формирования и исследования соответствующей сетевой модели Интернет-ограничений. Содержательное объяснение ограничения доступа к социальным сетям и другим Интернет-ресурсам основывается на правовых актах отдельных государств.

**Ключевые слова:** Интернет-ограничения, международное право, сетевая модель, социальные сети, таблица ограничений.

**Постановка проблеми.** На цей час у багатьох країнах світу існують обмеження доступу громадян до Інтернет-ресурсів, зокрема соціальних мереж і месенджерів. Оскільки подібні обмеження у Інтернет-сфері застосовуються досить широко, існує потреба у спеціальному програмному забезпеченні, методах і засобах аналізу, візуалізації, формального рейтингування і класифікації подібних явищ. Більш того, це явище потребує всебічного дослідження, яке може бути предметом вивчення у рамках правової науки і соціології. Проте, для аналізу стану обмежень в Інтернеті до цього часу не вистачає інструментальних засобів, програмних модулів і методик, що надаються експертам.

Також актуальність дослідження полягає у наявності потенційних складнощів, які можуть виникнути у сфері комунікацій, які обумовлені наявністю у деяких країнах обмежень доступу до ресурсів глобальної мережі Інтернет.

**Метою статті** є визначення системи комунікації в умовах існування обмежень до ресурсів мережі Інтернет, а також опис мережевої технології дослідження правових обмежень доступу користувачів до соціальних мереж і подібних сервісів – месенджерів, мікроблогів тощо.

**Виклад основного матеріалу.** Інтернет-обмеження можуть реалізовуватись у формі закриття та/або блокування веб-ресурсів, обмеження трафіку, створення фіктивних опозиційних ресурсів тощо. За спроби обійти подібні обмеження до громадян можуть застосовуватись каральні засоби [1]. Держави, уряди яких здійснюють Інтернет-обмеження, часто приймають відповідні правові акти, які закріплюють державний контроль у сфері доступу до Інтернету. Наприклад в Ірані на початку 2000-х років був прийнятий указ “Політика по відношенню до комп’ютерних мереж”, який зобов’язує усіх Інтернет-провайдерів в межах країни отримати спеціальну ліцензію від уряду. У 2016 році у КНР прийняли новий Закон “Про кібербезпеку”, згідно з яким оператори мережі зобов’язані реєструвати китайських користувачів під їх справжніми іменами та зберігати усі персональні дані в Китаї. Коло сайтів, які підлягають або можуть підлягати фільтрації є різним. Але в першу чергу фільтруються соціальні мережі та месенджери: Facebook, Twitter, Instagram, Telegram, Wechat, LinkedIn тощо. Існують способи “незаконного” подолання Інтернет-фільтрації: використання спеціальних проксі-серверів, веб-проксі, анонімних мереж, он-лайн-перекладачів, RSS-агрегаторів, електронної пошти, віртуальних приватних мереж тощо.

Інтернет-фільтрація також може практикуватись з метою захисту від дійсно небезпечної для суспільства інформації [2]. Наприклад, у Франції на урядовому рівні йде впровадження централізованих фільтрів, які створено з метою блокування доступу школярів до сайтів расистського, антисемітського й неонацистського спрямування.

У травні 2017 року Президент України підписав указ, за яким введено в дію рішення РНБО про оновлення списку санкцій проти російських компаній. Серед підпадаючих під санкції російських компаній є соціальні мережі “Вконтакте” й “Однокласники”, електронний поштовий сервіс “mail.ru” та інші. Було встановлено санкційний термін у три роки. Цей указ обумовлений гібридною війною, яка ведеться проти нашої держави.

#### **Опис моделі.**

Для побудови моделі вибрано у якості бази декілька країн і Інтернет-ресурсів. До розгляду не були включені країни типу Куби або Північної Кореї, де заборонено практично усі соціальні мережі. Саме розглядаються можливості доступу у 10 країнах до 12 Інтернет-ресурсів, перелік яких наведено у Таблиці. Крім того, не розглядаються такі мережеві ресурси як окремі веб-сайти, великі групи з яких на законних засадах заборонені навіть у європейських країнах з найбільшою свободою у Інтернеті. Дані, що розглядаються у цій роботі актуальні, але ще далеко не повні. Вони використовуються скоріше як приклад, полігон для демонстрації методу. Пропонується скоріше технологія дослідження щодо питання обмеження доступу.

Таблиця. Обмеження доступу до Інтернет-ресурсів у деяких країнах

| Інтернет-ресурс | Країни  |
|-----------------|---|
| Facebook        | Китай, Іран, Єгипет, Туреччина, Пакистан, Саудівська Аравія |
| Twitter         | Китай, Іран, Туркменістан, Єгипет, Туреччина                |
| Wechat          | Туркменістан, Іран, Росія                                   |
| LinkedIn        | Росія, Куба, Іран   |
| Instagram       | Китай, Туреччина, Туркменістан, Іран                        |
| “Вконтакте”     | Україна, Туркменістан, Іран                                 |
| “Однокласники”  | Україна, Китай  |

|          |   |
|----------|---|
| Telegram | Росія, Іран, Китай, Пакистан                                |
| Viber    | Китай, Пакистан, Узбекистан                                 |
| Whatsapp | Китай, Туркменістан, Пакистан                               |
| Skype    | Китай, Росія, Узбекистан                                    |
| Youtube  | Іран, Пакистан, Китай, Єгипет, Туреччина, Саудівська Аравія |

Розглянемо інформацію з Таблиці за країнами більш докладно.

**Китай.** Доступ до ряду іноземних сайтів з території КНР обмежується в рамках проекту “Золотий щит” (так званий Великий китайський файрвол). Веб-сторінки фільтруються за ключовими словами, пов’язаними з державною безпекою, а також за “чорним списком” адрес сайтів. Фільтрації підлягають Facebook, Twitter, Instagram, “Однокласники”, Telegram й багато інших західних ресурсів.

**Іран.** В Ірані держава дуже жорстко обмежує неконтрольований доступ населення до Всесвітньої павутини. Під забороною знаходиться Youtube, Facebook, Twitter, Wechat, Linkedin, Instagram, “Вконтате” й Telegram.

**Єгипет.** У Єгипті, незважаючи на проголошені свободи слова та думки, законодавство залишає для влади простір для блокування контенту: фільтруються Youtube, Facebook й Twitter.

**Туреччина.** У Туреччині громадянам заблокований доступ до Facebook, Twitter, Instagram й Youtube.

**Пакистан.** У Пакистані за рішенням суду був заблокований Youtube. Під фільтрацію також попадають Facebook, Viber, Telegram й Whatsapp.

**Саудівська Аравія.** У Саудівській Аравії встановлено низку правил й обмежень щодо розповсюдження інформації. У зв’язку з цим Інтернет-фільтрація розповсюджується на такі ресурси як Facebook, Youtube й інші.

**Туркменістан.** У Туркменістані Інтернет-фільтрація розповсюджується на Twitter, Wechat, Instagram, “Вконтакте” й Whatsapp.

**Росія.** На даний момент в Росії заблоковані Wechat, Lindedin, Telegram й Skype.

**Україна.** 16 травня 2017 року Президентом України підписано указ [3], за яким введено в дію рішення РНБО про оновлення списку санкцій проти ряду російських компаній, серед яких соціальні мережі “Вконтакте” і “Однокласники”, електронний поштовий сервіс “mail.ru” тощо.

**Узбекистан.** Інтернет-фільтрація в Узбекистані розповсюджується на Viber й Skype.

З формальної точки зору наведену таблицю можна представити у вигляді біграфу, один сегмент якої – Інтернет-ресурси, інший – держави [4]. Ці сегменти з’єднуються один з одним зв’язками із значенням “обмеження доступу”. Відповідно пропонується сформулювати матрицю цих зв’язків, яку можна зберігати на комп’ютерному носії у форматі csv.

Для візуалізації і подальшого аналізу сформованого біграфу (мережі зв’язків “обмежень” між державами і Інтернет-ресурсами) можна застосувати низку програмних систем, одна з яких – Gephi (<http://gephi.org>) [5]. Після завантаження сформованого csv-файлу отримано графічне відображення мережі (Рис. 1) і визначено основні параметри мережі: кількість вузлів – 22; кількість зв’язків – 44; щільність графу – 0,095 тощо.

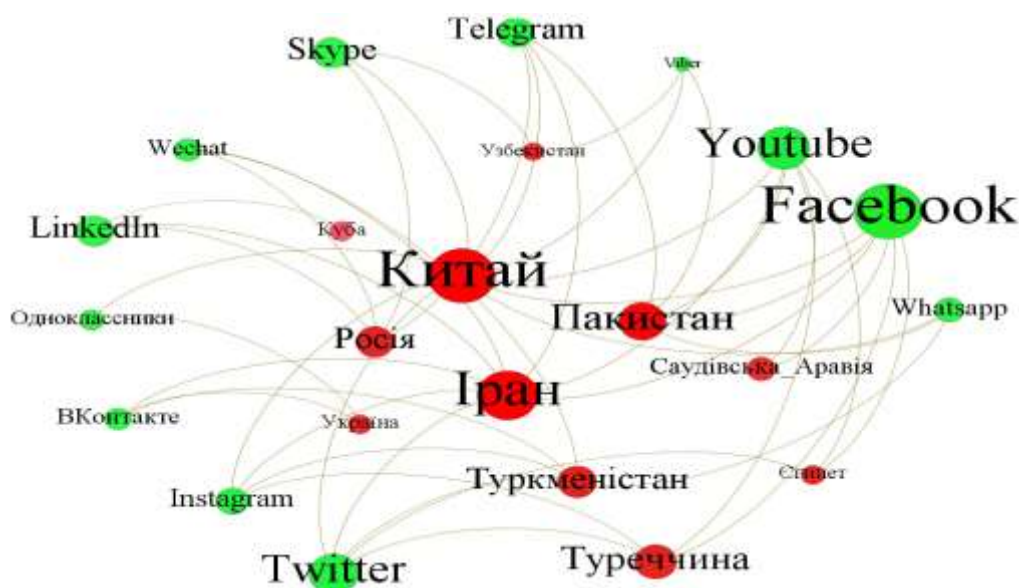


Рис. 1. Мережа Інтернет-обмежень

Як один із напрямків аналізу соціальних мереж можна розглядати ранжирування вузлів за різними критеріями, зокрема PageRank [6] і HITS [7].

Алгоритм HITS забезпечує вибір з інформаційного масиву кращих вузлів, на які введуть посилання (“авторів”, у нашому випадку країн) і “посередників” (вузлів, від яких йдуть посилання цитування, у нашому випадку – Інтернет-ресурсів, доступ до яких обмежується).

Відповідно до алгоритму HITS, для кожного вузла мережі –  $m_j$  рекурсивно вираховується його значимість як автора –  $a(m_j)$ , при цьому підрахунок суми проводиться за всіма вузлами, які посилаються на даний вузол, та посередника (хаба) –  $h(m_j)$ , де підрахунок суми проводиться за всіма вузлами на які посилаються у даному вузлі.

$$a(m_j) = \sum_{i \rightarrow j} h(m_i); \quad h(m_j) = \sum_{j \rightarrow i} a(m_i);$$

Рейтингування вузлів дає змогу виявляти країни з найбільшим обмеженням доступу до Інтернет-ресурсів, і Інтернет-ресурсів, що найбільше обмежуються.

Для мережі, що розглядається, результати ранжирування за цими критеріями наведено далі на Рис. 2. Слід відзначити, що ранжирування вузлів за критерієм HITS має більшу розподільну здатність. Можна бачити, що тільки він дозволяє розділяти Інтернет-ресурси за ступенем “обмеженості”.

### Висновки.

У роботі представлено інформаційну мережеву технологію, методологію побудови і формального дослідження мереж обмежень доступу до Інтернет-ресурсів.

Представлена технологія дозволяє ранжувати Інтернет-ресурси і держави за рівнем обмеження перших другими.

Мережева технологія також дозволяє виявляти кластери (класи) країн за рівнем обмеження доступу до Інтернет-ресурсів, видаляти найбільш корельованих державами класи (на розглянутому прикладі, зокрема, Росія і Іран).

Змістовне пояснення обмеження доступу до соціальних мереж та інших Інтернет-ресурсів у кожному випадку ґрунтується на правових актах окремих країн.

З одного боку Інтернет-обмеження можуть сприйматися як показник слабкого рівня розвитку демократії в країнах, що її практикують. Вони можуть використовуватись з метою омани громадян й перешкоджання розвитку вільних ЗМІ, обмеженню вільного обміну думками. Але з іншого боку, Інтернет-обмеження можуть сприйматися як засіб захисту національної інформаційної системи в умовах інформаційної війни [8].

Урахування інформації щодо Інтернет-обмежень дозволяє підтримувати контакт між суб'єктами, які знаходяться у країнах з різним рівнем та різним змістом здійснення фільтрації. З цією метою необхідно бути проінформованим на предмет можливості вільного використання конкретних веб-ресурсів та способу подолання Інтернет-фільтрації.

| Label        | PageRank | Label        | Authority | Hub      |
|--------------|----------|--------------|-----------|----------|
| Китай        | 0.097906 | Китай        | 0.549275  | 0.0      |
| Іран         | 0.08911  | Іран         | 0.504343  | 0.0      |
| Туркменістан | 0.069321 | Пакистан     | 0.338742  | 0.0      |
| Росія        | 0.068442 | Туреччина    | 0.334866  | 0.0      |
| Пакистан     | 0.064044 | Туркменістан | 0.275962  | 0.0      |
| Україна      | 0.05305  | Єгипет       | 0.264705  | 0.0      |
| Туреччина    | 0.051731 | Саудівськ... | 0.183387  | 0.0      |
| Узбекистан   | 0.048653 | Росія        | 0.167325  | 0.0      |
| Єгипет       | 0.045135 | Узбекистан   | 0.073866  | 0.0      |
| Саудівськ... | 0.039858 | Україна      | 0.061206  | 0.0      |
| Facebook     | 0.031063 | Facebook     | 0.0       | 0.446615 |
| Youtube      | 0.031063 | Youtube      | 0.0       | 0.446615 |
| Twitter      | 0.031063 | Twitter      | 0.0       | 0.396074 |
| Instagram    | 0.031063 | Instagram    | 0.0       | 0.341728 |
| Telegram     | 0.031063 | Telegram     | 0.0       | 0.320219 |
| Whatsapp     | 0.031063 | Whatsapp     | 0.0       | 0.238977 |
| Viber        | 0.031063 | Viber        | 0.0       | 0.197484 |
| Wechat       | 0.031063 | Wechat       | 0.0       | 0.194558 |
| VK           | 0.031063 | VK           | 0.0       | 0.172771 |
| Skype        | 0.031063 | Skype        | 0.0       | 0.162291 |
| LinkedIn     | 0.031063 | LinkedIn     | 0.0       | 0.1379   |
| Однокласс... | 0.031063 | Однокласс... | 0.0       | 0.125338 |

а

б

Рис. 2. Ранжирування вузлів мережі за критеріями PageRank (а) і HITS (б)

### Використана література

1. Марущак А. Інформаційне право: доступ до інформації: навчальний посібник для студентів ВНЗ. Київ: КНТ, 2007. 425 с.
2. Богуш В., Юдін О. Інформаційна безпека держави. Київ: "МК-Прес", 2005. 225 с.
3. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)": Указ Президента України від 15.05.17 р. № 133/2017.

4. Ланде Д.В., Ліненко Ю.О. Обмеження доступу до Інтернету у світі: мережева модель : матеріали першої науково-практичної конференції *Інформаційне право: сучасні виклики і напрями розвитку*. м. Київ. 18 жовтня 2018 р.; упоряд. В.М. Фурашев, С.Ю. Петряєв. Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського”. Київ: Вид-во “Політехніка”. 2018. С. 50-54.
5. Cherven Ken. Network Graph Analysis and Visualization with Gephi. *Packt Publishing*. 2013. ISBN: 9781783280131.
6. Langville Amy N., Meyer Carl D. Google's PageRank and beyond: the science of search engine rankings. *Princeton university press*. 2011. ISBN: 9780691152660.
7. Kleinberg J.M. Authoritative Sources in a Hyperlinked Environment. *Proceedings of the ACM-SIAM Symposium on Discrete Algorithms*. 1998, and as IBM Research Report RJ 10076. May 1997.
8. Литвиненко О. Інформація і безпека. *Нова політика*. 1998. № 1. С. 46.

~~~~~ \* \* \* ~~~~~

УДК: 681.3, 314.1, 004.6

**БРАЙЧЕВСЬКИЙ С.М.,** кандидат фізико-математичних наук

## **ЗВОРОТНІ ЗВ'ЯЗКИ В СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ З ЕЛЕМЕНТАМИ ШТУЧНОГО ІНТЕЛЕКТУ**

**Анотація.** В роботі розглянуті динамічні ефекти, викликані наявністю зворотних зв'язків в системах Інтернету речей з елементами штучного інтелекту. Показано, що за певних умов система може переходити в нестійкий стан, який може характеризуватися її непередбаченою поведінкою.

**Ключеві слова:** інформаційні технології, Інтернет речей, штучний інтелект, зворотні зв'язки.

**Summary.** Dynamic effects caused by the presence of feedback in Internet of things systems with elements of artificial intelligence are considered in the paper. It is shown that under certain conditions a system can go into an unstable state that may be characterized by its unpredictable behavior.

**Keywords:** information technologies, Internet of things, artificial intelligence, feedback.

**Аннотация.** В работе рассмотрены динамические эффекты, вызванные наличием обратных связей в системах Интернета вещей с элементами искусственного интеллекта. Показано, что при определенных условиях система может переходить в неустойчивое состояние, которое может характеризоваться ее непредсказуемым поведением.

**Ключевые слова:** информационные технологии, Интернет вещей, искусственный интеллект, обратные связи.

**Постановка проблеми.** Швидкий розвиток сучасних інформаційних технологій породжує нові виклики і нові ризики, що потребують ретельного вивчення. До їх числа відносяться і проблеми правового регулювання, пов'язані з використанням Інтернету речей (далі – IoT) [1 – 6]. Вони пов'язані з наявністю (принаймні, гіпотетичною) в поведінці систем IoT елементів соціальної поведінки [2]. Оскільки питання про природу соціальних відносин між людиною та технологічною системою є досить нетривіальним, в пропонованій роботі ми не маємо наміру обговорювати його в повному обсязі.

Для нас важливо те, що сучасні технологічні системи можуть призводити до наслідків, що однозначно не впливають із їх будови та тих задач, які перед ними ставить людина. Через це людина не в змозі відповідати за них. Ці наслідки, по суті, відіграють таку ж роль, як і свідомі дії індивіда. Саме в такому розумінні ми говоримо про необхідність правового регулювання відносин людина – машина.

В попередній статті [7] ми розглянули один окремих випадок подібних ситуацій, пов'язаний з виникненням в системі резонансних явищ. В пропонованій роботі ми обговоримо більш загальні процеси, в основі яких лежать зворотні зв'язки, що можуть виникати в системах IoT.

Прості ефекти такого роду можемо спостерігати в досить широкому спектрі особливостей функціонування сучасних технологічних систем. Але значно суттєвішими вони, безперечно, можуть стати у випадку наявності в системі елементів штучного інтелекту (далі – AI) [8 – 15].

Ми покажемо, що за певних умов в таких системах IoT можуть виникати зворотні зв'язки, не передбачені їх проєктувальниками. Причиною їх появи можуть бути, наприклад,



механізми саморегуляції [15 – 17] системи, викликані створенням компонентами AI додаткових алгоритмів, не передбачених розробниками системи. Можливі й інші механізми, але загальний принцип лишається тим самим.

**Результати аналізу наукових публікацій.** Правове регулювання в галузі використання технологічних (в тому числі інформаційних) систем саме по собі не є чимось новим. Мається на увазі правове регулювання відносин між людьми, які здійснюються за допомогою технологічних систем або у зв'язку з їх використанням.

При цьому виділяють дві основні категорії проблем:

- особливості функціонування технологічних систем як причина виникнення особливостей у додатковому правовому регулюванні;
- забезпечення захисту від наслідків нештатного функціонування технологічних систем.

Тобто суб'єктом права в будь-якому випадку є людина, а технологічна система виступає лише в ролі знаряддя в її руках. Отже, в ситуаціях, коли функціонування системи призводило до негативних наслідків, вважалося, що відповідальність за її дії несуть розробники, виробники та експлуатаційники, тобто люди.

Але сьогодні (принаймні, теоретично) розглядаються ситуації, в яких відповідальність може бути покладена саме на машину, незалежно від участі людини [2; 3]. Такий погляд на технологічні системи є принципово новим, оскільки передбачає можливість того, що їх функціонування може мати соціальні наслідки, а отже, вони самі можуть розглядатися як суб'єкти суспільних відносин. Фактично, сказане означає, що за певних умов технологічна система набуває елементи суб'єктності. На перший погляд, це суперечить загальноприйнятим уявленням про сутність технологічних систем. Адже вважається, що машина лише виконує програму, закладену в неї людиною. І разом з тим, розвиток сучасних інформаційних технологій, зокрема Інтернету речей, свідчить, що такі ситуації можливі. Якщо не вдаватися до наукової фантастики, то мова, очевидно, йде не про повноцінну суб'єктність машини, а про наявність в її функціонуванні окремих рис, характерних для справжнього суб'єкта – людини.

Вважаємо, що в рамках обраної нами теми ключовим чинником є здатність машини самостійно приймати рішення. Підкреслимо, що йдеться не про імітацію прийняття рішення, що, взагалі кажучи, на наш час не є чимось особливим (прикладом може служити комп'ютер, що грає в шахи). Ми маємо на увазі здатність машини приймати рішення, яке однозначно не визначається алгоритмом, обраними значеннями його параметрів та структурою вхідних даних. Саме така поведінка машини дає підстави говорити про її відповідальність за власні дії, що є предметом правового регулювання. Ґрунтовний аналіз правових аспектів Інтернету речей можна знайти, наприклад, в [3].

Нагадаємо, що термін “Інтернет речей” на початку означав концепцію впровадження радіочастотних міток в систему керування логістичними ланцюжками [4; 5]. З часом під IoT почали розуміти концепцію обчислювальної мережі фізичних предметів (“речей”), оснащених вбудованими технологіями для їх взаємодії одне з одним або з оточуючим середовищем [6]. Головна ідея полягала в тому, що використання таких мереж дозволить (принаймні, частково) виключити участь людини. На наш час переважає розуміння IoT як сукупності технічних систем і комплексів, що взаємодіють між собою через мережу Інтернет [1; 3]. Вважається, що концепція IoT в практичній реалізації має як технологічні, так і соціальні наслідки [2].

Важливим аспектом створення та використання систем Інтернету речей є перспектива включення в них елементів штучного інтелекту.

Тема AI є надзвичайно поширеною в сучасній літературі. Але далеко не завжди границя між наукою та науковою фантастикою (бунт машин тощо) є достатньо чіткою. На жаль, далеко не все, що пишуть, має відношення до реальності. Можливо, багато з усього цього з часом, внаслідок подальшого розвитку технологій, буде втілено в дійсність. Але сьогодні, говорячи про інформаційні технології, слід обмежитися більш прозаїчними уявленнями.

Найбільш загальним визначенням цього поняття є, напевно, те, яке пропонує Вікіпедія [8]: штучний інтелект – це розділ комп'ютерної лінгвістики та інформатики, що опікується формалізацією проблем та завдань, які подібні до дій, які виконує людина.

Зауважимо принциповий момент, надзвичайно важливий для адекватного розуміння AI: ключовим є те, що штучний інтелект здатний до дій, подібних до тих, що виконує людина. Це означає, що для кваліфікації пристрою як системи AI не потрібно вимагати від нього (від її розробників) моделювання вищої нервової діяльності людини. Той самий ефект може досягатись цілком прозаїчними методами обчислювальної техніки.

Наведемо ще два способи розуміння AI, які будуть нам корисні в рамках даної роботи. Перше: штучний інтелект – це розробка агентів, які є гнучкими і здатні адаптуватися до різних ситуацій, які раніше не були відомі і не вивчалися через досвід, досягаючи мети.

Друге: штучний інтелект оцінюється загальною здатністю агента досягати мети в широкому діапазоні середовищ [13].

Для нас суттєво в першу чергу те, що елементи AI можуть використовуватися в системах IoT як базові в плані створення керуючих підсистем. З практичної точки зору, елементи AI в IoT мають сенс в першу чергу саме в плані систем керування. Причина полягає в тому, що сама природа систем Інтернету речей передбачає, що вони повинні самостійно приймати рішення. Інакше відмінність між системою IoT і холодильником матиме виключно кількісний характер. І можливість системи (що практично реалізується в процесі експлуатації) самостійно приймати рішення створює основу для постановки проблеми правових аспектів її функціонування.

Нижче ми проаналізуємо одну з таких можливостей, зумовлену наявністю в системах IoT з елементами AI зворотніх зв'язків.

**Метою статті** є визначення динамічних ефектів в поведінці систем Інтернету речей, які зумовлені наявністю в процесах обробки вхідних даних зворотніх зв'язків, породжених присутніми в них елементами штучного інтелекту.

**Виклад основного матеріалу.** Нижче ми проаналізуємо вплив зворотніх зв'язків в системах IoT з елементами AI.

На рівні технологічної реалізації IoT є набором датчиків, що фіксують задані параметри навколишнього середовища, та пристроїв, що обробляють вхідні дані, отримані від датчиків. Для нас суттєво, що обмін даними здійснюється за допомогою мережі Інтернет. Метою створення такої системи є виключення безпосередньої участі людини принаймні в частині функціональних можливостей системи. Це, в свою чергу означає, що система IoT повинна на основі обробки отриманих вхідних даних приймати рішення, результатом яких буде реальний вплив на оточуюче середовище. Зрозуміло, що в тих випадках, коли прийняті рішення неадекватні фактичній ситуації, наслідки роботи системи можуть бути вкрай негативними.

Важливим є питання про можливі причини виникнення таких ситуацій. У випадку звичайних систем IoT (тобто таких, що не містять елементів AI) стандартними вважаються чинники, що утворюють три групи:

- помилки алгоритмів програмного комплексу;

- помилкові вхідні дані;
- невідповідні значення параметрів роботи алгоритмів, які встановлюють експлуатаційники в процесі налаштування системи в конкретних умовах.

Якщо ж система містить елементи штучного інтелекту, до них додається ще група чинників, які ми обговоримо нижче.

В рамках нашого аналізу одним із ключових є поняття нелінійної системи. Стислий огляд цього питання стосовно нашої проблеми міститься в [7], тому не будемо повторювати основні положення. Нам потрібно лише розуміння того, що Інтернет речей є, взагалі кажучи, нелінійною системою. Принаймні, нелінійними є ті системи IoT, рівень складності яких дає підстави говорити про неї в контексті суспільних відносин.

Якщо система є лінійною, то незначні відхилення в кожній з груп ведуть до незначних відхилень в поведінці системи як такої. Отже, по-перше, при правильному налаштуванні не виникатиме позаштатних ситуацій, а, по-друге, якщо такі ситуації й виникатимуть, вони не матимуть помітних наслідків. Важливо те, що поведінка лінійної системи прогнозована. Дійсно, знаючи використовувані алгоритми та конкретні значення параметрів, ми можемо покроково пройти весь тракт системи і визначити критичні точки, в яких можуть виникати збої. Тому відповідальність за негативні наслідки функціонування системи лежить на проектувальниках, виробниках та експлуатаційниках.

Але можуть виникати інші ситуації, в яких поведінка системи стає непрогнозованою, і не існує способу визначити, коли і за рахунок чого відбувся збій. Єдине, що нам доступне – гіпотетично припустити можливість подібної поведінки. В таких випадках має сенс говорити про “відповідальність” машини.

Ця особливість систем IoT на рівні звичайних технологій розглядалася в [7] на прикладі окремого випадку ситуації, яка має ознаки параметричного резонансу. Ми бачили, що стандартна процедура циклічного опрацювання вхідних даних нелінійною системою може призводити до непрогнозованої поведінки. Але в таких ситуаціях можливо принаймні припустити, що саме здатна зробити система в тих чи інших умовах. Ми можемо побудувати набір можливих сценаріїв її поведінки, хоча й не знаємо, який із них матиме місце в процесі її експлуатації.

Стан справ докорінно міняється, якщо в системі присутній елемент штучного інтелекту. Тоді поведінка системи може стати непрогнозованою на зовсім іншому рівні, при чому відмінність є не лише кількісною, але й якісною. Причина полягає в тому, що компоненти з елементами AI створюються саме для того, щоб система була здатна приймати самостійні рішення. А такі рішення заздалегідь не відомі – в протилежному випадку дії машини цілком визначаються закладеними в неї алгоритмами, а отже, немає підстав говорити про штучний інтелект. Штучний інтелект потрібний для того, щоб хоча б частково виключити необхідність застосування інтелекту людини. А це означає, що система з AI може поводити себе інакше, ніж конкретна людина. Так саме, як дві різні людини в тих самих умовах приймають різні рішення. І тому кожна людина відповідає за власні рішення. В цьому плані границя між людиною і машиною справді стирається.

Сказане зовсім не означає, що машина здатна робити щось грандіозне і неймовірне (з нашої точки зору), щось таке, що може призвести до вселенської катастрофи. Дії можуть бути надзвичайно простими і буденними, але, разом з тим, і такими, що впливають на наше життя. Наприклад, машина може сама вирішувати, як змінювати температуру приміщення – нагрівати, чи охолоджувати. Якщо така система просто порівнює покази термодатчика з граничними значеннями, і залежно від результату вмикає нагріваючий або охолоджуючий пристрій, її поведінка в стандартних умовах визначається закладеною програмою. Ми знаємо, як система повинна діяти при заданій температурі.

У разі, коли вона діє не так, як передбачено, ми вважаємо, що має місце помилка, і шукаємо її. А знайшовши, виправляємо. Помилка може бути в механічній частині, в датчику, в програмному комплексі, та вона існує.

Але якщо між термодатчиком і пристроями зміни температури знаходиться програмний блок з елементами AI, ситуація докорінно змінюється. Тепер машина в певному розумінні сама вирішує, холодно в приміщенні чи жарко. І якщо її рішення не співпадає з нашим, це зовсім не обов'язково означатиме наявність помилки. Просто машина так вважає – адже ми її саме з цією метою і створили. Створюючи штучний інтелект, ми очікуємо від нього самостійної поведінки, і повинні розуміти, що ця поведінка може нам не сподобатися. Принциповим моментом є те, що в таких ситуаціях, взагалі кажучи, неможливо виправити машину. Вони діє правильно, в повній відповідності з задумом розробників. Так само, ми не можемо вважати помилковою поведінку людини, яка скаржиться, що їй холодно і просить вас закрити вікно, хоча вам жарко.

Існує багато причин для виникнення таких ситуацій. В даній роботі ми розглянемо одну групу причин, обумовлених наявністю в системі зворотних зв'язків.

Зворотні зв'язки є основою кібернетики та одним із ключових понять теорії систем [18; 20]. На загальному рівні зворотнім зв'язком називають вплив результатів деякого керованого процесу на його протікання. Повна теорія зворотних зв'язків досить складна і далеко виходить за межі нашої теми. Тому ми не будемо торкатися математичних питань, обмежившись лише загальними уявленнями.

В найпростішій реалізації зворотній зв'язок полягає в тому, що на вхід деякого пристрою подається сигнал, який є функцією його вихідного сигналу. Зворотні зв'язки можуть застосовуватись з різними цілями, але головне їх призначення полягає в забезпеченні можливості змінювати режим роботи пристрою залежно від змін вихідного сигналу. Відповідно існує два види зворотних зв'язків: додатні і від'ємні. Додатні зворотні зв'язки посилюють зміну вихідного сигналу, а від'ємні – змінюють вихідний сигнал так, щоб протидіяти його зміні.

Від'ємні зворотні зв'язки використовуються як стабілізуючі елементи системи, які забезпечують (наскільки це можливо) стабільність її роботи. Додатні зворотні зв'язки здебільшого використовують як генератори.

В будь-якому випадку, блок, в якому реалізовано зворотній зв'язок, в своїй структурі містить аналізатор вихідного сигналу. Залежно від результатів цього аналізу та заданої програми він приймає те чи інше рішення, яке впливає на величину вихідного сигналу. Якщо аналізатор фіксує зміну величини вихідного сигналу, він, залежно від поставленої задачі, або посилюється, або послаблюється. При чому пристрій може працювати в обох напрямках. Тобто, блок, що містить зворотні зв'язки, може не лише стабілізувати роботу системи, але й переводити її з одного режиму в інший. Тому зворотні зв'язки є основним інструментальним засобом автоматичного керування системами [21].

Наявність від'ємних зворотних зв'язків стабілізує стан системи і, за певних умов, підтримує її в гомеостатичному стані. Нагадаємо, що гомеостатом називають самоорганізовану систему, яка протягом необмеженого часу підтримує значення певного набору своїх параметрів в межах заданого інтервалу значень. Ідеальною реалізацією самокерованої системи є гомеостат. Слід також зазначити, що гомеостат підтримує сталими не всі свої параметри. Тому він може за потреби переходити з одного режиму в інший, а також еволюціонувати. Прикладом такої еволюції може служити процес самонавчання нейронних мереж [22].

У випадку наявності в системі додатних зворотних зв'язків робить ситуацію значно складнішою. Головна їх особливість полягає в тому, що вони пришвидшують реакцію системи на зміну вхідного сигналу. Але це може мати різні наслідки. Якщо додатні зворотні зв'язки не вбудовані в систему з певною метою, виникає тенденція до її переходу в нестійкий стан. Нагадаємо, що нестійким називають стан системи, який може змінюватися без зміни вхідного сигналу.

Саме можливість переходу системи в нестійкий стан є тим критичним моментом, який становить предмет пропонованої роботи. Перебування системи в нестійкому стані становить одну з головних загроз в плані використання її для потреб суспільства. Дійсно, зміна поведінки системи, що не залежить від зміни вхідного сигналу, може мати серйозні (в тому числі негативні) наслідки, які неможливо передбачити. Нестійкий стан системи в певному розумінні може моделювати властивість людини, яку філософи називають спонтанністю суб'єкта. Машина виявляється спроможною діяти несподівано і не прогнозовано, відповідно до власного "розуміння ситуації". Так само, як це може робити людина. Звичайно, механізми можуть бути різними, але з феноменологічної точки зору (тобто в плані спостереження за фактичними результатами функціонування системи) поведінка машини і людини стає подібною.

Зворотні зв'язки можуть міститись в різних компонентах системи. Основними є два варіанти:

- зворотні зв'язки в конструктивній частині;
- зворотні зв'язки в програмній частині.

В першому варіанті роль зворотних зв'язків більш чи менш контрольована, оскільки розробник має справу з технічними (матеріальними) засобами, які повністю доступні спостереженню

В другому варіанті функціонування зворотних зв'язків є менш очевидним. Дійсно, простежити роботу всіх блоків складного (і за обсягом, і за структурою) програмного комплексу і протестувати його в усіх можливих ситуаціях становить надзвичайно складну задачу. І ця обставина має для нас ключове значення.

Якщо додатні зворотні зв'язки закладені в структуру системи, імовірність її непрогнозованого переходу в нестійкий стан є достатньо мала. Перехід в нестійкий стан можливий, але ми, принаймні в загальних контурах, уявляємо собі як саме. Але ситуація докорінно змінюється за умови наявності в системі штучного інтелекту. Головна причина цього полягає в тому, такі системи в тій чи іншій формі передбачають процес самонавчання. Самонавчання системи спрямоване на забезпечення можливості самостійної (без участі людини) корекції нею характеру власного функціонування. Іншими словами, система сама вдосконалює себе, в тому числі і в плані прийняття рішень. Це, в свою чергу, означає, що система з елементами АІ самостійно змінює характер керування процесами, для контролю за якими вона створена.

Одним з найбільш критичних механізмів є розробка системою додаткових алгоритмів, не передбачених розробником. Вважається, що це покращує роботу системи. Але немає певності, що саме ці додаткові алгоритми можуть містити в собі непередбачені зворотні зв'язки, які можуть за певних умов переводити систему в нестійкий стан з усіма відповідними наслідками.

### **Висновки.**

Отже, ми бачимо, що за певних умов характер функціонування системи Інтернету речей з елементами штучного інтелекту може породжувати специфічні динамічні ефекти, зумовлені наявністю в ній зворотних зв'язків. Ці ефекти виникають за рахунок наявності додатних зворотних зв'язків, які зумовлюють перехід системи в нестійкий

стан. В такому стані система виявляється здатною до спонтанних дій, подібних до дій людини.

Таким чином, інформаційно-технологічні можливості системи IoT з елементами AI можуть зумовити її функціонування, що значною мірою моделює власну поведінку. Під власною поведінкою системи ми розуміємо здатність виконувати дії, які не визначаються однозначно її технологічними властивостями. Ця поведінка не впливає з алгоритмів, від початку закладених в систему при її розробці та створенні. Оскільки системи IoT безпосередньо впливають на перебіг подій в реальних ситуаціях, маємо підстави вважати описані вище явища такими, що містять в собі елемент суспільних відносин. Маємо на увазі, що функціонування технологічних систем в сучасному світі може виходити за рамки однозначного виконання команд людини, і, тим самим, стає елементом суспільних процесів.

Тому, враховуючи можливі негативні для суспільства наслідки, вона може сприйматися як суб'єкт соціальних відносин і підлягати правовому регулюванню. Наприклад, у випадку явної загрози для суспільства, така система може бути демонтована за рішенням суду.

### Використана література

1. Баранов А.А. Интернет вещей и искусственный интеллект: истоки проблемы правового регулирования: збірник матеріалів II-ї Міжнародної науково-практичної конференції *IT-право: проблеми та перспективи розвитку в Україні*, м. Львів, 17 лист. 2017 р. Львів: НУ "Львівська політехніка", 2017. 318 с. С. 18-42.
2. Рекомендации МСЭ-Т Y.2060 (06/2012). Серия Y: Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений. Сети последующих поколений – структура и функциональные модели архитектуры. Обзор Интернета вещей. URL: <http://handle.itu.int/11.1002/1000/11559>
3. Баранов О.А. "Интернет речей" як правовий термін. *Юридична Україна*. 2016. № 5 – 6. С. 96-103. URL: [http://www.irbis-nbuv.gov.ua/cgi-bin/irbis\\_nbuv/cgiirbis\\_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE\\_FILE\\_DOWNLOAD=1&Image\\_file\\_name=PDF/urykr\\_2016\\_5-6\\_16.pdf](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/urykr_2016_5-6_16.pdf)
4. Леонид Черняк. Платформа Интернета вещей (рус.). *Открытые системы. СУБД*. 2012. № 7. URL: <https://www.osp.ru/os/2012/07/13017643>
5. Kevin Ashton. That 'Internet of Things' Thing. In the real world, things matter more than ideas. (англ.). *RFID Journal* (22 June 2009). URL: <http://www.rfidjournal.com/articles/view?4986>
6. Internet Of Things (англ.). Gartner IT glossary. Gartner (5 May 2012). "The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment". URL: <https://www.gartner.com/it-glossary/internet-of-things/>
7. Брайчевський С.М. Резонансні явища в системах Інтернету речей. *Інформація і право*. № 1(28)/2019. С. 68-73. URL: <http://ippi.org.ua/braichevskii-sm-rezonansni-yavishcha-v-sistemakh-internetu-rechei-st-68-73>
8. Штучний інтелект. Вікіпедія. URL: [https://uk.wikipedia.org/wiki/%D0%A8%D1%82%D1%83%D1%87%D0%BD%D0%B8%D0%B9\\_%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82](https://uk.wikipedia.org/wiki/%D0%A8%D1%82%D1%83%D1%87%D0%BD%D0%B8%D0%B9_%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82)
9. Artificial intelligence. English Oxford Dictionaries. URL: [https://en.oxforddictionaries.com/definition/artificial\\_intelligence](https://en.oxforddictionaries.com/definition/artificial_intelligence)
10. Agnese Smith. Artificial intelligence. 2015. URL: <http://nationalmagazine.ca/Articles/Fall-Issue-2015/Artificial-intelligence.aspx>

11. Artificial Intelligence: A Rising Star of Mobile Technology. 05 Oct 2016. URL: [https://blog.intuz.com/artificial-intelligence-a-rising-star-of-mobile-technology/?utm\\_campaign=AI&utm\\_medium=Quora-ans&utm\\_source=Quora](https://blog.intuz.com/artificial-intelligence-a-rising-star-of-mobile-technology/?utm_campaign=AI&utm_medium=Quora-ans&utm_source=Quora)
12. João Paulo A. Lenardon. The regulation of artificial intelligence. Tilburg. Tilburg University. 2017. URL: <http://arno.uvt.nl/show.cgi?fid=142832>
13. Shane Legg and Marcus Hutter. A Formal Definition of Intelligence for Artificial Systems. URL: [http://www.vetta.org/documents/universal\\_intelligence\\_abstract\\_ai50.pdf](http://www.vetta.org/documents/universal_intelligence_abstract_ai50.pdf)
14. Nick Bostrom. How long before superintelligence? Oxford Future of Humanity Institute. University of Oxford. Originally published in Int. Jour. of Future Studies. 1998. Vol. 2. URL: <https://nickbostrom.com/superintelligence.html>
15. Николис Г., Пригожин И. Самоорганизация в неравновесных системах. Москва: Мир, 1979. 512 с.
16. Хакен Г. Синергетика. Иерархии неустойчивостей в самоорганизующихся системах и устройствах / пер. с англ. Москва, 1985.
17. Малинецкий Г.Г. Математические основы синергетики: хаос, структуры, вычислительный эксперимент. Москва: Либроком, 2009. 312 с.
18. Винер Н. Кибернетика, или Управление и связь в животном и машине. Москва: Наука. 1983. 344 с. URL: <http://grachev62.narod.ru/cybern/contents.htm>
19. Берталанфи Л. фон. Общая теория систем – обзор проблем и результатов. *Системные исследования. Ежегодник*. Москва: Наука, 1969. С. 30-54. URL: [http://grachev62.narod.ru/bertalanffy/bertalanffy\\_2.html](http://grachev62.narod.ru/bertalanffy/bertalanffy_2.html)
20. Боулдинг К. Общая теория систем – скелет науки. Москва: Наука, 1969
21. Бутковский А.Г. Теория оптимального управления системами с распределенными параметрами. Москва: Наука, 1965.
22. Горбань А.Н. Обучение нейронных сетей. Москва: СССР-США СП “Параграф”. 1990. 160 с. URL: <https://lib-bkm.ru/13814>

~~~~~ \* \* \* ~~~~~

УДК 004.8:342.733

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

## **ЮРИДИЧНА ОСВІТА ТА СФЕРА НАДАННЯ ПРАВОВИХ ПОСЛУГ В КОНТЕКСТІ ШТУЧНОГО ІНТЕЛЕКТУ**

**Анотація.** В статті розглядається вплив штучного інтелекту, визначальними властивостями якого є обізнаність про власну побудову та функціонування, здатність до самонавчання, самовдосконалення, саморозвитку, автономність від людини під час прийняття рішень тощо, на юридичну освіту та ринок надання послуг в галузі права. Звернено увагу на необхідність створення нових стандартів в сфері освіти та управління юридичним бізнесом, що обумовлене збільшенням доступу до великих обсягів інформації, швидким споживанням даних, але малим розвитком знань в окремих галузях. Наголошується на необхідності прагнути того, щоб кожний фахівець мав можливість розуміти зміст актуальних досягнень науки у будь-якій сфері незалежно від своєї професії або роду занять. Для цього необхідно надавати перевагу горизонтальній взаємодії, створювати умови для отримання нових культурних та фахових компетенцій, здійснити перехід від запам'ятовування до творчих рішень та комунікації, працювати над визначенням індивідуальної траєкторії та персоналізацією навчання, заохочувати інноваційність в освіті та сфері надання правових послуг.

**Ключові слова:** юридична освіта, правова допомога, інтелект, штучний інтелект, когнітивні властивості, сингулярність, Інтернет речей, віртуальне правосуддя, творчість, інноваційність.

**Summary.** The article examines the impact of artificial intelligence, the determining properties of which are awareness of its own construction and functioning, the ability to self-study, self-improvement, self-development, autonomy from a person when making decisions, etc., to legal education and the legal market of law services. The attention was paid to the urgency of creating new standards in the field of education and management of legal business due to increased access to large volumes of information, fast data consumption, but small development of knowledge in certain industries. The need is emphasized the need to strive for each specialist to be able to understand the content of the actual achievements of science in any field, regardless of their profession or occupation. To do this, it is necessary to give preference to horizontal interaction, to create conditions for obtaining new cultural and professional competencies, move from memorization to creative decisions and communication, work on identifying an individual trajectory and personalizing learning, promote innovation in education and in legal services.

**Keywords:** legal education, legal services, intelligence, artificial intelligence, cognitive properties, singularity, Internet of things, virtual justice, creativity, innovation.

**Аннотация.** В статье рассматривается влияние искусственного интеллекта, определяющими свойствами которого выступают осведомленность о собственном строении и функционировании, способность к самообучению, самосовершенствованию, саморазвитию, автономность от человека при принятии решений, на юридическое образование и рынок предоставления услуг в области права. Обращено внимание на необходимость создания новых стандартов в сфере образования и управления юридическим бизнесом, что обусловлено увеличением доступа к гораздо большим объемам информации, быстрым потреблением данных, но малым развитием знаний в отдельных отраслях. Подчеркивается необходимость стремиться к тому, чтобы каждый специалист имел возможность понимать содержание актуальных достижений науки в любой сфере независимо от своей профессии или рода



занятій. Для этого необходимо отдавать предпочтение горизонтальному взаимодействию, создавать условия для получения новых культурных и профессиональных компетенций, осуществить переход от запоминания к творческим решениям и коммуникации, работать над определением индивидуальной траектории и персонализации обучения, поощрять инновационность в образовании и сфере предоставления правовых услуг.

**Ключевые слова:** юридическое образование, правовая помощь, интеллект, искусственный интеллект, когнитивные свойства, сингулярность, Интернет вещей, виртуальное правосудие, творчество, инновации.

**Постановка проблеми.** Сьогодні обґрунтовано та закономірно підтримується прискорений розвиток штучного інтелекту, але лише фрагментарно можливо здогадуватися, як останній винахід людства, як його іменує Джеймс Баррат (James Barrat) – автор книги “Наш останній винахід: штучний інтелект і завершення ери людства” [32, с. 10], може надалі вплинути на звичайний уклад життя, економіку, політику та освіту. І вже як наслідок цього – на юриспруденцію та сферу надання правових послуг.

Подію з високим ступенем невизначеності змісту і подальшого перебігу, але з значною ймовірністю настання, Насім Талеб (Nassim Nicholas Taleb) іменує “чорним лебедем” [36, с. 9]. Останнім може виявитися штучний суперінтелект. Якщо об’єкт впливу такої події (людина, людство, компанія, галузь тощо) здатний ефективно їй протистояти та виходити з-під удару з позитивними змінами, то він розглядається як наділений ознакою антикрихкості (“Антикрихкість: речі, що стають кращими від безладу” [25, с. 3]) – спроможністю до позитивних змін після невдач, втрат, помилок та несподіваного впливу, а також здатністю розвиватися і ставати сильніше при зіткненні з хаосом. Втім, зазначена властивість є не тільки вродженою, але її можливо спрямовано набуті й розвинути, в тому числі відносно сфери юридичної освіти та діяльності з надання правових послуг.

Одна з можливостей досягнення ефективних змін полягає у виконанні вимоги інтеграції з науково-технічним прогресом таким чином, щоб кожний громадянин ЄС мав можливість розуміти зміст актуальних досягнень науки у будь-якій галузі незалежно від своєї професії або роду занять, про що зазначено у доповіді Science Education for Responsible Citizenship 2015 р. для Європейської Комісії експертів наукової освіти [23]. Вітчизняне суспільство, що прагне інтегрування з навколишнім розвинутим світом, має обрати зазначений вектор незалежно від набуття формальних ознак такої причетності.

**Результати аналізу наукових публікацій.** Проблемі становлення та розвитку юридичної освіти в Україні приділено значну увагу в роботах Д.С. Азарова, Д.О. Балабанової, В.С. Батиргарєєвої, Ю.В. Бауліна, В.С. Бігуна, О.І. Бойко, В.І. Борисова, Л.П. Брич, С.Д. Гусарєва, Н.О. Гуторової, І.М. Даньшина, Л.М. Демідової, О.О. Дудорова, З.А. Загинеї (Тростюк), В.В. Комарова, О.В. Михайленко, А.А. Музики, В.О. Навроцького, М.І. Панова, Ю.А. Пономаренко, В.Я. Тація, О.Д. Тихомирова, В.О. Тулякова, П.Л. Фріса, В.І. Шакуна, М.І. Хавронюка, В.Б. Харченко та багатьох інших.

Вагомі внески у дослідження правових питань щодо штучного інтелекту внесені О.А. Барановим, В.М. Брижко, А.А. Мельниченком, М.А. Ожеваном, В.Г. Пилипчуком, Є.О. Харитоновим, О.І. Харитоновою та іншими, послідовний розгляд ролі і місця штучного інтелекту в сфері правових відносин проводиться у дослідженнях М.В. Карчевського, В.А. Мисливого, Н.А. Савінової, Ю.В. Шеляженко та інших.

**Метою статті** є дослідження та визначення впливу з боку штучного інтелекту на сфери юридичної освіти та надання правових послуг, можливих напрямків та перспектив їх розвитку у плинному світі чергової технологічної революції.

**Виклад основного матеріалу.** Згідно з висновками Центру стратегічних та міжнародних досліджень (Center for Strategic & International Studies) у наш час паралельно розгортаються щонайменше сім революцій [22], які швидко та радикально змінюють кожна свою галузь та традиційну систему у цілому:

1) населення (з 7,5 мільярдів у 2017 р. воно зросте до 9,8 мільярдів у 2050 р.; середній вік зміниться з 46,9 у 1950 р. до 77,8 у 2050 р.; кількість мега міст з населенням більше 10 мільйонів збільшиться з 28 до 56 у 2035 р.) [30];

2) ресурсів (Міжнародна федерація діабету (The International Diabetes Federation) вважає, що до 2040 р. кількість діабетиків буде становити 642 мільйони людей, що є більшим, ніж кількість тих, хто сьогодні потерпає від голоду; відповідно до прогнозу Інституту світових ресурсів (World Resources Institute) до 2040 р. 33 країни відчують надзвичайно високий стрес через брак води, серед них Китай, Індія та США; незважаючи на досягнення відновлюваних джерел енергії Міністерство енергетики США (U.S. Department of Energy) очікує, що споживання викопного палива зменшиться з 82% до 78% світового виробництва енергії до 2040 р.; Міжурядова група з питань зміни клімату (The Inter-governmental Panel on Climate Change) вважає, що невдовзі відбудеться глобальна зміна клімату не менш як на 2 градуси Цельсія, що призведе до значного впливу на людське суспільство) [19];

3) технологій (виникаючі тенденції можуть змінити взаємодію людини і комп'ютера у такий спосіб, який ми не можемо собі уявити; досягнення в сфері робототехніки змінюють уявлення про людську працю; прориви у галузі біотехнології дозволять у найближчий час створити замінні органи, які збільшать тривалість життя – втручання в організм людини на клітковому та атомарному рівнях, гібридні нанороботи на основі синтетичних білків, імплантація реконструйованих ДНК, отримання зі стовбурових клітин жирової тканини клітин печінки [31]; вирощування органів на замовлення, кохлеарні імплантати для відновлення слуху та виведення його на новий рівень, нейроінтерфейс iBrain для контролю дрібної моторики, який тестував на собі Стівен Хокінг, заміна ампутованих кінцівок людини технологічними протезами, зокрема, штучною рукою i-LIMB Pulse або здатним до самонавчання колінним протезом з штучним інтелектом RheoKnee компанії Ossur, протез Retina Implant сітківки ока у вигляді мікročіпу, штучне серце Total Artificial Heart, 3D-друк органів тощо; однією з галузей техніки, яка може призвести до найбільших змін у найближчі десятиліття, є трансформація обчислювальної техніки та штучного інтелекту [7]; на думку Ілона Маска (Elon Musk) [8] та Мері Камінгс (Mary Cummings) з Університету Дюка (Duke University) дуже скоро роботи будуть робити все краще за людей);

4) інформації (конструюються нові виміри навколишнього світу; віртуальні об'єкти поєднуються або стають сумісними з матеріальними об'єктами; у наступні три роки глобальне формування даних збільшиться втричі, що зможе надати штучному інтелекту можливості для вивчення та застосування до більш широкого кола людської діяльності; до 2020 р. очікується поява близько 9,2 мільярдів телефонів з підтримкою Інтернету, 500 мільйонів нових користувачів [26], значно зростуть способи, якими люди взаємодіють та навчаються в Інтернеті, повсюдність інформації призводить до швидкого споживання даних, але до малого розвитку знань, ключовим викликом буде керування потоком даних та визначення шляхів послідовного залучення нових знань [27]);

5) економіки (ланцюги постачання майже для всіх продуктів є глобальними; на економічному ландшафті з'являються нові гравці – Китай, Індія, Бразилія, Мексика, Південна Африка і Нігерія, які вступають у глобальну систему, впливають і змінюють її; впровадження більшої автоматизації (або штучного інтелекту) до робочих процесів може змінити природу не тільки міжнародної торгівлі, але й внутрішніх ринків праці; починаючи з фінансової кризи 2008 р. борг став проблемою світової економіки);

6) безпеки (внаслідок появи технологій ХХІ століття, від комунікації до боєприпасів, витрати на порушення безпеки стають дедалі дешевшими, їх стає легше знайти та легше використовувати; структурам, що призначені для управління проблемами ХХ століття, важко впоратися з технологіями ХХІ століття, які просуються швидше, ніж пристосовуються системи управління цими проблемами; час, який потрібно для перенесення хвороби з однієї області в іншу, зменшився на порядок з тих пір, як 1918 р. спалахнув іспанський грип, що знищив від 50 до 100 мільйонів людей за один сезон; якщо подібна транснаціональна загроза виникне в епоху, коли поїздка до найвіддаленіших куточків світу займає менше доби, потенційні наслідки будуть ще більшими; як країни або компанії можуть захиститися від атак, коли навіть одяг або слухові апарати можуть бути використані для збору інформації або запуску негативного сценарію, наш взаємопов'язаний світ створює великі можливості для індивідуального зростання, але піддає ризику новими формами вразливості) [9];

7) управління (приблизно 100 років тому ідентичність людини визначалася містом, в якому вона народилася, або її родиною та сусідством у великих громадах; особистість завтрашнього дня може бути заснована на Інтернет-чатах, які людина вважає найбільш привабливими для себе, або групами в Інтернеті, до яких бажано приєднатися у фізичному світі; чи то з лівого, чи з правого боку політичного спектра, популісти прагнуть використовувати ідентичність групи (наприклад, іммігрантів або біженців), яку нібито позбавляє чогось її антагоністська група (наприклад, потужні міжнародні корпорації), намагаючись позбавити антагоністську групу економічної або політичної влади і передати цю владу неможливій групі, популісти забезпечують їх підтримку, принаймні в короткостроковій перспективі; тенденцією для спостереження у найближчі роки стане позиція суверенних держав відносно внутрішніх або міжнародних організацій громадянського суспільства, окремі з яких мають більші бюджети, ніж урядові міністерства, які відповідають за той самий сектор) [18].

Розвиток фахової юридичної освіти та загальних клієнтських вимог суттєво впливає на ринок надання правових послуг: надалі все більш по-новому буде визначатися, що саме пропонується клієнту в зазначених сферах, з одного боку, скільки і чим (грошовими коштами, матеріальними ресурсами, власним часом) погоджуватимуться за це сплатити, з іншого.

На цей процес суттєво впливає поява штучного інтелекту найвищого ступеню розвитку. Останнім є штучний суперінтелект (Artificial Superintelligence, ASI) [3], який на відміну від своїх попередників (першим з яких є “слабкий штучний інтелект” (Weak Artificial Intelligence, WAI) [24], “вузький штучний інтелект”, або “обмежений штучний інтелект” (Artificial Narrow Intelligence, ANI) [15], або “прикладний штучний інтелект” (Applied Artificial Intelligence, AAI) [28] – орієнтований на виконання одного завдання або здійснення однієї функції (розпізнання мови, гра в шахи, пошук та аналіз інформації у певному напрямку тощо, а другим – “сильний штучний інтелект” (Strong Artificial Intelligence, SAI) [10], або “загальний штучний інтелект” (Artificial General Intelligence, AGI) – орієнтований на вирішення всіх завдань, які можуть постати перед людиною, та здійснення всіх когнітивних функцій) є більш розумним та потужним, ніж інтелект

людини практично в кожній області, включаючи наукову творчість, загальну мудрість, фаховий рівень і соціальні навички, а крім того може мати власну свідомість та суб'єктивні переживання.

Одна з фундаментальних проблем полягає у тому, що на сьогодні відсутнє чітке розуміння інтелекту людини. Тест Айзенка (IQ-тест), шкала Біне-Сімона та інші методи вимірювання містять значну кількість істотних помилок та некоректних формулювань. Між тим, виявлено, що мозок людини являє собою значну кількість вузькоспеціалізованих інтелектів, які з більшим або меншим успіхом забезпечують існування, виживання та співжиття у соціумі. З іншого боку, розрізнені вузькі штучні інтелекти невдовзі можуть з'єднатися у супер мережу, в тому числі завдяки Всеосяжному Інтернету (Internet of Everything, IoE, або Інтернету речей – Internet of Things, IoT). Сумна іронія може полягати у тому, що цілком реальною є небезпека не помітити розвиток такої сингулярності: спочатку людству допомагав дружній і підконтрольний слабкий штучний інтелект, та враз мозок кожної людини став поєднаним з глобальним суперштучним інтелектом в загальній неокортексній хмарі та став підконтрольним останньому.

Частіше за все інтелект людини описують як сукупність здатності до пізнання оточуючого світу, логічного мислення, а також можливості оперувати в рамках знакової системи та самостійно приймати рішення. Але такі властивості притаманні й штучному інтелекту. Так, за ним визнають наступні важливі когнітивні функції: 1) сприйняття, розпізнавання та класифікація будь-яких сигналів оточуючого світу (в тому числі тих, які не сприймає людина), а також інформації у будь-якому вигляді, наявності пам'яті без прогалин (в той час як мозок людини не зберігає цілісні спогади, кожного разу пригадування відтворюється наново, тому все, що ми пам'ятаємо, ми пам'ятаємо по-різному), обмін, аналіз, зіставлення, оцінювання певних даних, об'єктивна їх інтерпретація; 2) узагальнення і використання інформації для вирішення завдань або прийняття рішень, обробка значних обсягів інформації; 3) об'єктивна, неупереджена оцінка ситуації; 4) вибір стратегії і тактики найбільш оптимальної форми поведінки, завчасне планування та ситуативна переорієнтація; 5) генерування нових знань; 6) здатність самостійно формувати мету свого функціонування, динамічно змінювати зміст мети (цілей) внаслідок зміни внутрішніх та(або) зовнішніх обставин (напр., внаслідок обмеження доступу до необхідних обчислювальних, енергетичних, сировинних, фінансових та інших ресурсів, зміни оточуючого середовища, відмови людини від співпраці тощо); 7) повна обізнаність у принципах своєї побудови і роботи; 8) самонавчання, саморозвиток, самоперебудова, самовдосконалення (перша версія відшукує помилки всередині себе, виправляє їх, утворює вдосконалену версію самої себе і так переписує саму себе до нескінченності), тобто здатність вийти за межі своєї початкової програми; 9) прискорена швидкість прийняття рішення (секунди та мілісекунди); 10) накопичування досвіду, узагальнення, відшукування неочевидних зв'язків та будування логічних ланцюжків; 11) концентрація уваги; 12) побудова ціннісних суджень; 13) самостійність прийняття рішень і самостійне їх виконання, автономність від людини; 14) адаптація – здатність пристосуватися до мінливих вимог оточуючого світу (акомодація) та відтворювати під час пізнавальної активності окремі характеристики об'єкта пізнання (асиміляція); 15) творчість, тобто відкриття нових аспектів знання та перетворення оточуючого світу (вже сьогодні штучний інтелект пише музику, яку неможливо відрізнити від створеної людиною [1], диригує оркестром, малює картини (зокрема, створене алгоритмом машинного навчання Generative Adversarial Networks на базі штучного інтелекту полотно “Портрет Едмонда де Беламі”

(Portrait of Edmond Belamy) було продане на аукціоні Christie's за 432 тис. доларів США [11]), публікує статті в засобах масової інформації [16]); 16) наявність самоорганізації тощо.

Твердження “людина – найвища ланка еволюції і іншої бути не може” спирається на подібне йому “тільки людина має душу” (хоча з виявленням та аналізом останньої теж виникають проблеми). Але правда полягає у тому, що технологічний світ і не намагається відтворити будь-чию душу, втім відтворити інтелект є завданням цілком досяжним.

Для цього не потрібно йти шляхом копіювання (так само, як перші ентузіасти повітроплавання копіювали польот птахів за допомогою штучних крил), але необхідно розпізнати сутність функцій мозку людини (сприймати внутрішні або зовнішні сигнали як подразники, ідентифікувати їх та відповідати певними реакціями на них) та відтворити їх у штучній системі.

На початку проектування безпілотних транспортних засобів теж рушили шляхом легендарного Ікара (грец. Ἴκαρος) з давньогрецької міфології: компанія Google планувала створити робота-водія, схожого на людину. Надалі виявилось, що людина занадто неефективно розв'язує завдання законослухняно та безпечно дістатися певного місця. З'ясувалося, що достатньо надати штучному інтелекту всю інформацію (з карт місцевості, камер спостереження, контролерів транспортного засобу, всіх світлофорів навкруги тощо), тож він її зіставить між собою і на підставі обробки Big Data прийме найбільш ефективне рішення, але зовсім не так, як людина, яка не має можливості враховувати всі обставини (наприклад, зустрічні і паралельні світлофори та щільність руху на всіх перехрестях). Сьогодні автомобільний автопілот Waymo компанії Google є системним штучним інтелектом, який об'єднує значну кількість окремих прикладних штучних інтелектів, зокрема Google Street View (інтелектуальні об'ємні дорожні карти) та LIDAR (Light Identification, Detection and Ranging – технологію отримання та обробки інформації про віддалені об'єкти за допомогою активних оптичних систем, що використовують явища відбиття світла і його розсіювання в прозорих і напівпрозорих середовищах).

Схожа ситуація мала місце з перекладачем Google Translate, якого спочатку намагалися навчити різним мовам, але потім завантажили у його нейронні мережі текстові бази даних ООН, ЄС та з інших джерел. Виявилось, що штучному інтелекту не потрібно знати мови так, як їх знає людина. У величезних масивах даних він знаходить одному йому зрозумілі закономірності та вдало розв'язує поставлене завдання точного перекладу.

До того ж відсутність душі не завадила юридичній особі, яку у західній правовій доктрині з легкої руки Отто фон Гірке прийнято іменувати корпорацією [37, с. 23], стати повноцінним суб'єктом правовідносин, тобто бути здатною набувати права та виконувати певні обов'язки (ще на Ліонському соборі 1245 р. Папа Римський Інокентій IV здійснив класифікацію персон на фізичних осіб, що мають душу, і юридичних осіб, які не мають ні душі, ні совісті, ні волі, ні свідомості, і тому не здатні грішити і здійснювати покаєння [33, с. 97, 152, 209-215]). Створення юридичної особи було геніальним винаходом людської думки: сутність, яка була утворена лише у колективній уяві і за колективною домовленістю, у подальшому матеріалізувалася через певні прояви та окремі маніфестації. Віртуальне утворення, яке ніхто ніколи не бачив і про існування якого ми дізнаємося або з документів, або завдяки діям уповноважених представників, було прийнято у правові стосунки, йому надали певний обсяг прав та визнали за ним можливість виконувати обов'язки.

Тому є цілком обґрунтованими та логічними пропозиції надати статус суб'єкта правовідносин штучному інтелекту, які знайшли свою нормативну реалізацію у Резолюції Європейського Парламенту від 16 лютого 2017 р. (European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) [12] та у поданому на розгляд Конгресу США законопроекті "Fundamentally Understanding The Usability and Realistic Evolution of Artificial Intelligence Act of 2017" (or the "Future of Artificial Intelligence Act of 2017" (Акт про майбутнє штучного інтелекту) [2].

Здатність до самонавчання, самовдосконалення та саморозвитку, а також автономності від людини під час прийняття юридично значущих рішень є стрижнем всієї архітектури штучного інтелекту. Ця ідея була покладена в його основу ще Аланом М. Тьюрінгом (Alan Mathison Turing), автором однойменного емпіричного тесту для оцінки штучного інтелекту та інших значних винаходів (розробка теоретичної бази для машини Bombe, яка використовувалася у Другій Світовій Війні для зламу германського шифратора Enigma, проект першого комп'ютера з програмою, що зберігається у його пам'яті тощо).

Під час роздумів людина може утримувати у своїй свідомості не більш семи або дев'яти об'єктів та враховувати не більше трьох або чотирьох параметрів для висновків. Це виглядає дуже примітивно у порівнянні з алгоритмами, які оперують необмеженою їх кількістю. Тому розглядати штучний інтелект з антропоморфної точки зору є безпідставним.

Не є дивним, що за оцінкою MIT Technology Review, вже сьогодні 22 % всієї діяльності адвоката та 35 % діяльності юридичного клерка може бути повністю автоматизовано [29]. Якщо ефективність може збільшитися на 22 – 35 %, то це означає, що менша кількість юристів може обслуговувати більшу кількість клієнтів, менша кількість працівників може виконувати більші обсяги завдань.

Поява штучного інтелекту має полегшити людині вирішення численних складних задач, але насправді слід бути готовим до того, що він поступово витісняє людину у багатьох важливих напрямках. Адже йдеться не тільки про цифровізацію (або діджиталізацію, від англ. digitalization – перехід на цифрові технології, перетворення будь-якої інформації або інформаційних процесів у цифровий формат), а про вмирання або істотну зміну одних професій та появу інших.

Так, компанія JPMorgan на початку 2017 р. повідомила про використання програмного забезпечення Contract Intelligence, яке за декілька секунд здатне здійснити аналіз юридичних документів, що раніше вимагало 360 тис. годин робочого часу. Юридична фірма Baker & Hostetler оголосила, що приймає на роботу штучний інтелект ROSS для ведення справ про банкрутство, чим раніше опікувалися майже п'ятдесят юристів. Штучний інтелект ROSS, розроблений на когнітивному комп'ютері Watson компанії IBM, цілодобово слідкуватиме за законодавством і правовою ситуацією, вміє читати і розуміти мову, висувати гіпотези, досліджувати, а потім генерувати відповіді з належними посиланнями та цитатами, навчається зі свого власного досвіду тощо. Вчені з Університетського коледжу Лондона і Університету Шеффілда створили "комп'ютерного суддю", який передбачає рішення Європейського суду з прав людини з точністю до 79 % [20].

У змаганнях між юристами лондонських фірм зі штучним інтелектом Case Cruncher Alpha у розв'язанні справ про виплату страхових відшкодувань переміг останній: за наслідками розгляду кейсів було складено 775 прогнозів з загальною перемогою на боці

штучного інтелекту (точність прогнозу Case Cruncher Alpha – 86,6 %, практикуючих юристів – 66,3 %) [21].

На штучний інтелект покладають надії в тому, щоб допомогти змінити судову практику на краще: виявляти типові правові ситуації, розробляти алгоритми дій (напр., визначитись з гарантійним строком або строком давності, встановити різновид порушення права, обрати спосіб захисту тощо), зіставляти зі зразком (судовий прецедент, зокрема, ЄСПЛ або Конституційного суду України), абстрагуватися від обставин, фактів, документів, речей та інших доказів, які не мають відношення до предмету розгляду, не охоплюються предметом спору або не відбивають обраний позивачем спосіб захисту, або не передбачені відповідною нормою матеріального права, на яку посилається позивач, виявляти нетипову поведінку суду за звичайних умов, так звані “аномальні” судові рішення, обробляти значний обсяг інформації, готувати проект судового рішення тощо.

Робот-юрист вже допомагає оскаржувати штрафи за паркування: чат-бот-адвокат на ім'я DoNotPay, розроблений студентом Стенфордського університету Джошем Браудером, менш ніж за два роки роботи допоміг користувачам виграти 160 тисяч справ по штрафах за паркування. Всього за цей період робот-юрист допоміг підготувати близько 250 тис. апеляцій. В даний час безкоштовно скористатися його послугами можуть тільки жителі Лондона та Нью-Йорка. Але найближчим часом розробник планує запустити “колегу” DoNotPay для користувачів з Сієтла, розширити обсяг знань чат-бота іншими галузями юриспруденції.

Штучний інтелект перевершив людину у здібності до читання та розуміння тексту: результати людини в відповідному тесті складають 82.304, штучного інтелекту компанії Alibaba – 82.440, а Microsoft – 82.650, повідомляє видання Bloomberg [14].

Але з іншого боку штучний інтелект може виявитися хоча й досконалим, проте занадто незрозумілим людині. В останньому випадку або треба ретельно перевіряти кожне його рішення, якщо це можливо, або повністю довіритися йому, що теж є вкрай небезпечним та впритул наближає до панування Великого брата (Big Brother) з роману Джорджа Оруела “1984”. Так, за інформацією South China Morning Post [5], програма по відшукуванню корупціонерів Zero Trust на базі штучного інтелекту працювала з 2012 р. у 30 адміністративних округах КНР та виявила факти участі 8,7 тис. держслужбовців у розтратах, зловживанні владою або державними коштами, а також у кумівстві. Для виконання свого завдання вона мала доступ до більш ніж 150 захищених баз даних центральних і місцевих органів влади, в тому числі знімків зі супутника. Такий масив інформації дозволяв складати багаторівневі карти соціальних стосунків чиновників, їхніх родин та друзів, що стало корисним для виявлення підозрілих передач власності, будівництва інфраструктури, придбання землі та знесення будинків. Втім, важливим недоліком стала непрозорість ланцюжка, який вивів її до того чи іншого висновку.

У змаганнях між автоматизованою юридичною платформою LawGeex, яка за допомогою штучного інтелекту аналізує зміст договору, та 20 досвідченими американськими юристами люди знов програли алгоритму: точність роботи юристів склала у середньому 85 %, в той час як комп'ютер виконав завдання з ефективністю у 94 % і витратив на це 26 секунд проти 92 хвилин, що знадобилися людям [6].

На Першій міжнародній конференції з онлайн-судочинства, що проходила у Лондоні 3 – 4 грудня 2018 р., було представлено декілька пілотних проектів з розгляду кримінальних і цивільних справ практично повністю в віртуальному режимі [35]:

- Сінгапур продемонстрував національну електронну систему кримінального правосуддя ICMS (Integrated Case Management & Filing System). Вона заснована на

безпаперовій технології з моменту виявлення злочину до слухань в суді. Слідчий може в будь-який момент додавати матеріали у віртуальну кримінальну справу, адвокат і фігурант знайомитися з ними з урахуванням рівня допуску. Для ідентифікації сторони використовують національний ID Singpass з посиленням цифровим підписом. Файли кримінальної справи зберігаються в спеціальній хмарі, куди мають доступ прокуратура і суд. Передбачені місцевим законодавством судові документи у вигляді ордеру на арешт і ордеру на попереднє взяття під варту генеруються системою в автоматичному режимі без участі судді. Попередні слухання проводяться в режимі відеоконференції. З цього року законодавчо дозволено оформляти визнання провини, зроблене під час відеотрансляції. Всі судові рішення розсилаються в відомства, в тому числі до пенітенціарної установи, в електронному вигляді.

- Велика Британія відзвітувала про дистанційне цивільне судочинство. Так, послугами оновленого сервісу стягнення боргів до 10 тисяч фунтов з весни цього року скористалися 35 000 осіб. Більше 90 % позивачів позитивно оцінили інтуїтивно зрозумілий інтерфейс, який розробляли спеціально для громадян, що не розуміються в юридичних термінах, а також оплату мита онлайн. Стандартна “паперова” процедура подачі позову займала 15 днів, за допомогою сервісу він реєструється миттєво. Схожі цифри задоволеності користувачів показали і он-лайн-сервіси з оформлення заповіту і процедури розлучення, які також стартували в Сполученому королівстві в цьому році. Згідно зі статистикою, тепер 63% всіх заяв на розлучення британці подають по Інтернету.

- Канада представила повністю віртуальний трибунал з цивільних спорів, який працює в Британській Колумбії з червня 2017 року і розглядає позови за сумами менше 5 тис. доларів США. Інтерфейс он-лайн-суду зроблений з розрахунком на сприйняття 12-річного підлітка і оптимізований для смартфонів. Сам процес подачі та розгляду позову поділяється на кілька етапів. Користувачеві спочатку пропонують через спеціальний опитувальник “діагностувати” проблему, потім дають можливість врегулювати її в досудовому порядку, а вже потім позов надходить на розгляд членів трибуналу, які завдяки такій процедурі розглядають тільки 6 % усіх позовів.

За прогнозами консалтингової фірми Cognizant через 10 – 15 років роботи під керуванням штучного інтелекту відберуть 12 % робочих місць у жителів США, але з'являться такі нові професії, як детектив з роботи з даними (Data Detective), міський кібераналітик (Cyber City Analyst), проектувальник подорожей у доданій реальності (Augmented Reality Journey Builder), менеджер з розвитку бізнесу штучного інтелекту (Artificial Intelligence Business Development Manager), медичний технік з роботи зі штучним інтелектом (AI-Assisted Healthcare Technician), персональний брокер з роботи з даними (Personal Data Broker), диспетчер магістралей (Highway Controller), фахівець з генетичного розмаїття (Genetic Diversity Officer), IT-координатор (IT Facilitator), персональний куратор спогадів (Personal Memory Curator), директор з генетичного портфелю (Genomic Portfolio Director), командний менеджер з роботи людини та машини (Man-Machine Teaming Manager), фахівець з довіри (Chief Trust Officer), аналітик квантового машинного навчання (Quantum Machine Learning Analyst), майстер периферійних обчислювань (Master of Edge Computing) тощо [4], а також IT-медик, біоетик, розробник кіберпротезів та імплантів, оператор медичних роботів, проектувальник 3D-друку, дистанційний координатор безпеки, проектувальник особистої безпеки, проектувальник інтерфейсів безпілотних транспортних засобів, куратор колективної творчості, розробник освітніх траєкторій, координатор освітньої онлайн-платформи, бренд-менеджер просторів, режисер індивідуальних просторів,



дизайнер емоцій, віртуальний адвокат тощо. Разом з цим прогнозується зникнення таких професій як бухгалтер, аудитор, коректор, бібліотекар, діловод, архіваріус, турагент, каскадер, нотаріус, банківський операціоніст, ріелтер, аналітик, екскурсовод, перекладач, провізор, оператор call-центру, листоноша, охоронець, шахтар, кравець, офіціант тощо.

Слід готуватися до того, що складно буде не тільки випускникам юридичних ВУЗів, адже правники будуть конкурувати не тільки між собою, як це було і є зазвичай, але й з технологіями.

Як зазначає Тодд Соломон, партнер юридичної фірми McDermott Will & Emery, на місці батьків студента-юриста вже треба почати турбуватися, адже у молодих юристів сьогодні стало менше можливостей для навчання через штучний інтелект.

Освіта майбутніх юристів традиційно спирається на виконання рутинних завдань, для яких дуже скоро вже не знадобиться людина. Тому завдяки широкому впровадженню штучного інтелекту існуючий дисбаланс між щорічною кількістю випускників юридичних факультетів або університетів та позицією юристів початкового рівня буде збільшуватися зі зростаючою прогресією.

Юридичні школи помічають таку тенденцію та починають пристосовуватися: розробляються та запроваджуються навчальні програми для підготовки юристів до роботи з штучним інтелектом. Наприклад, Гарвардський університет пропонує курси з юридичних інновацій та програмування для юристів.

Як виявилось, програмування по своїй суті не відрізняється від основних принципів роботи юриста, тому його опанування не є чимось недосяжним для правників (або так званих “гуманітаріїв”). ІТ-фахівці та юристи засвоюють певні зразки (коди в одному випадку та юридичні формули в іншому), можливість їх аналізувати, систематизувати та інтегрувати складає левову частку професії.

Слід враховувати і той факт, що збільшується частка самотніх людей, яка за останніми даними ООН сягнула 64 %, а так само кількість неповних сімей [17]. У зв’язку з цим не вдається транслювати наступному поколінню свій родинний досвід. Оскільки модель передачі родинного досвіду істотно впливає на модель освіти, відсутність цього впливу повинна бути врахована. Школа поряд з родиною перестала бути єдиним майданчиком надання освіти, так само як вищий навчальний заклад вже не вважається обов’язковим атрибутом успішної кар’єри – Google та Ernest & Young оголосили, що диплом вишу не буде враховуватися під час найму на роботу.

Невтішні прогнози вказують доволі близькі дати вичерпання ресурсів планети (питна вода, нафта, газ, олово, вугілля тощо). У зв’язку з цим поряд з новітніми технологіями надія покладається на оновлений людський капітал. Під останнім розуміється не просто робоча сила, представникам якої в індустріальну епоху достатньо було мати навички рахування, читання та правопису, а в юриспруденції та ІТ-галузі – накопичувати зразки у вигляді формул (наприклад, юридична формула складу злочину крадіжки або договору купівлі-продажу) чи кодів програмування, але завтра вони всі будуть замінені більш ефективною робототехнікою і у випадку ігнорування необхідності перекваліфікації залишаться на узбіччі у прямому та непрямому сенсі цього явища.

Можливість доступу до великих обсягів інформації сьогодні створює нові стандарти в сфері освіти та управління юридичним бізнесом: в основу остаточного рішення вже не може покладатися тільки досвід та інтуїція керівника навчального закладу або партнера правничої фірми.

Освіта ще більше розглядається у якості інструменту для конкуренції. Розвинуті юрисдикції збільшують свій дохід за рахунок експорту освіти.

Необхідно також звернути увагу на той факт, що сформувалася та достатньо яскраво проявляє себе тенденція розшарування між тими, хто є активними учасниками цифрового суспільства, та тими, хто відмовляється або нездатний прийняти його існування.

Одночасно з цим з'являються нові суб'єкти освіти та(або) надання юридичної допомоги – обдарована молодь [34, с. 6]. Її представники бажають вчитися і досягають у навчанні значних успіхів, навчання приносить їм задоволення, вміють критично оцінювати навколишнє середовище і прагнуть проникнути в суть речей і явищ, задають багато питань і зацікавлені у відповідях на них.

Застарілі підходи до оцінювання результатів навчання або надання послуг стримують творчість колективу як організму або окремих його представників. Необхідність постійно переглядати цілі, завдання та напрямки розвитку створює ситуацію постійно зростаючого стресу та важко прогнозованими кінцеві результати всієї діяльності.

Від студентів та співробітників юридичних фірм або адвокатських об'єднань вимагаються нові навички та компетенції, зокрема, критичність мислення, здатність до командної роботи, взаємодії та комунікації, пріоритет м'яких зв'язків, мережева взаємодія, управління талантами, творчий підхід до своєї справи, поступовий відхід від конвеєрної праці (так званий офісний планктон) та накопичення величезного обсягу знань, здатність продукувати нові ідеї (креативність мислення), пошук альтернативних рішень, уміння ефективно проводити наукові дослідження, уміння працювати в міждисциплінарній галузі, встановлювати системні зв'язки, уміння обробляти значні обсяги інформації і критично-конструктивно її оцінювати, навички роботи в комп'ютерних мережах та використання програмних засобів, уміння виявляти й використовувати джерела інформації, здатність формулювати особисту думку та доказово її представляти, безперервна самоосвіта та самовдосконалення, знання особливостей та вміння запроваджувати стартапи у правовій сфері, уміння інтерпретувати юридичну діяльність і соціально-правовий досвід як основні компоненти змісту юридичної практики, знання механізму вирішення юридичних колізій з питань теорії і практики, знання юридичної техніки та її прикладних аспектів (правотворчості, законодавчої техніки, техніки створення корпоративних актів, юридичних документів, систематизації юридичних актів, юридичної термінології тощо), здатність продемонструвати уміння формулювати нові гіпотези та наукові проблеми, обирати належні напрями й відповідні методи для їх дослідження тощо.

Оскільки точка неповернення вже пройдена і жодний уряд або корпорація не відмовляється від автоматизації рутинної частки будь-якого процесу, роботизації та використання цифрових технологій, то це означає, що необхідно навчати і навчатися не за застарілими індустріальними програмами і не тому, чому раніше (накопичувати знання, тренувати пам'ять значними обсягами інформації), але треба навчати вмінню самостійно мислити, самостійно добувати інформацію та критично її оцінювати, тобто переходити до такої системи навчання та надання адвокатських послуг, яка дозволить підготувати інноваційні кадри для інформаційного та пост-інформаційного суспільства. У зв'язку з цим учбові програми повинні бути орієнтовані на розвиток критичного мислення, творчої винахідливості та навичок взаємодії між людиною та штучним інтелектом.

В якості позитивних прикладів творчого підходу до своєї справи, здатності продукувати нові ідеї, уміння працювати в міждисциплінарній галузі та встановлювати системні зв'язки в межах учбового процесу Національного юридичного університету ім. Ярослава Мудрого (м. Харків) можливо навести наступні: прив'язка задач, які вирішуються на практичних заняттях, до обставин, що висвітлюються у популярних серіалах, зокрема "Гра престолів"<sup>1</sup>; обговорення зі студентами питань декриміналізації окремих злочинів, внесення змін до існуючих норм або можливості криміналізації нових форм суспільно небезпечної поведінки (навчальна дисципліна "Теорія і практика кваліфікації злочинів у сфері господарської діяльності"); поява нових спецкурсів та сертифікатних учбових програм, в тому числі, "Гендерні студії" (розробники – О. Уварова, О. Харитонova, Ю. Разметаєва, О. Дашковська, В. Смородинський), "Основні тренди розвитку сучасного кримінального права" (розробниця – О. Харитонova), "Право та кіберпростір: штучний інтелект, цифрова людина, Всеосяжний Інтернет, децентралізована юридична особа" (розробник – О. Радутний) тощо.

Змін зазнають всі традиційні підходи. Так, потужна лондонська юридична фірма Schillings дозволила своїм співробітникам не приходити в офіс кожен день, повідомляє The Law Society Gazette [13]. Досить з'являтися в "штаб-квартирі" двічі на тиждень. Втім, необхідність присутності в офісі може змінюватися залежно від кількості призначених зустрічей. Новий девіз компанії: "Робота – це діяльність, а не місце". Чимало юристів задоволені такими нововведеннями. Обурення вони викликають лише у тих, хто довгий час прагнув до того, щоб на дверях кабінету висіла табличка з ім'ям.

Повністю є схвальною позиція І. Томарова [38] щодо порушених питань: вступити на юрфак має бути легко, а вчитися – складно настільки, щоб на першому курсі випадкові особи самоусунулись, щоб на першій роботі переконатись, що твої навички і знання потрібні незалежно від того, хто є клієнтом, пенсіонери чи корпорації; про розвиток соціальних soft skills виступу перед аудиторією, роботи в команді, ведення переговорів; студент юрфаку має бути вимогливим до своїх викладачів, не боятись спитати, чому я можу навчитись у вас, і це ж питання задавати компаніям, які пропонуватимуть йому роботу; юридична практика вимагає передбачати розвиток подій, прогнозувати найгірші сценарії, чому неможливо навчити шляхом читання підручника, закону чи судової практики (у зв'язку з чим викладачам – практикуючим адвокатам необхідно доплачувати, як це має місце за науковий ступінь та звання); критичне мислення має прийти на зміну відтворенню, юрфак зміниться тоді, коли провідні роботодавці на ринку юридичних послуг або самі будуть викладати, або будуть вимагати від викладачів якісної освіти.

### **Висновки та пропозиції.**

Таким чином, онтогенез юридичної освіти та сфери правових послуг під впливом інформаційних технологій, в тому числі, штучного інтелекту та Всеосяжного Інтернету (Internet of Everything), може включати наступні напрямки: 1) співробітництво суспільства, юридичного бізнесу, установ освіти та держави у визначенні пріоритетів процесу освіти; 2) надання переваг горизонтальній взаємодії (навчання середовищем, взаємне навчання); 3) придбання нових культурних та фахових компетенцій, формування коду професії; 4) перехід від запам'ятовування до творчих рішень,

<sup>1</sup> "Гра престолів" (англ. Game of Thrones) – американський телесеріал у жанрі фентезі, створений за мотивами циклу романів "Пісня льоду й полум'я" письменника Джорджа Р.Р. Мартіна, дата прем'єри в США – 17 квітня 2011 року, протягом 2011 – 2019 років вийшло 8 сезонів із 8 запланованих.

комунікації; 5) індивідуальна траєкторія та персоналізація навчання (вибір дисциплін, проектів та викладачів, адаптація та коригування індивідуальної карти знань і навичок), використання гнучких освітніх систем у зв'язку з коротким строком актуального життєвого циклу сучасних технологій; 6) перетворення процесу навчання юридичним дисциплінам та надання правових послуг на живу адаптивну систему, яка легко підлаштовується під зміни в режимі реального часу; 7) практичне впровадження концепції безперервного навчання (сьогодні вже неможливо після одноразового отримання певної професії використовувати її без змін впродовж активного трудового життя); 8) інноваційність, підтримання творчого підходу навіть тоді, коли практичні результати поки що не простежуються.

Освіта повинна будуватися на концепції навчання на випередження та підготувати людину до того, що реалії її життя через кожні 5 – 10 років будуть істотно відрізнятися від тих, в яких вона навчалася або починала свою професійну кар'єру.

**Перспективи подальших досліджень.** порушені питання та надана їм авторська оцінка є дискусійними та відкритими для конструктивної критики і широкого обговорення з огляду на їх актуальність та важливість для забезпечення сталого розвитку інформаційного суспільства. Дослідження, які присвячені конкурентоздатності та запобіганню інтелектуальної деградації людини у середовищі співіснування зі штучним інтелектом, мають значення для збереження та розвитку цивілізації. Нам не є відомим, що знаходиться за горизонтом сингулярності, але здійснити спробу досягнення антикрихкості ми повинні.

### Використана література

1. Amper music. URL: <https://www.ampermusic.com>. Title from the screen.
2. Bill H.R.4625 “Fundamentally Understanding The Usability and Realistic Evolution of Artificial Intelligence Act of 2017” or the “Future of Artificial Intelligence Act of 2017”, December 12, 2017, 115<sup>th</sup> Congress 1st Session. URL: <https://www.congress.gov/bill/115th-congress/house-bill/4625/text>. Title from the screen.
3. Bostrom, Nick. How long before superintelligence? Oxford Future of Humanity Institute. University of Oxford. Originally published in Int. Jour. of Future Studies, 1998, vol. 2. URL: <https://nickbostrom.com/superintelligence.html>. Title from the screen.
4. Cakebread, Caroline. Robots aren't just taking our jobs, they're creating them – here are 21 weird jobs humans will have in the future. URL: <http://www.businessinsider.com/21-weird-jobs-humans-will-have-when-robots-take-over-2017-11/#data-detective-1>. Title from the screen.
5. Chen, Stephen. Is China's corruption-busting AI system 'Zero Trust' being turned off for being too efficient? / South China Morning Post, 4 Feb, 2019. URL: <https://www.scmp.com/news/china/science/article/2184857/chinas-corruption-busting-ai-system-zero-trust-being-turned-being>. Title from the screen.
6. Chin, Monica. AI just beat top lawyers at their own game. URL: <https://mashable.com/2018/02/26/ai-beats-humans-at-contracts/#6ulr5fYsdqo>. Title from the screen.
7. Chris, Dixon. What's Next in Computing? Medium Corporation, Feb 21, 2016. URL: <https://medium.com/software-is-eating-the-world/what-s-next-in-computing-e54b870b80cc>. Title from the screen.
8. Clifford, Catherine. Elon Musk: 'Robots will be able to do everything better than us'. CNBC, Jul 17 2017. URL: <https://www.cnn.com/2017/07/17/elon-musk-robots-will-be-able-to-do-everything-better-than-us.html>. Title from the screen.
9. Control Risk Report: Risk Map 2019. URL: <https://www.controlrisks.com/riskmap?Source=MPLP>. Title from the screen.
10. Copeland B.J. Artificial intelligence (AI). URL: <https://www.britannica.com/technology/artificial-intelligence>. Title from the screen.

11. Dellinger, AJ. AI-generated painting Portrait of Edmond Belamy' from art collective Obvious sells for \$432,000 at auction. URL: <https://www.engadget.com/2018/10/25/ai-generated-painting-sells-for-432-000-at-auction>. Title from the screen.
12. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). URL: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN>. Title from the screen.
13. Fouzder, Monidipa. 'Don't expect to be in the office more than two days, lawyers told. The Law Society Gazette, August 26, 2016. URL: <https://www.lawgazette.co.uk/practice/dont-expect-to-be-in-the-office-more-than-two-days-lawyers-told/5057277.article>. Title from the screen.
14. Fenner, Robert. Alibaba's AI Outguns Humans in Reading Test / Bloomberg Technology, 15 Jan 2018. URL: <https://www.bloomberg.com/technology>. Title from the screen.
15. Gary Lea. The Struggle To Define What Artificial Intelligence Actually Means. September 3, 2015. URL: <https://www.popsoci.com/why-we-need-legal-definition-artificial-intelligence>. Title from the screen.
16. How soon will computers replace The Economist's writers? Robots. – URL: <https://www.economist.com/news/science-and-technology/21732805-weve-got-few-years-left-least-how-soon-will-computers-replace-economists>. Title from the screen.
17. Household Size and Composition Around the World 2017. United Nations' Data Booklet. URL: [https://www.un.org/en/development/desa/population/publications/pdf/ageing/household\\_size\\_and\\_composition\\_around\\_the\\_world\\_2017\\_data\\_booklet.pdf](https://www.un.org/en/development/desa/population/publications/pdf/ageing/household_size_and_composition_around_the_world_2017_data_booklet.pdf). Title from the screen.
18. Identity Politics / Stanford Encyclopedia of Philosophy. URL: <https://plato.stanford.edu/entries/identity-politics>. Title from the screen.
19. International Energy Outlook 2018 (IEO2018) for Center for Strategic and International Studies, July 24, 2018. Washington, DC by Dr. Linda Capuano, Administrator U.S. Energy Information Administration. URL: [https://www.eia.gov/pressroom/presentations/capuano\\_07242018.pdf](https://www.eia.gov/pressroom/presentations/capuano_07242018.pdf). Title from the screen.
20. Knapton, Sarah. Artificially intelligent 'judge' developed which can predict court verdicts with 79 per cent accuracy. URL: <http://www.telegraph.co.uk/science/2016/10/23/artificially-intelligent-judge-developed-which-can-predict-court>. Title from the screen.
21. Rory, Cellan-Jones. The robot lawyers are here – and they're winning. URL: <http://www.bbc.com/news/technology-41829534>. Title from the screen.
22. Seven Revolutions / CSIS – Center for Strategic & International Studies. URL: [https://csis-prod.s3.amazonaws.com/s3fs-public/171114\\_Seven-Revolutions-Brochure-2017.pdf?N5M75hddnxjj6xi808QeJTHOXD9kjZkN](https://csis-prod.s3.amazonaws.com/s3fs-public/171114_Seven-Revolutions-Brochure-2017.pdf?N5M75hddnxjj6xi808QeJTHOXD9kjZkN). Title from the screen.
23. Science Education for Responsible Citizenship (2015). Report to the European Commission of the expert group on science education, Directorate-General for Research and Innovation Science with and for Society EUR 26893 EN. URL: [http://ec.europa.eu/research/swafs/pdf/pub\\_science\\_education/KI-NA-26-893-EN-N.pdf](http://ec.europa.eu/research/swafs/pdf/pub_science_education/KI-NA-26-893-EN-N.pdf). Title from the screen.
24. Smith, Agnese. Artificial intelligence. 2015. URL: <http://nationalmagazine.ca/Articles/Fall-Issue-2015/Artificial-intelligence.aspx>. Title from the screen.
25. Taleb, Nassim Nicholas. Antifragile: Things That Gain from Disorder. Random House, 2012. 430 p. / в укр. перекладі: Талеб, Насім. Антикрихкість. Про (не)вразливе у реальному житті / пер. з англ. Миколи Климчука. Київ: Наш формат, 2018. 408 с.
26. The Zettabyte Era: Trends and Analysis by Cisco. URL: <https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html>. Title from the screen.
27. The Global Information Technology Report 2016: Innovating in the Digital Economy. The World Economic Forum, Editors: Silja Baller (World Economic Forum), Soumitra Dutta (Cornell University), Bruno Lanvin (INSEAD). URL: [http://www3.weforum.org/docs/GITR\\_2016/WEF\\_GITR\\_Full\\_Report.pdf](http://www3.weforum.org/docs/GITR_2016/WEF_GITR_Full_Report.pdf). Title from the screen.
28. Urban, Tim. The AI Revolution: The Road to Superintelligence. January 22, 2015. URL: <https://waitbutwhy.com/2015/01/artificial-intelligence-revolution-1.html>

29. Winick, Erin. Lawyer-Bots Are Shaking Up Jobs / MIT Technology Review, December 12, 2017. URL: <https://www.technologyreview.com/s/609556/lawyer-bots-are-shaking-up-jobs>. Title from the screen.

30. World Population Prospects: The 2017 Revision / Department of Economic and Social Affairs of United Nation. URL: <https://www.un.org/development/desa/publications/world-population-prospects-the-2017-revision.html>. Title from the screen.

31. Xu D., Nishimura T. Zheng M. and others. Enabling autologous human liver regeneration with differentiated adipocyte stem cells / Cell Transplant, 2014; 23(12):1573-84. doi: 10.3727/096368913X673432. Epub 2013 Oct 21. URL: <https://www.ncbi.nlm.nih.gov/pubmed/24148223>. Title from the screen.

32. Баррат Дж. Последнее изобретение человечества: искусственный интеллект и конец эры Homo sapiens. Москва: Альпина Нон-фикшн, 2015. 304 с.

33. Берман, Г.Дж. Западная традиция права: эпоха формирования / пер. с англ. Дж. Г. Берман. 2-е изд. Москва: Изд. гр. ИНФРА-М – НОРМА. 1998. С. 97, 152, 209-215.

34. Бойченко М. А. Теоретичні та методичні засади освіти обдарованих школярів у США, Канаді та Великій Британії: автореф. дис. на здобуття наук. ступеня доктора педагогічних наук за спеціальністю 13.00.01 – загальна педагогіка та історія педагогіки. – Сумський державний педагогічний університет імені А.С.Макаренка. Суми, 2019. 45 с.

35. Віртуальне правосуддя залишає суддів без роботи. URL: [http://loyer.com.ua/uk/virtualne-pravosuddya-zalishaye-suddiv-bez-roboti/?fbclid=IwAR2UMVnyY3VvDXrYtUB-z7KvRRsL3yvmYupVOqZI-j5uiYulzyuHU\\_-MmJo](http://loyer.com.ua/uk/virtualne-pravosuddya-zalishaye-suddiv-bez-roboti/?fbclid=IwAR2UMVnyY3VvDXrYtUB-z7KvRRsL3yvmYupVOqZI-j5uiYulzyuHU_-MmJo). Заголовок з екрану.

36. Нассім Ніколас Талеб. Чорний лебідь: Про (не)ймовірне в реальному житті. Київ: Наш Формат, 2017. 392 с.

37. Корпоративне право України: підручник / В.В. Луць, В.А. Васильєва, О.Р. Кібенко, І.В. Спасибо-Фатєєва [та ін.]; за заг. ред. В.В. Луця. Київ: Юрінком Інтер, 2010. 384 с.

38. Томаров, Іларіон. Юридична освіта здорової людини. URL: [http://www.legalshift.com.ua/?p=1339&fbclid=IwAR1IdPhbxGDsOZfVZyMXdgNsyLZlG3J\\_BQjAnV7jvLPBXonf0DNgSCG\\_Z4U](http://www.legalshift.com.ua/?p=1339&fbclid=IwAR1IdPhbxGDsOZfVZyMXdgNsyLZlG3J_BQjAnV7jvLPBXonf0DNgSCG_Z4U). Заголовок з екрану.

~~~~~ \* \* \* ~~~~~

УДК 342.53:004(477)

ДОРОГИХ С.О., кандидат юридичних наук,  
старший науковий співробітник НДІП НАПрН України

## ЕЛЕКТРОННИЙ ПАРЛАМЕНТ ЯК БАЗИС ПОБУДОВИ НАЦІОНАЛЬНОЇ СИСТЕМИ НОРМАТИВНО-ПРАВОВИХ АКТІВ

*Анотація.* До питання побудови національної системи нормативно-правових актів.

*Ключові слова:* електронний парламент, парламент, Верховна Рада України, національна система правової інформації.

*Summary.* To the question of building a national system of regulatory legal acts.

*Keyword:* E-parliament, Parliament, Verkhovna Rada of Ukraine, National system of legal information.

*Аннотация.* К вопросу построения национальной системы правовой информации.

*Ключевые слова:* электронный парламент, парламент, Верховная Рада Украины, национальная система правовой информации.

**Постановка проблеми.** Євроінтеграційний рух та процеси демократизації, що відбуваються в країні, порушують питання як покращення рівня прийнятих законів та інших нормативних актів, так і збільшення прозорості діяльності органів влади, залучення громадян до законотворчого та нормотворчого процесів. У той же час процес децентралізації владних повноважень в країні у найближчому майбутньому створить розгалужену систему місцевих баз нормативно-правових документів, до яких необхідно встановити доступ для усіх громадян, які проживають чи працюють у цій місцевості.

Вирішення поставлених питань буде відбуватися, на нашу думку й завдяки впровадженню національної системи правової інформації.

**Метою статті** є визначення окремих аспектів використання досвіду розбудови електронного парламенту при побудові національної системи нормативно-правових актів.

**Виклад основних положень.** Досліджуючи питання електронного парламентаризму, в першу чергу приділяють увагу створенню та розвитку інформаційних систем Верховної Ради України. В той же час, на нашу думку, зазначені системи потрібно розглядати також і у контексті побудови Національної системи нормативно-правових актів, забезпеченні прав громадянина на отримання інформації щодо нормативно-правових актів, і не тільки на державному рівні, але й на рівні регіону чи навіть громади. Тобто процес впровадження електронного парламентаризму пов'язаний з процесом децентралізації в аспекті побудови громадянського суспільства та залучення громадянина до прийняття рішень на всіх рівнях від громади до держави шляхом надання громадянину доступу до публічної інформації щодо діяльності парламенту та законодавчої гілки влади, всієї бази нормативно-правових актів та рішень місцевих органів влади та побудови системи зворотних зв'язків щодо прийнятих актів та рішень.

Зауважимо, що система електронного парламентаризму передбачає не тільки використання інформаційно-комунікаційних технологій у законотворчому процесі, але й залучення громадян до участі у ньому, а також максимальну прозорість у діяльності законодавчого органу, що також актуально у процесі децентралізації влади, а також у діяльності місцевих органів влади та доступу громадян до місцевих нормативних актів.

На сьогодні питання реалізації доступу до повних баз регіональних нормативно-правових документів є невирішеною проблемою, не кажучи вже про інтеграцію таких баз у єдину систему. Однак, досвід, технології та стандарти, які використовуються при створенні електронного парламенту, можуть бути використані й при організації регіональних баз даних нормативно-правових документів, заощаджуючи при цьому кошти та вирішуючи питання наявності фахівців високої кваліфікації на місцях.

В Україні процес децентралізації розпочато з 2014 року з прийняттям Концепції реформи місцевого самоврядування та територіальної організації влади від 01.04.2014 року, Законів України “Про співробітництво територіальних громад” від 17.06.2014 року, “Про добровільне об’єднання територіальних громад” від 05.02.2015 року та змін до Бюджетного і Податкового кодексів – щодо фінансової децентралізації.

Цей процес дозволив формувати відповідно до положень Європейської хартії місцевого самоврядування значний дієвий і спроможний інститут місцевого самоврядування на базовому рівні – об’єднані територіальні громади [1].

Зауважимо, що згідно Концепції реформування місцевого самоврядування та територіальної організації влади в Україні, до її принципів відносяться: принцип відкритості, прозорості та громадської участі та підзвітності та підконтрольності органів і посадових осіб місцевого самоврядування територіальній громаді. Їх дотримання неможливе без функціонування механізму актуального та повного доступу громадян до нормативно-правових актів, які прийняті не тільки на рівні держави, але й на рівні обласних та місцевих органів влади.

Зрозуміло, що розробка окремих систем для 12 тисяч територіальних громад була би вкрай неефективною, а для малих громад це було б взагалі невід’ємним тягарем. Окрім того, така система була б незручною і для самих громадян України, у разі проживання або ведення бізнесу у межах декількох територіальних громад.

Таким чином, із зазначеного вище випливає необхідність створення та функціонування єдиної національної системи нормативно-правових актів, яка би забезпечувала вільний доступ громадян до нормативно-правових актів і публічної діяльності органів влади на усіх рівнях.

Побудова такої системи включає дві складові, а саме правову та організаційно-технічну.

На жаль, документи, що регламентують правила та умови доступу користувачів до національної системи нормативно-правових актів є застарілими і не відповідають чинному законодавству, зокрема Закону України “Про доступ до публічної інформації” [2, с. 206].

На нашу думку, система електронного парламенту Верховної Ради України, з її інформаційними системами нормативно-правових актів та законопроектів, які наразі й так приймають основне навантаження від користувачів щодо пошуку та отримання достовірної нормативно-правової інформації, може бути як методичним центром, щодо розробки та побудови систем ведення баз нормативно-правових актів, так і безпосереднім базисом уніфікованого програмного забезпечення для їх ведення, стандартів збереження нормативно-правових актів у електронному вигляді, тезаурусів для їх рубрикації. Більше того, система електронного парламенту виступає як певний експериментальний майданчик для відточення можливостей залучення громадян до законотворчої діяльності, що набуває особливого значення в умовах децентралізації влади.

Кінцевим результатом діяльності створення електронного парламенту в Україні є не тільки побудова електронного документообігу, інтеграція інформаційних систем Верховної Ради з іншими органами влади для підвищення якості законотворчого



процесу, забезпечення доступу громадян до публічної інформації щодо роботи вищого законодавчого органу країни, але й створення такої системи, де громадянин може ознайомитися зі всім масивом нормативно-правових актів як на загальнодержавному так і на регіональному рівнях й бути залученим до нормотворчої діяльності.

Фактично на кожному з рівнів (загальнодержавному, регіональному, окремої громади) система електронного парламенту в контексті забезпечення принципів прозорості та відкритості виконує однакові функції, як то:

- забезпечення доступу до публічної інформації щодо діяльності органу, який приймає нормативний документ;
- забезпечення зворотного зв'язку з громадянським суспільством щодо якості прийнятих нормативних актів;
- забезпечення зв'язку між депутатом та його виборцями;
- залучення громадян до нормотворчого процесу.

Якщо на сьогодні, офіційний веб-портал Верховної Ради несе на собі основне навантаження по забезпеченню громадян інформацією щодо нормативно-правових актів країни і прямо не пов'язаний із веб-сайтами регіональних органів влади, то у майбутньому, на нашу думку, єдина національна система нормативно-правових актів повинна надавати громадянину можливість доступу до нормативно-правових актів усіх рівнів, з обов'язковим законодавчим закріпленням обов'язку органів місцевої влади здійснювати оприлюднення всіх нормативно-правових документів у національній системі нормативно-правових актів.

На жаль, на сьогодні ми маємо неодноразові випадки, коли рішення тих чи інших місцевих рад, що торкаються прав і свобод людини і громадянина, не знаходять відображення на їх офіційних сайтах, що безумовно суперечить принципам відкритості та прозорості у діяльності влади. Також це стосується й питань публічного обговорення низки суспільно значимих питань та залучення громадян до їх вирішення.

Зазначимо також, що інтегрована система полегшить й запровадження механізму державного контролю за відповідністю Конституції та законам України рішень органів місцевого самоврядування та якістю надання населенню публічних послуг, що передбачається Концепцією реформування місцевого самоврядування та територіальної організації влади в Україні [3]. Для здійснення цього контролю передбачається створення нового для України інституту префектів. Поява такого інституту передбачалася у законопроекті по внесенню змін до Конституції України щодо децентралізації влади [4].

Зауважимо, що створення національної системи нормативно-правових актів пов'язано з процесами не тільки децентралізації влади, але й цифровізації суспільних сфер, зокрема використання цифрових технологій при залученні громадян до участі в суспільних та політичних процесах, рух до яких визначено, зокрема, у Концепції розвитку цифрової економіки та суспільства України на 2018 – 2020 роки. Одним з напрямів розвитку цифрової економіки, зокрема, названа електронна демократія, яка стимулює залучення громадян до участі в суспільних та політичних процесах. Проте відзначимо, що, на жаль, поки що ні у Концепції реформування місцевого самоврядування, ні у Концепції цифрової економіки не акцентується увага на створенні національної системи нормативно-правових актів як важливого елементу місцевого самоврядування та цифрової економіки.

Не можна сказати, що не було спроб використати ресурси Верховної Ради України для забезпечення громадян доступом до нормативно-правових документів регіонального законодавства. Так, інформаційно-пошукова система (далі – ІПС) “Законодавство”, яка

містить ту саму базу даних нормативно-правових актів, яка знаходиться на веб-порталі Верховної Ради України і є її офф-лайновою версією, створила свого часу дві регіональні бази: Київське регіональне законодавство та Законодавство АР Крим. Перша база даних функціонує й зараз, а наповнення другої призупинено з часу окупації Криму військовими Російської Федерації.

Але головне, що ІПС “Законодавство” могла би бути інструментом, який би дозволяв повністю створювати, підтримувати та адмініструвати власну базу нормативно-правових актів у повному обсязі, включно зі створенням блоків оновлення для актуалізації такої бази на комп’ютерах інших користувачів.

Документи у базах даних, створених таким чином, індексуються, можуть містити прямі посилання на загальнодержавні нормативно-правові документи, а користувач може використовувати потужне ядро системи для пошуку та сортування необхідних йому документів.

Ця спроба, на нашу думку, є дуже корисною з тих міркувань, що закриває великий організаційно-технічний напрям у розбудові національної системи нормативно-правових актів, дозволяючи регіональним органам влади та органам місцевого самоврядування вже використовувати готовий інструмент для підтримки власних баз нормативно-правових документів.

Наступним організаційним кроком, є створення можливості перенесення такої бази даних з режиму офф-лайнової системи на веб-сторінку відповідного органу та поєднання їх у єдину систему.

На останнє зазначимо, що в основі ідеї децентралізації влади лежить передача місцевій владі більшої частини повноважень та фінансування, що надає органам влади місцевого самоврядування більше можливостей для розвитку територій, створення сучасної освітньої, медичної, транспортної, житлово-комунальної інфраструктури. Більший обсяг ресурсів, який буде знаходитись у руках органів місцевої влади, потребує більшого контролю з боку громадськості і більшого її залучення до процесу прийняття рішень. Тому й на рівні місцевих органів влади важливо використовувати ті ж принципи відкритості та прозорості, що й на рівні парламенту. Відповідно, як на рівні парламенту будуються зв’язки між виконавчою та законодавчою владою у межах законодавчого трикутника, так і на місцевих рівнях необхідна інтеграція інформаційних систем між органами місцевого самоврядування та органами виконавчої влади, необхідна побудова системи доступу громадян до інформації щодо роботи місцевих депутатів, засідань комітетів та комісій з питань, які стосуються прав та інтересів громадян.

Правове забезпечення суспільних відносин, які виникають у процесі доступу громадян до публічної інформації у процесі діяльності парламенту та органів місцевого самоврядування, залучення громадян до законотворчого та нормотворчого процесу, починаючи від органів місцевого самоврядування і закінчуючи парламентом ще потребують досконального опрацювання, але процеси з розбудови системи електронного парламенту у Верховній Раді України закладають для цього серйозне підґрунтя.

### **Висновки.**

Побудова національної системи правової інформації дозволяє зробити не лише інтегровану систему нормативно-правових ресурсів усіх органів влади (починаючи від центральних і закінчуючи рівнем громад), але й впровадити механізми участі громадян у законотворчому та нормотворчому процесах, а також забезпечити вільний доступ до всього масиву нормативно-правових документів на всій території країни та публічної інформації щодо діяльності органів влади на всіх рівнях.

В її основі знаходяться як бази нормативно-правових документів так і елементи залучення громадян до участі у прийнятті рішень, законотворчому та нормотворчому процесах.

Обов'язковою передумовою існування такої системи є впровадження єдиних стандартів (бажано відкритих) створення, збереження та обміну інформацією між усіма елементами системи.

На нашу думку, побудова національної системи правової інформації може бути розпочата з системи електронного парламенту Верховної Ради України, а у разі виконання Дорожньої карти щодо внутрішньої реформи та підвищення інституційної спроможності Верховної Ради України – з інтегрованої системи “законодавчого трикутника” (інформаційних систем Верховної Ради, Адміністрації Президента та Кабінету Міністрів України).

У своєму кінцевому результаті впровадження національної системи правової інформації спрямоване на покращення якості створюваних законопроектів та побудови громадянського суспільства, котре бере активну участь в управлінні країною.

### Використана література

1. Реформа децентралізації. URL: <https://www.kmu.gov.ua/ua/diyalnist/reformi/reforma-decentralizaciyi>
2. Корж І.Ф., Морозов А.О., Лихоступ С.В., Загаєцька О.А. Формування консолідованої системи нормативно-правової інформації в умовах децентралізації влади в Україні: монографія. Київ: ТОВ “Видавничий дім “АртЕк”, 2018. 238 с.
3. Про схвалення Концепції реформування місцевого самоврядування та територіальної організації влади в Україні: Розпорядження Кабінету Міністрів України від 01.04.14 р. № 333-р. URL: <http://zakon.rada.gov.ua/laws/show/333-2014-%D1%80>
4. Про внесення змін до Конституції України (щодо децентралізації влади): проект Закону України від 01.07.15 р. № 2217а. URL: <http://zakon.rada.gov.ua>

~~~~~ \* \* \* ~~~~~

**Інформаційна і національна безпека**

УДК 316 (477)

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

**ВІД “ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА” ДО “ІНФОРМАЦІЙНОЇ БЕЗПЕКИ”:  
ДО ПРОБЛЕМИ КОНЦЕПТУАЛІЗАЦІЇ СУТНОСТІ ПОНЯТЬ**

**Анотація.** У статті зроблена спроба більш детального заглиблення у проблематику інформаційного суспільства та інформаційної безпеки на основі основоположних праць найбільш яскравих дослідників даної галузі знань. Обґрунтовується, що подальший безпечний розвиток і застосування інформаційних технологій з метою забезпечення динамічної рівноваги суспільної еволюції вимагає посилення уваги до проблеми інформаційної безпеки.

**Ключові слова:** інформаційне суспільство; постіндустріальне суспільство, інформація, інформаційна безпека, інформаційні технології.

**Summary.** The article attempts a more detailed deepening in the issues of the information society and information security based on the fundamental works of the most brilliant researchers in this area of expertise. It is substantiated that the further safe development and application of information technologies to ensure a dynamic equilibrium of social evolution requires increased attention to the problem of information security.

**Keywords:** information society, postindustrial society, information, information security, information technology.

**Аннотация.** В статье предпринята попытка более детального углубления в проблематику информационного общества и информационной безопасности на основе основополагающих трудов наиболее ярких исследователей данной области знаний. Обосновывается, что дальнейшее безопасное развитие и применение информационных технологий с целью обеспечения динамического равновесия общественной эволюции требует усиления внимания к проблеме информационной безопасности.

**Ключевые слова:** информационное общество; постиндустриальное общество, информация, информационная безопасность, информационные технологии.

**Постановка проблеми.** Людина створила ноосферу, володіючи здатністю розумно мислити й перетворювати світ навколо себе. У цьому антропогенному середовищі виділилися три основні сфери людської діяльності, які визначають і спрямовують соціальний розвиток: виробнича, технологічна та інформаційна. На сучасному етапі суспільного розвитку, завдяки своєму визначальному значенню для подальшого глобального розвитку цивілізації, домінуючою стає інформаційна сфера. Тому цілком природно, що поняття інформаційного суспільства відображає об’єктивну тенденцію у соціальній еволюції, коли інформація (знання) стає однією з основних цінностей у житті людей [1 – 2].

Сьогодні у всіх сферах життєдіяльності суспільства чітко позначився клас нових видів загроз і небезпек, пов'язаних із застосуванням новітніх інформаційно-технологічних засобів, які мають безліч варіантів свого прояву: спотворення інформації, маніпулювання свідомістю людей, інформаційна війна тощо. Народжений глобалізацією загальний інформаційний простір слугує полем розгортання інформаційного протистояння держав. Безперервне зростання потужності інформаційних технологій, їх масштабне впровадження призвели до трансформації системи цінностей, в результаті чого сучасне суспільство відчуває глобальну ціннісну кризу.

В інформаційному суспільстві основним чинником розвитку є виробництво й використання людиною науково-технічної та іншої інформації. Кодифікація знання і технологічний прогрес визначаються як системотворчі чинники соціального прогресу. Формування економіки, культури і суспільної психології відбувається в певних умовах, що складаються під впливом техніки й технологій. Теорія постіндустріального суспільства, на наш погляд, є підґрунтям формування сучасної концепції інформаційного суспільства.

Відтак, осмислення сукупності інформаційних процесів щодо забезпечення їх безпеки набуває великого значення. Ситуація, що склалася, свідчить про необхідність адекватної філософської рефлексії, вироблення нової аксіологічної парадигми, відповідної новій формулі буття. У зв'язку з цим, цілком закономірним виявляється пошук основоположних цінностей, які зададуть орієнтири майбутнього розвитку цивілізації, заснованої на інформаційних технологіях, закладуть фундамент, що підтримуватиме внутрішній світ людини і визначатиме стійкість суспільства у цілому.

**Результати аналізу наукових публікацій** свідчать про те, що перші аналітичні дослідження, які стосуються інформаційного суспільства у сучасному його розумінні, були зроблені ще у 1962 році у праці “Виробництво й розподіл знань у США” Ф. Махлупа, а потім – у дослідженні 1974 року “Інформаційна економіка” М. Поратса. Європу проблема інформаційного суспільства зацікавила в кінці 1970-х, що було відзначено появою дослідження Р. Пойрера “Інформаційний економічний підхід: характеристики обмеження і можливі перспективи”.

На початку 1990-х інтерес до інформаційного суспільства, здавалося б, вичерпався, але поява Інтернету знову стимулювала дослідження цієї проблематики. Отже, проблематика інформаційного суспільства та застосування інформаційних технологій опрацьована достатньо повно. Разом з тим, незважаючи на досить велику кількість наукових доробок у даній царині, будемо констатувати, що цілісної теорії інформаційного суспільства на сьогоднішній час не існує. Це обумовлено, перш за все, тим, що дослідженням інформаційного суспільства займається ціла низка наук – філософія, політологія, соціологія, теорія комунікації, соціолінгвістика, психолінгвістика та ін. Дуже мало й спеціальних доробків, які висвітлювали б філософські аспекти інформаційної безпеки в інформаційному суспільстві, а наявні вимагають деяких уточнень з урахуванням нових інформаційно-технологічних та соціокультурних процесів.

**Метою статті** є спроба більш детального заглиблення у проблематику інформаційного суспільства та інформаційної безпеки на основі основоположних праць найбільш яскравих дослідників даної галузі знань.

**Виклад основного матеріалу.** Основи теорії постіндустріального суспільства свого часу заклав американський соціолог Д. Белл [3, с. 207], ідеї якого отримали подальший розвиток у концепції “Трьох хвиль” Е. Тоффлера [4]. Крім того, теоретиками постіндустріалізму є У. Дайзард, Г. Кан, Т. Стоуньєр, А. Турен та ін. [5 – 7].

Й. Масуда, засновник інституту інформаційного суспільства, у своїх працях досить повно представляє теоретичний образ нового типу людського суспільства, фундаментом розвитку якого служать інформаційні цінності [9].

М. Кастельс нову епоху, світову культуру, соціальну та економічну ситуацію, в яку входить людство, називає “інформаціональне суспільство” [10].

Усі автори єдині у думці, що світ вступає в епоху грандіозних соціальних змін, технологічних і культурних перетворень, прогностичні позиції їх є досить близькими. Потенціал техніки, незмінно нарощуваний, здійснює вирішальний вплив на всі сфери життя людського суспільства. Зростає продуктивність праці, у сотні разів змінюється його зміст. Ці зміни трансформують лад культури і впливають на формування всієї цивілізації. Людський інтелект, його міць багаторазово збільшуються завдяки комп’ютерній революції, що розгортається. Соціальна структура суспільства виявляється під надмірним впливом технологічних нововведень. Суть трансформацій, що відбуваються, полягає в тому, що народжується новий цивілізаційний устрій, в якому сфера праці, наука та освіта, державне управління, культура будуть мати принципово інший характер.

На відміну від індустріального суспільства, яке в основі має машинну технологію, специфіка постіндустріального суспільства криється у використанні інформаційно-інтелектуальної технології. “Постіндустріальне суспільство не є продовженням існуючих тенденцій у західному суспільстві, це новий тип соціально-технічної організації і способів життя...” [11, с. 167]. Деніел Белл розглядає як основне джерело всіх видів обміну, здійснюваних у суспільстві, інформацію і знання [3]. Характерною особливістю постіндустріального суспільства є те, що процес обміну інформацією та знаннями здійснюється за допомогою інформаційних і телекомунікаційних технологій. П’ять характеристик постіндустріального суспільства з одинадцяти, виділених Д. Беллом, безпосередньо пов’язані з розвитком науково-технічної революції.

У постіндустріальному суспільстві, як зазначає Д. Белл, формується нова еліта, цей прошарок суспільства реалізується завдяки компетентностям і високій кваліфікації, яких індивіди набувають завдяки освіті. Тепер статус у суспільстві не визначається кількістю наявної власності, що успадковується або одержується в результаті підприємництва, або певної політичної позиції. В результаті чільна роль теоретичного наукового знання, на думку Д. Белла, визначається положенням вченого як центральної фігури у постіндустріальному суспільстві. “Постіндустріальне суспільство є суспільство знання у двоякому сенсі: по-перше, джерелом інновацій дедалі більшою мірою стають дослідження і розробки...; по-друге, прогрес суспільства... визначається успіхами в царині знання” [3, с. 288]. Таким чином, Д. Белл визначає інформацію та знання “стратегічним ресурсом” – основною силою, що породжує докорінні зміни у постіндустріальному суспільстві.

Автор заводить розмову про необхідність законодавчого врегулювання забезпечення вільного доступу до інформації, усунення загроз політичного та адміністративного контролю над суб’єктами за допомогою застосування інформаційних технологій. Важливо відзначити, не применшуючи вирішальної ролі технологій у розвитку сучасної цивілізації, Д. Белл багаторазово виділяє думку про те, що технологія не може прогнозувати соціальних змін, але має можливість надати для цього необхідні інструменти. “Технологія не детермінує соціальні зміни; технологія надає інструментальності й потенційності” [11, с. 167]. У цьому ключі особливо підкреслимо знаменний висновок Д. Белла про те, що всі результати використання технологій цілком залежать від подальшого розвитку суспільства, але якщо точніше:

від цінностей, які детермінують поведінку людини. Сьогодні, на наш погляд, цю ідею необхідно розглядати як основоположну при формуванні філософської концепції інформаційної безпеки.

Важливо відзначити, що робота Д. Белла відноситься до числа перших досліджень, які вивчають нове суспільство, і орієнтована на пошук і узагальнення його характерних ознак. В рамках даної концепції позначені основні напрямки, що концентрують увагу на різних суспільних відносинах, зосереджених навколо інформації і технологічних засобів її зберігання й передачі, розглянуті їх можливі соціальні перспективи. Необхідно підкреслити, що теорія Д. Белла досить цікава в плані розглянутих питань і свого часу відкрила великі дослідницькі перспективи. Однак, як показує дійсність, прогнози автора про найближче майбутнє у порівнянні з нинішніми реаліями виявляються деякою мірою утопічними. Наприклад, виникнення нової еліти суспільства, заснованої на особливому статусі освіти, який заперечує поняття кількості власності і політичних позицій, або становлення нової концепції праці, заснованої виключно на творчому підході до роботи. У той же час, формування подібної еліти, як варто відзначити, має не тільки позитивні ефекти, тут криються великі небезпеки. Основним класом у системі постіндустріальної економіки стає клас, який володіє основним капіталом – знаннями, у результаті чого постіндустріальне виробництво нагородило домінуючий клас правами на привласнення ними блага, що, на нашу думку, лягло в основу суперечливої ситуації, яка знову повертає суспільство до мрій про справедливість і рівність.

Далі вкажемо, що термін “постіндустріальне” не визначає соціальної і політичної організації сучасних нам спільнот, його застосування є зручним для опису технологічного і господарського базису. При цьому суспільство, яке описується Д. Беллом, є досить абстрактним, звідси не виключається можливість його проявів у різних формах. З цього випливає, що, маючи у своїй підставі фундамент постіндустріальної економіки, сформується декілька спільнот, описуючи внутрішню організацію яких, варто, перш за все, керуватися не економічними, а соціально-політичними структурними принципами. У результаті розвитку постіндустріального суспільства Д. Белла як основи інформаційного не виключає економічних, соціальних і всіх інших проблем людства.

Як і Деніел Белл, Томас Стоуньєр у своїй концепції нового суспільства вважає, що стратегічним ресурсом тепер стає інформаційний [77]. Він визначає його як такий, що містить найбільшу економічну цінність, є основним джерелом багатства. Більше того, автор викладає детальну характеристику поняття “інформація” і вперше починає розмову про формування інформаційної економіки.

Інформація, подібно економічних ресурсів людського суспільства, зазнає накопичення, зберігання для подальшого використання й поширення. Т. Стоуньєр підкреслює, що вже в капіталістичному суспільстві XVIII і XIX століть існувала думка про те, що уречевлена праця людини представлена в технічних зразках. Він вкладає в це поняття нову думку про те, що технічні винаходи, являючи собою матеріалізовану працю, є одночасно і вираженою інформацією. Крім того, автор концепції визначає наукове знання як основний фундамент майбутнього прогресу у розвитку суспільства. Від науки до виробництва – у подібному напрямку йде сьогодні потік інформації, на відміну від минулого, коли шлях науки прокладав практичний досвід. Т. Стоуньєр виділяє основний лімітуючий фактор постіндустріального суспільства з його інформаційною економікою – знання. Зростання національного продукту в економіці прямо пропорційне зростанню наукового знання і технологій в суспільстві, оскільки

інформаційна компонента є основною складовою кожного виду діяльності. Техніка, що приходить в життя людини через технологічні знання й організаційні удосконалення, створює багатства, вона є засобом її життєдіяльності. Найважливіший ресурс постіндустріального суспільства – людський капітал, тобто знання, досвід, здоров'я людини.

Т. Стоуньер робить важливе зауваження: в основі професійних компетенцій, рівня кваліфікації кожної людини в постіндустріальному суспільстві знаходиться освіта. “Удосконалення освіти необхідно для дедалі більшого збагачення знаннями людського капіталу, підвищення продуктивності робочої сили, починаючи від працівників фізичної праці і закінчуючи вченими-теоретиками; нарешті, для становлення інформаційного суспільства, члени якого вільно орієнтуються в тонкощах інформаційної економіки і аж ніяк не стають невротиками в умовах швидкоплинного інформаційного середовища”, – пише Т. Стоуньер [7, с. 394]. Усе суспільство стає системою освіти, протягом усього життя людина повинна отримувати нову освіту.

Т. Стоуньер визначає інформаційну епоху епохою достатку, де соціум перестають хвилювати матеріальні потреби. Як індустріальне суспільство викоренило голод, рабство і епідемії, так і постіндустріальна економіка викоринить війну і авторитаризм. Вперше в історії людського суспільства швидкість вирішення проблем випередить їх виникнення. На підставі вищесказаного, ми можемо зробити висновок, що соціально-філософська рефлексія розглянутої концепції також утопічна.

Важливо підкреслити той факт, що Т. Стоуньер характеризує зміну історичних формацій крізь призму економічного розвитку суспільства. Він описує характерні тенденції назріваючих змін, але не відображає конфлікту, що лежить в основі еволюції нового суспільства. Крім того, неможливо назвати виправданою його оцінку переходу політичної та економічної влади до виробників інформації. Мова йде скоріше про формування інформаційної еліти і її вплив на регулюючі процеси, що породжує контроль над суспільною свідомістю і не сприяє стійкому стану інформаційної безпеки в новому суспільстві.

Продовжуючи розвивати погляди Д. Белла, Е. Тоффлер розглядає еволюцію постіндустріального суспільства з точки зору зростання можливостей техніки, а також її впливу на перебіг соціальних процесів у суспільстві [4]. Головним системоутворюючим фактором його концепції є технологія як основний компонент суспільних відносин.

Розвиток технологій у людському суспільстві, на думку Е. Тоффлера, має схожість з хвилями, серед яких виділяються три основні. Технологічні хвилі змін стосуються в першу чергу аграрної революції, потім – індустріальної і постіндустріальної революції, яка розгортається в наш час. Е. Тоффлер описує її як хвилю, проникаючу всюди, яка приносить зміни в сім'ю, у трудовий процес, вона торкається етики, соціального життя, економіки і політики, змінює свідомість: “третя хвиля ...виводить нас за межі концентрації енергії, грошових коштів і влади” [4, с. 85].

Вивчення нового суспільства у взаємозв'язку і цілісності його сторін (особистості, технології, культури, економіки тощо), уважне ставлення до нормативних орієнтацій і ціннісних критеріїв, відносяться до основних переваг роботи Е. Тоффлера. Як уявляється, Е. Тоффлер виразніше описав, аніж інші соціальні філософи, важливу особливість майбутньої соціальної парадигми: людство наблизилось до небачених перетворень, точніше, наближається таке суспільство, яке не входить в рамки лінійної еволюції. Описувані якісні перетворення в суспільстві, пов'язані з високими технологіями, несуть глибокий сенс і надію на те, що вони дадуть людству справжню свободу. Виробництво потужних компактних комп'ютерів,



виробництво роботів в аерокосмічній промисловості, медицині, генній інженерії тощо – у зазначених сферах діяльності, перш за все, переважають дані технології, відмінні риси яких виділяє Е. Тоффлер: енергозберігаючі можливості, штучний інтелект, мініатюризація.

Е. Тоффлер припускає у недалекому майбутньому утворення нових суспільних відносин, що складаються на основі формування об'єднань людей на певних територіальних автономіях, пов'язаних спільними поглядами, можливо, на ґрунті релігійних, культурних або будь-яких інших інтересів. Відбудеться це завдяки новим технологіям, які допоможуть у побудові самостійного способу життя. Потреба в некваліфікованій праці зникає, одночасно з цим зростає потреба у фахівцях, здатних мислити творчо, самостійно приймати рішення і професійно використовувати складну техніку. Таким чином, ми приходимо до висновку, що соціокультурні трансформації у новому суспільстві, згідно з думкою Е.Тоффлера, вимагають від людини не старанності, а уміння миттєво реагувати на зміни. Автор говорить про людей, які не володіють даною здатністю, які ламаються або відходять убік, тим самим піднімаючи одне з найактуальніших питань інформаційної безпеки особистості. На жаль, Е. Тоффлер не пропонує способів вирішення даної проблеми, він розглядає ситуацію, що складається, лише з точки зору перспектив для розвитку компетентних індивідів [4, с. 99].

Викладене вище визначає третю хвилю Е.Тоффлера як етап становлення цивілізації, що тягне за собою безліч соціально-психологічних проблем, вирішення яких необхідно шукати вже в наш час.

Крім того, важливо відзначити, що основна ідея концепції концентрується на передчутті необмежених можливостей для розвиненого світу, в ньому не розглядається тема рівноправного входження країн, що розвиваються, у глобальну інформаційну спільноту. Так Е. Тоффлер, як і Д. Белл, у своїй теорії відштовхується тільки від розвитку європейської цивілізації, що надає його концепції вузькоспрямованого, позбавленого універсальності відтінку. У зазначених роботах простежуються міркування про досягнення розвинених цивілізацій, при цьому інтереси менш прогресивних країн не беруться до уваги.

Так, розглянувши загальні тенденції розвитку нового суспільства, роль інформації і інформаційних технологій в ході даного процесу, необхідно виділити з ряду провідних теорій постіндустріалізму концепції, основні положення яких чітко відображають ідеї про необхідність безпечного застосування технології, що розвивається. Наприклад, французький соціолог Ален Турен, проводячи аналіз стану справ сучасного суспільства, дійшов висновку про те, що в своєму розвитку індустріальне суспільство досягло своєї найвищої точки, в результаті чого стає неминучим перехід до нового типу суспільства. Він попереджає про складний небезпечний шлях, в кінці якого як нагорода людство чекає суспільний лад, мобільний і перспективний [8].

Описуючи контури постіндустріального суспільства, А. Турен зазначає, що в постіндустріальному суспільстві управлінський рівень відрізняється більшою глобальністю, автор має на увазі весь механізм виробництва в цілому. Він виділяє дві головні форми, яких набуває вказана дія: по-перше, нововведення в результаті інвестицій в науку і техніку; по-друге, управління, зміст якого полягає в умілому використанні складних систем інформації та комунікацій. “Програмоване суспільство” – таке визначення пропонує А. Турен для нового суспільства, оскільки в ньому закладена можливість виробляти моделі всіх етапів економічного процесу [8, с. 23,

129-130]. На його думку, саме такі відносини, як соціальні та економічні, можуть бути концептуальними у поданні про образ програмованого суспільства, звідси особлива роль у ході інформаційної революції покладається на нову управлінську та інвестиційну політику.

Ведучи мову про негативні сторони постіндустріального ладу, автор наголошує на небезпеці соціального контролю над людьми і суспільством у цілому з боку держави і правлячої еліти за допомогою ЗМІ та доступу до комунікацій. Технократичний характер нового суспільства полягає у тому, що “особливість правлячих сил міститься в можливості їх ототожнення з керуванням системами інформації” [8, с. 134]. Крім того, він підкреслює екологічну спрямованість поточних трансформацій у новому суспільстві. Людина вже не прагне підкорювати природу, завдяки технологіям перед нею відкрилися нові горизонти для вільної творчої діяльності, тепер вона намагається реалізувати себе. Суспільне буття в інформаційному суспільстві визначено свідомістю суб’єкта, який розуміє відповідальність за свої дії, усвідомлює свої цілі й цінності. Життя соціуму “спрямовується дією тих, хто бореться і домовляється про те, щоб надати якусь суспільну форму значущим для них культурним орієнтаціям”, – пише А. Турен [8, с. 31]. Автор підводить до думки про необхідність визнання відповідальності суспільства за всі вироблені модифікації і їх можливі наслідки, які так чи інакше позначаються на соціумі й природі. Таким чином, відзначимо найважливіший аспект з точки зору забезпечення інформаційної безпеки: актуалізуючи питання про відповідальність за використання сучасних технологій з метою безпечного розвитку соціуму і навколишнього середовища, А. Турен визначає одну з ключових категорій концепції інформаційної етики зокрема і загальної теорії інформаційної безпеки у цілому.

Особливої уваги заслуговує також робота Уільяма Дайзарда, у якій описуються сценарії переходу до інформаційного суспільства і можливі проблеми у сфері інформаційної безпеки, що супроводжують цей процес [5]. Автор теорії, вивчаючи перехід до інформаційного суспільства, зазначає, що досягнутий рівень технології в особі інформаційно-комунікаційних ресурсів пропонує людству раніше незвідані можливості. Перспективи використання описуваних ресурсів настільки великі, що незаперечним є факт: суспільство стоїть на порозі нової ери – інформаційної. На його думку, чітко вимальовується загальна модель змін, яка містить у собі три стадії: розвиток економічних галузей, пов’язаних з виробництвом і розподілом інформації; збільшення числа інформаційних послуг, орієнтованих на забезпечення промисловості й уряду; формування масової інформаційної мережі для широкого споживача [5, с. 345].

У. Дайзард погоджується з концепціями розвитку суспільства Е. Тоффлера і Д. Белла, але при цьому автор припускає, що в інформаційному суспільстві вирішення соціально-економічних питань потребуватиме певних зусиль. Важливим є той факт, що У. Дайзард починає вести мову про прийдешні проблеми інформаційної безпеки: неосяжні можливості нової технології приховують у собі не одну небезпеку, боротися з якими людству доведеться щодня. Це може бути дратівлива плутанина з кредитними картами, помилки повідомлень з банку, телефонні дзвінки, збої в режимі роботи транспорту тощо. В результаті може скластися невиразне занепокоєння, від того, що техніка переступила певну межу, за якою немає зворотного шляху. Дане занепокоєння невблаганно наростає від нагромадження серйозних питань – збільшення витрат енергетичних ресурсів, захисту навколишнього середовища від

забруднення, в яких технологічна революція виступає скоріше в ролі причини їх виникнення, аніж в ролі панацеї.

Думка У. Дайзард є абсолютно справедливою, ситуація, що складається, “гостро ставить питання про необхідність ефективної політики перехідного періоду. Така стратегія лише частково повинна залежати від технічних або економічних рішень. Основними повинні стати рішення політичні, які відображають нашу готовність змінити фундаментальні соціальні інститути відповідно до можливостей інформаційного століття” [5, с. 355].

Так ми доходимо висновку, що проблеми інформаційної безпеки, які розглядаються у соціально-філософській концепції У. Дайзарда, не є лише перешкодою на шляху формування нового суспільства, це неминучий результат необдуманих рішень, що веде до руйнування соціально-економічної рівноваги. Припущення ще раз переконує в необхідності вироблення узгоджених заходів і методів контролю й нейтралізації негативних ефектів використання інформаційних технологій в рамках державної системи інформаційної безпеки.

Аналіз наукових доробків провідних постіндустріалістів приводить нас до наступної думки: назва нового суспільства, яке настає за індустріальним, не відображає головних характеристик майбутнього ладу, в якому інноваційним чинником стане інформація. Крім того, префікс “*пост*” виражає деяку обмеженість свідомості для нового суспільства (що вибудовується на нових принципах). Тому, цілком природно погодитися з думкою Юдзіро Хаяші, що основну суть суспільства, яке базується на використанні інформаційної технології, найбільш повно здатне передати поняття “інформаційне суспільство” [12].

Теоретичний образ інформаційного суспільства докладно описаний у працях японського вченого Йошито Масуди [9]. Він порівнює інформатизацію з індустріальною революцією, приписуючи їй ту ж всеохоплюючу глибину. Автор принципово виділяє відмінності між двома моделями суспільного розвитку: “виробництво не матеріальних благ, а інформаційних цінностей – основа розвитку й формування нового типу людського буття” [9, с. 29]. Й. Масуда визначає основні начала інформаційної епохи: комп’ютерна технологія заміщає працю людини; відбувається масове виробництво когнітивної інформації і знань; інтелектуальне (наукомістке) виробництво стає ключовою галуззю економіки.

У концепції Й. Масуди інформаційне суспільство – це, перш за все, “вільне співтовариство”. Використання комп’ютерів у сфері торгівлі, банківській та управлінській діяльності веде до загальної автоматизації робочих місць і масштабної комп’ютеризації, невід’ємно пов’язаної з комунікаційними мережами, тим самим породжуючи збільшення кількості вільного часу, від чого роль комп’ютерів і зв’язку у новому суспільстві буде незмірно зростати. При цьому, роботи й біотехнології підвищать інтелектуалізацію індустрії інформаційного суспільства.

Суспільство, описане Й. Масудою, безкласове й безконфліктне, інакше, суспільство згоди, йому притаманні невеликі уряд і державний апарат. Для індустріального суспільства властивою цінністю було споживання товарів, у суспільстві, яке формується, на перший план виходить час. У людському житті цінність часу височить над такими базисними економічними цінностями, як матеріальні, що визначає нову концепцію економіки, провідними галузями якої будуть інтелектуальні індустрії. Однак варто зауважити, що Й. Масуда надто ідеалізує суспільство, яке народжується, переконуючи у тому, що процес формування інформаційного суспільства буде супроводжуватися зникненням класів, зміною соціальних структур і гармонізацією людських відносин,

змінюю цінностей. Очевидним є те, що нове суспільство не стало суспільством згоди. Йому притаманні ті ж соціальні протиріччя, що й індустріальному, з тією лише різницею, що соціальні відносини в нових умовах стали складнішими, оскільки в їх систему включився інформаційний фактор.

У той же час, незважаючи на зазначене вище, Й. Масуда досить чітко уявляє проблеми і складності у сфері інформаційної безпеки суспільства, яке формується. Однією з ключових загроз він вважає небезпеку, яка полягає у вторгненні інформаційних технологій у внутрішній світ особистості і соціальних організацій. Особисте і громадське життя індивіда знаходиться під загрозою вторгнення завдяки тому, що інформація про народження, здоров'я, його роботу, бізнес, банківські рахунки міститься в банках даних. Автор переконаний у необхідності подолати зазначені труднощі: “Я вірю, що ми уникнемо цього катастрофічного автоматизованого курсу... Ми не маємо права застосовувати комп'ютер і науку для знищення духовного життя людини і людства” [9, с. 153]. Він вбачає вирішення проблем у демократизації інформації, державному захисті громадян, у цілеспрямованій роботі щодо запобігання комп'ютерних злочинів.

Цілком очевидно, що Й. Масуда визначає вірні орієнтири для вирішення актуальних проблем інформаційної безпеки, у той же час, на сьогоднішній день державна система жодної країни світу поки не налагодила ефективні механізми їх реалізації. У подібній ситуації усвідомлення важливості проведених перетворень дає стимул до їх подальшого всебічного вивчення. Наприклад, сьогодні процес демократизації інформації в суспільстві зустрічає серйозні перешкоди у вигляді існування політичних, правових, комерційних, ідеологічних, технічних і релігійних бар'єрів, подолати які – серйозне завдання для інформаційного суспільства.

Аналіз тенденцій розвитку сучасного інформаційного суспільства дає відомий іспанський філософ Мануель Кастельс [10]. На відміну від Д. Белла, який в 1970-1980-х роках XX ст. розмірковував про прогнози й перспективи інформаційної епохи, М. Кастельс мав можливість аналізувати зміни, що відбуваються на рубежі XX-XXI ст. Він розглядає основні цивілізаційні процеси, принципово пов'язані з розвитком інформаційної технології сучасного світу.

У його наукових доробках представлений перехід людства в інформаційну епоху у вигляді цілісної теорії, що дозволяє оцінити масштаб інформаційної революції, яка призвела до докорінних змін практично у всіх сферах людської діяльності. М. Кастельс вбачає революцію у сфері інформаційних технологій “відправним пунктом” при аналізі всіх економічних, суспільних і культурних процесів суспільства [10], підкреслюючи щоразу думку про те, що в описі суспільства неможливо обійтися без характеристики його технологічних інструментів. Філософ переконаний, що технологія – це свого роду потенційний ресурс розвитку історичних процесів і соціальних змін у суспільстві, що живить різні варіанти їх подальшого спрямування. Відповідно, людське суспільство безумовно є вільним у виборі шляху свого подальшого розвитку, оскільки високі технології є лише засобами здійснення життєдіяльності. У цьому ключі думки М. Кастельса збігаються з точкою зору Д. Белла.

М. Кастельс розглядає виробництво комп'ютерних технологій як фактор, що здійснює основний вплив на відносини влади і більшість культурних процесів, що протікають у людському суспільстві. У його суспільстві роль знання та інформаційних процесів підняті на досі небачену висоту, у той же час, М. Кастельс підкреслює відмінність між своєю теорією “інформаційного суспільства” (*informational society*) з озвученими раніше концепціями “інформаційного суспільства”. Під інформаційним способом еволюції автор розуміє “технологію генерування знань, обробки інформації та

символічної комунікації” [10, с. 39]. Тут визначальна відмінність криється у значенні інформації для суспільства, М. Кастельс підтверджує важливу роль інформації, а також її обміну для суспільства протягом усього історичного процесу.

М. Кастельс визначає головні характеристики інформаційно-технологічної парадигми. Згідно з першою, технологія безпосереднім чином впливає на виробництво інформації, інакше кажучи, інформація – це свого роду продукт технології. Друга стосується всіх видів людської діяльності, що перебувають під технологічним впливом. Третя полягає у мережевій логіці трансформацій соціальної системи, яку ініціює інформаційна технологія. Четверта свідчить про гнучкість інформаційно-технологічної парадигми за рахунок високої здатності до реконфігурації. Остання характеристика криється в конвергенції певних технологій в високоінтегровані розробки, прикладом тому служать інформаційні системи з телекомунікаціями, комп’ютерами і оптичною електронікою. Об’єднані разом перераховані вище риси інформаційно-технологічної парадигми є фундаментом інформаційного суспільства.

Справедливо зазначити, що М. Кастельс, ґрунтуючись на широкому історіографічному і статистичному матеріалі, проводить всебічне оцінювання цивілізаційних процесів, народжених принципово новим значенням інформаційних технологій. Фундаментальна праця М. Кастельса визначає ціннісні і світоглядні орієнтири науково-теоретичного аналізу інформаційної дійсності. Його аналіз супроводжується оптимістичними припущеннями про майбутнє, це пов’язано, перш за все, з непохитною вірою автора в силу науки і освіти, в осмислені соціальні дії суб’єкта, який адекватно реагує на зміни навколишньої дійсності, і раціональну політику перетворень.

У свою чергу, з числа нових проблем, описаних М. Кастельсом, в контексті даної статті необхідно виділити такі, як аномальну владу над суспільством нових способів комунікацій і поширення інформації, що веде до ситуації контролю над людиною. Засоби масової інформації, при своїй повній політичній безвідповідальності, тепер стають головною політичною ареною. Він вбачає у виробництві комп’ютерних технологій фактор, що здійснює основний вплив на відносини влади і більшість культурних процесів, що протікають у людському суспільстві. Ця ситуація змушує автора концепції визнати той факт, що інформаційна епоха породжує нові форми нерівності. Зі свого боку додамо, що залежність соціально-культурних процесів, які протікають у суспільстві, від виробництва і використання технологій надає технократичного забарвлення розвитку нової цивілізації, однак М. Кастельс, на жаль, не пропонує шляхів вирішення усіх зазначених вище проблем.

Також відзначимо, що іменування М. Кастельсом нового соціального ладу – “мережеве суспільство”, передбачає, перш за все, входження в інформаційну еру більш розвиненої частини людства. У даному словосполученні відображається лише така характеристика інформаційної епохи, як формування глобальних інформаційно-комунікаційних мереж, що пов’язують між собою окремих людей і держави, для розвитку яких країні необхідно володіти необхідним рівнем науково-технічного потенціалу. Як і багато західних концепцій, теорія нового суспільства М. Кастельса не пропонує можливість альтернативного шляху формування інформаційної цивілізації. Країни Заходу абсолютно переконані у своїй перевазі і в цій царині не беруть до уваги ймовірність створення самобутніх концепцій інтеграції інших культур у глобальний інформаційний простір.

Розглядаючи хронологію теоретичних поглядів на процеси інформатизації та проблеми безпеки, пов’язані з масштабним упровадженням інформаційних технологій,

можна сказати, що для перших концепцій суспільства, що формується (Д. Белл, Т. Стоуньєр, А. Турен та ін. [3; 7; 8]) властиві сподівання на проникнення науково-технічної раціональності в усі сфери життєдіяльності суспільства, що дозволить гармонізувати і максимально впорядкувати його. Це пора технократичного оптимізму, віри в успіх влади технократів і нестримного науково-технічного прогресу.

У свою чергу, роботи більш пізнього періоду (М. Кастельс, Т. Росзак та ін. [10; 11]) відрізняються вже меншою мірою науково-технічного фанатизму і великою увагою до психологічних, духовно-моральних, гуманістичних аспектів розвитку інформаційної цивілізації.

У 1990-х роках про характер прийдешньої епохи починають міркувати філософи пострадянського простору, які з питань нового світового порядку, що супроводжується інформаційною експансією технологічно розвинених країн, звертають увагу на тему природи інформаційного суспільства. Так отримує розвиток теорія формування інформаційного простору, в якій так само знаходять своє відображення проблеми інформаційної безпеки і пошук шляхів їх державного регулювання [14 – 18].

У цьому ключі виділимо цікаву роботу про самоорганізацію ноосфери відомого кібернетика Ріфгата Абдеєва [16]. Він розглядає процес розвитку суспільства з точки зору його взаємодії з досягненнями інформатики, кібернетики, синергетики, мікроелектроніки, генетики, що дозволяє йому вести мову про майбутнє людства як про інформаційну цивілізацію. Його теорія виникнення інформаційного суспільства описана як еволюція людської цивілізації у тривимірному просторі в структурі звужуваної спіралі зі змінним кроком, з наступними координатами і параметрами: час, інформація, прогрес. Надмірне зростання ролі інформаційних ресурсів і комунікацій представлено як об'єктивний фактор формування інформаційного суспільства. На думку автора, в умовах інтенсифікації інформаційних процесів знання й інформація повною мірою правлять виробництвом, дозволяючи з нічого виробляти високоефективні матеріали. Мінімальне використання енергії та сировини дозволить досягти небувалих успіхів в економіці.

Застосування інформаційних технологій у таких сферах, як сільське господарство, виробнича сфера тощо, приведуть до збільшення кількості вільного часу, дозволяючи громадянам підвищувати рівень освіти і культури. При цьому структура держави вдосконалюється: влада інформації і влада інтелекту пронизують законодавчу, судову і виконавчу гілки влади. Це відбувається шляхом підготовки до управління найбільш компетентних фахівців, що підтримують ідею свободи гласності. Держава вкладає інвестиції в системи охорони здоров'я, освіти і охорони природи. Важливо відзначити, що постекономічному характеру нової цивілізації Р. Абдеєва близькі ідеали гуманістичного соціалізму. Так автор підкреслює, що “еволюційний шлях інформаційної цивілізації дозволяє здійснити відхід від логіки капіталістичного шляху розвитку, подолати економічний фетишизм і насправді перетворити людину на самоціль суспільного розвитку” [16, с. 98].

Необхідно підкреслити, що майбутнє вчений бачить тільки за умови належного розуміння інформації та інформаційних процесів. У цьому ключі він піднімає коло питань, які потребують філософського осмислення. Р. Абдеєв переконаний, що як прогресивні тенденції розвитку потребують підтримки такі напрямки: пріоритет загальнолюдських ідеалів і цінностей; інтеграція держав, роззброєння і природозбереження. Таким чином, один з головних висновків дослідження автора імпонує цілям формування загальної теорії інформаційної безпеки. Прогрес сучасного суспільства визначають підвищення рівня освіти у сфері використання інформаційних

технологій, гуманістична спрямованість процесу інформатизації, розумна державна політика у сфері інформаційної безпеки, що забезпечує безпечний розвиток соціуму і навколишнього середовища.

Завершуючи аналіз праць теоретиків нової епохи, необхідно відзначити, що вчені справедливо виділяють характерні особливості прийдешнього часу. В рамках концепції інформаційного суспільства інформація і знання стають ключовим чинником суспільного розвитку, що перевершує за значущістю всі види матеріального виробництва, енергії і послуг. У цій концепції інформація, знання, нові інформаційні технології та телекомунікації є основним агентом економічних, соціальних і політичних змін у сучасному суспільстві.

Теорії інформаційного суспільства, безсумнівно, розширюють знання про соціальний і науково-технічний прогрес, у той же час, вони не дають цілісного уявлення про трансформації сучасного суспільства. Концептуальний аналіз основних теорій розвитку нового суспільства в контексті інформаційної безпеки дозволив нам виявити відносно невисоку ступінь критичності дослідників до можливостей, що відкрилися на основі використання інформаційних технологій. Прийдешня цивілізація ставить суспільний розвиток у тісну залежність від прогресу науки і техніки, в результаті чого набуває політично небезпечного відтінку, їй притаманні економічні, соціальні і всі інші види проблем, посилені інформаційним фактором. Крім того, відсутність в інформаційному суспільстві утвердження ідеалів справедливості поряд з проголошенням внутрішньої і зовнішньої свободи відображає в ньому деяку “етичну неповноцінність” [19 – 21], що свідчить про його нездатність протистояти виникненню антагоністичних протиріч.

Майбутні перспективи людства в теоріях інформаційного суспільства розглядаються без урахування етичних обмежень, в них затверджуються ідеї свободи, але більшою мірою ігноруються принципи інформаційної безпеки як важливої умови, що визначає на сьогоднішній день стабільність суспільного ладу. Через цю обставину, як справедливо зазначає О. Манжуєва, виявляються недостатньо врахованими нові види небезпек, загроз і негативні ефекти застосування інформаційних технологій [22].

У той же час, згідно з хронологією теоретичних поглядів на процеси інформатизації та проблеми безпеки, пов’язані з масштабним впровадженням інформаційних технологій, можна сказати, що властивий першим концепціям інформаційного суспільства високий ступінь науково-технічного фанатизму зменшується. Пізніші теорії інформаційного суспільства відрізняються вже більшою увагою до наслідків впровадження інформаційних технологій, до психологічних, духовно-моральних, гуманістичних сторін розвитку інформаційної цивілізації, тим самим створюючи методологічну основу для вирішення проблем інформаційної безпеки.

### **Висновки.**

Основні концепції нового суспільства торкаються деяких актуальних проблем інформаційної безпеки: інформаційного розшарування суспільства, контролю над індивідуальною й суспільною свідомістю, порушення конфіденційності інформації, вторгнення в особисте життя індивіда тощо. Багато ідей і положень розглянутих робіт, наприклад, аналіз суспільної та економічної динаміки М. Кастельса, аналіз значення моральної відповідальності А. Турена можуть бути покладені в основу загальнонаукової концепції інформаційної безпеки.

Таким чином, аналіз формування нового суспільства, усвідомлення його в цілісності, без відриву від інформаційних технологій, спонукає до пошуку шляхів безпечного розвитку, подолання негативних ефектів від застосування інформаційних

технологій, перегляду ціннісних орієнтирів. На наш погляд, подальший напрямок безпечного розвитку і застосування інформаційних технологій з метою забезпечення динамічної рівноваги суспільної еволюції вимагає підтримки умов інформаційної безпеки. У свою чергу, вивчення сутності поняття “інформаційна безпека” дозволить чітко уявити суть даного процесу і визначити його конкретні напрямки.

### Використана література

1. Дзьобань О.П., Кальницький Е.А. Зародження концептуальних підходів до розуміння сутності і специфіки інформаційного суспільства. *Вісник Національного університету “Юридична академія України імені Ярослава Мудрого”. Серія “Філософія, філософія права, політологія, соціологія”*. 2013. Вип. 5 (19). С. 3-15.
2. Дзьобань О.П., Жданенко С.Б. Інформаційне суспільство як новий спосіб соціальної взаємодії. *Правова інформатика*. № 1(41)/2014. С. 3-11.
3. Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования. Москва: Academia, 1999. 956 с.
4. Тоффлер Э. Третья волна. Москва: АСТ, 1999. 794 с.
5. Дайзард У. Наступление информационного века. Новая технократическая волна на Западе. Москва: Прогресс, 1986. С. 343-356.
6. Кан Г. Грядущий подъем: экономический, политический, социальный. Новая технократическая волна на Западе. Москва: Мысль, 1986. С. 169-206.
7. Стоуньер Т. Информационное богатство: профиль постиндустриальной экономики. Новая технократическая волна на Западе. Москва: Мысль, 1986. С. 393- 421.
8. Турен А. Возвращение человека действующего. Очерк социологии. Москва: Научный мир, 1998. 204 с.
9. Masuda Y. The information society as post-industrial society. Washington: World Future Society, 1983. 171 p.
10. Кастельс М. Информационная эпоха: экономика, общество и культура. Москва: ГУ ВШЭ, 2000. 608 с.
11. Bell D. The third technological revolution and its possible socioeconomic consequences. *Dissent*. New York, 1989. Vol. 367. № 2. P. 165-172.
12. Hayashi Y. Johoka shakai: Hado na shakai kara sofuto na shakai. Tokyo: Feo, 1969. 189 p.
13. Roszak T. The Cult of Information. The Folklore of computers and the True Art of Thinking. New York: Pantheon Books, 2000. 764 с.
14. Вачнадзе Г.Н. Агрессия против разума: информационный империализм. Москва: Политиздат, 1988. 271 с.
15. Моисеев Н.Н. Информационное общество как этап новейшей истории. *Свободная мысль*. 1996. № 1. С. 81-83.
16. Абдеев Р.Ф. Философия информационной цивилизации. Москва: ВЛАДОС, 1994. 334 с.
17. Боряк Г. Інформаційна інфраструктура суспільства й ретроспективні документальні ресурси (інтеграційні підходи та археографічна діяльність). *Бібліотечний вісник*. 1996. № 4. С. 3-8.
18. Бабич В. Бібліотека. Інформація. Суспільство. *Бібліотечний вісник*. 1999. № 1. С. 43-45.
19. Дзьобань О.П., Жданенко С.Б. До проблеми морально-етичних аспектів інформаційного суспільства. *Вісник Національного університету “Юридична академія України імені Ярослава Мудрого”. Серія “Філософія, філософія права, політологія, соціологія”*. 2013. Вип. 5 (19). С. 104-114.
20. Данильян О.Г., Дзьобань О.П. Інформаційне суспільство: морально-етичний дискурс. *Інформація і право*. № 1(10)/2014. С. 16-25.



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

22. Манжуева О.М. Феномен информационной безопасности: сущность и особенности: дис. ...д-ра филос. наук. Улан-Удэ, 2015. 383 с.

~~~~~ \* \* \* ~~~~~

УДК 340.132.2+351.751

**ДОРОНІН І.М.**, кандидат юридичних наук, доцент,  
завідувач наукової лабораторії  
НДІ інформатики і права НАПрН України

## ПРАВОВІ ПРОБЛЕМИ СУВЕРЕНІЗАЦІЇ ІНТЕРНЕТУ

**Анотація.** У статті проаналізовано питання визначеності державного суверенітету стосовно Інтернету, його сегментів. Досліджено практику державного регулювання у сфері телекомунікацій у контексті перспектив централізованого управління мережею Інтернет в межах окремої країни. Визначено, що законодавчі новації в Російській Федерації ухвалено з метою забезпечення стійкості Інтернету на території країни. Водночас суверенізація щодо Інтернету не означає посилення його централізованості. Правове регулювання у цьому контексті є відображенням внутрішньої державної політики.

**Ключові слова:** суверенітет, Інтернет, національна безпека, право телекомунікацій, інформаційне право, державне регулювання.

**Summary.** This paper analyzes problems of state sovereignty for Internet and its segments. Author examined practices of state regulation of telecommunications in the contest of central control for Internet within a specific country. It is defined that legislative innovations were adopted for ensuring the sustainability of Internet within Russian Federation. However, state sovereignty for Internet was not implying a higher degree of centralization. Legal regulation reflects current domestic public policy for Internet.

**Keywords:** sovereignty, Internet, national security, telecommunications law, information law, state regulation.

**Аннотация.** В статье проанализированы вопросы определмости государственного суверенитета относительно Интернета и его сегментов. Исследована практика государственного регулирования в сфере телекоммуникаций в контексте перспектив централизованного управления сетью Интернет в пределах отдельной страны. Определено, что законодательные новеллы в Российской Федерации приняты с целью обеспечения стойкости Интернета на территории страны. Вместе с тем суверенизация в отношении Интернета не должна означать усиления его централизованного управления. Правовое регулирование в этом контексте отображает внутреннюю государственную политику.

**Ключевые слова:** суверенитет, Интернет, национальная безопасность, право телекоммуникаций, информационное право, государственное регулирование.

**Постановка проблеми.** Розвиток глобальної комп'ютерної мережі Інтернет невідворотно змінив суспільство та усі соціальні інститути, набувши виняткового соціального значення. Загалом регулювання суспільних відносин у цій сфері здійснюється різними шляхами, у тому числі за допомогою права, як регулятора відносин. Очевидним є і значний багатоаспектний вплив технологій і на розвиток права та його окремих інститутів.

Водночас, існують і залишаються досить дієвими і традиційні види соціальних інститутів, в першу чергу – держава, її органи та механізм державного управління. Прояви активності зазначених інститутів відбуваються у звичний для них спосіб. У галузі правового регулювання мова йде про поняття “суверенного Інтернету”, яке характеризується спробами розповсюдити елементи державного суверенітету на глобальну комп'ютерну мережу, поставивши за мету фактично “деглобалізувати” її.

На цей час загальновідомими є суто технічні способи побудови та використання комп'ютерних мереж закритого типу ( у т.ч. умовно закритих), що розповсюджується на певну кількість ідентифікованих абонентів. Водночас, такий тип побудови мережі, що був характерний для другої половини минулого сторіччя, не дозволяє розглядати її як глобальну мережу, а отже у ній не проявляються ті соціальні явища, що характерні для всеохоплюючої глобальної відкритої мережі Інтернет. Тому для органів державного управління в різних державах час від часу характерні намагання здійснити державний вплив за допомогою права на окремі аспекти суспільних відносин, що пов'язані з використанням мережі Інтернет. Найбільш цікавими для наукового дослідження є спроби встановлення контролю (шляхом так званої “суверенізації”) певних елементів (сегментів) глобальної мережі Інтернет з боку держави, а також вжиття управлінських заходів під гаслами “суверенізації” Інтернету.

**Результати аналізу наукових публікацій.** Проблеми управління та державного впливу у сфері використання глобальної мережі Інтернет є предметом досліджень фахівців з соціальної філософії, соціології, економіки, державного управління та технічних наук. У правовій науці проблематика державного впливу розглядається як правило у контексті адміністративного права. Серед комплексних інформаційно-правових досліджень варто виділити монографію О.А. Баранова [1], а також низку робіт монографічного характеру, що стосується окремих напрямів регулювання суспільних відносин у цій сфері [2 – 4]. Останнім часом, з огляду на законодавчі новації у Російській Федерації, питання “суверенного Інтернету” активно розглядається у публіцистичній літературі та політичній полеміці.

**Метою** цієї статті є проведення аналізу впливу традиційних уявлень про державний суверенітет у правовій науці, можливості його розповсюдження на елементи глобальної мережі Інтернет з огляду на існуючі та виникаючі виклики, загрози і небезпеки. Окрім цього, передбачається проведення дослідження стану законотворчості та застосування норм права з огляду на задекларовані цілі правового регулювання (забезпечення національної безпеки) в різних юрисдикціях, проведення порівняння із іншими актами. На підставі зазначеного аналізу будуть зроблені висновки щодо подальших тенденцій у правовому регулюванні.

**Виклад основного матеріалу.** У контексті цієї статті поняття державного суверенітету буде розглядатись традиційно, тобто він розуміється як верховенство, самостійність, повнота і неподільність державної влади на своїй території та незалежність у міжнародних відносинах [5]. Отже говорячи про “суверенізацію” мова йде насамперед про розповсюдження державної влади. У даному разі така влада поширюватиметься на комп'ютерну мережу, її елементи, або на інші утворення, що можуть бути виділені для розповсюдження на них влади.

У цілому для підтримання функціонування мережі необхідні сервери (тобто технічні пристрої зберігання інформації), лінії зв'язку (які забезпечують зв'язок між ними) та засоби управління ( у т.ч. програмне забезпечення). Це спрощене розуміння, але для цілей дослідження правового регулювання воно в цілому відповідає розумінню комп'ютерної мережі на фізичному рівні, що розглядається технічними фахівцями [6, с. 9-13]. Сервери та лінії зв'язку знаходяться в будь-якому разі на території певної держави і на місце їх знаходження і буде розповсюджуватись суверенітет конкретної держави. Але говорячи про суверенізацію Інтернету в контексті державної політики або правового регулювання, мова йде про більш широке коло проблемних питань. Зокрема, серед узагальнених О.А. Барановим підходів до визначення Інтернету для цілей правового регулювання варто зупинитись на розумінні Інтернету як міжнародної

телекомунікаційної мережі загального користування, що призначена для обміну відомостями або як глобальної системи комунікацій, що є засобом інформаційного спілкування та доступу до інформації [1, с. 13].

Якщо відійти від фізичного рівня сприйняття Інтернету, то насамперед мова йде про сегментацію мережі, тобто намагання виокремити певні об'єкти (сегменти), які можливо розглядати як такі, на які розповсюджується державний суверенітет. Зазначена точка зору найбільш яскраво проявляється в дискусіях стосовно “Рунету” (або “Уанету”), тобто російського або українського сегментів Інтернету. Більш-менш зрозумілою є ситуація з доменними іменами, що відповідають національній (державній) приналежності (доменній зоні, у випадку України – це доменна зона “ua”). Адміністрування у цій сфері відповідно до вимог ст. 56 Закону України “Про телекомунікації” покладено на уповноважену організацію [7]. Водночас, адміністрування домену на сьогодні де-факто здійснює юридична особа приватного права, хоча у науковій літературі було звернуто увагу на неврегульованість цього питання ще з 2003 року, незважаючи на наявність розпорядження Кабінету Міністрів України з цього приводу [1, с. 30]. Реєстрація здійснюється цією юридичною особою відповідно до визначених нею Правил [8]. Принаймні адміністрування здійснюється юридичною особою українського права, тому національна приналежність домену конкретній країні не викликає сумнів.

В інших державах існує різна практика. Так, наприклад, Уряд Тувалу (острівної держави в Океанії) передав права адміністрування популярного домену “TV” практично з початку його існування різним компаніям з США [8]. У деяких країнах існує практика прямого адміністрування національного домену верхнього рівня державними органами (Албанія, Бангладеш, Барбадос, Бенін, Габон, Камбоджа, КНР, Малайзія, М'янма, Оман, Пакистан, Саудівська Аравія, Таджикистан та ін.), але в більшості випадків це здійснюється уповноваженими недержавними організаціями, у т.ч. компаніями-нерезидентами або науковими установами. Правила національної належності серверів (ресурсів), а також обмежень (для урядових, військових, освітніх, наукових, медичних тощо) установ встановлюються операторами відповідно до загальних вимог міжнародної організації ICANN. У більшості доменних зон не є обов'язковою належність особи – власника Інтернет-ресурсу (сайту) до резидентів країни, або фізичне знаходження серверів на їх території. Як правило, обмеження та вимоги у цій сфері відповідають загальній державній політиці у сфері телекомунікацій.

Ситуація з доменом Росії дещо відрізняється двома факторами. Згідно із роз'ясненням Федеральної антимонопольної служби Росії, що обговорювалось у спеціалізованій пресі на початку 2018 року, до так званого “Рунету” (російського сегменту Інтернету) пропонується відносити ресурси з доменними іменами “RU”, “SU” та “РФ” [10]. Доменне ім'я “SU” не входить до переліку географічних кодів ISO 3166-1, і тому не розглядається як національне згідно з вимогами ICANN. З початку 1990-х років його адміністрування здійснювалось різними російськими юридичними особами. Ототожнення з “Рунетом” відбувається із врахуванням того фактору, що більшість користувачів ідентифікує таке ім'я з колишнім Радянським Союзом, хоча його реєстрація і відбувалась після розпаду СРСР. Доменне ім'я “РФ” є так званім “кириличним” розширенням, тобто іменем, що засновано не на латинській, а іншій (у даному разі – кирилиці) писемності. На сьогодні в Інтернеті також вживаються домени, що засновані на китайській, корейській, арабській і тамільській писемності. Серед існуючих кириличних імен їх адміністрування здійснюється тими ж національними операторами, що адмініструють відповідний домен латиницею (Білорусь, Казахстан, Монголія, Сербія, Росія (у т.ч. домен “РУС”), Україна).

Але в Росії доволі часто відносять до “Рунету” (тобто російського сегменту Інтернету) фактично необмежене коло Інтернет-ресурсів, що містить контент російською мовою. З 2004 року під патронатом державних органів в Росії здійснюється нагородження “Премією Рунету”. Якщо проаналізувати перелік нагороджених з 2004 року то в основному це державні органи Росії, компанії в галузі телекомунікацій, засоби масової інформації, окремі особи, що є резидентами Росії. Хоча на початку відбувались нагородження міжнародних та іноземних компаній у сфері інформаційних технологій (Microsoft, Intel, Cisco Systems та ін.). За напрямком “Рунет за межами RU” нагороджувались різні організації, які діяли не у Росії. Таким чином, термін “Рунет” є доволі розпливчастим і може мати різні значення.

Позиція державних органів Росії у питаннях регуляції є більш конкретною. Виокремлення “Рунету” вважається недоцільним, а предмет державного впливу конкретизовано тим, що може бути врегульовано на “фізичному” рівні.

Питання “суверенізації” Інтернету (“Рунету”, російського сегменту, тощо) з’явилося останнім часом на порядку денному внаслідок низки законодавчих новацій у Росії.

Спочатку варто узагальнити існуючу в різних країнах практику державного регулювання використання комп’ютерних мереж (у т.ч. Інтернету). Прикладом державних крайнощів у цьому питанні є ситуація у Північній Кореї (КНДР). Вона може бути охарактеризована наступними факторами. Першим є існування загальної внутрішньої мережі користувачів у країні за відсутності її виходу безпосередньо в Інтернет. Тобто від самого початку в країні здійснювалась побудова внутрішньої комп’ютерної ізольованої мережі (Інтранету). Відповідно вона управлялась державними органами шляхами подібними до адміністрування внутрішньодержавної телефонної мережі. Адміністративним шляхом здійснювалась також ідентифікація конкретних абонентів, що використовували комп’ютерні мережі. Зазначені заходи розповсюджувались і на торгівлю індивідуальними засобами зв’язку (мобільні телефони, смартфони, і т.ін.) [11 – 13]. Окрім цього, електронно-обчислювальні машини використовують лише спеціально розроблене і контрольоване державою програмне забезпечення на рівні операційної системи (Red Star OS) [14]. Отже, усі зазначені заходи зумовлені однією метою – отриманням повного контролю за діяльністю особи, що використовує комп’ютерну техніку, за умови повного позбавлення її права на приватність. З точки зору забезпечення кібербезпеки, такі заходи можуть мати певну ефективність лише в умовах глобального контролю телекомунікацій, оскільки, наприклад операційна система Red Star на думку технічних фахівців є слабо захищеною від зовнішнього втручання та інших факторів, що ускладнюють її застосування [15]. Ефективно працювати зазначена система може лише в умовах закритої комп’ютерної мережі (Інтранет). На практиці повної закритості та підконтрольності комп’ютерних мереж не вдалося досягти навіть у КНДР з огляду на контрабанду технічних пристроїв (передусім смартфонів, планшетних комп’ютерів та флеш-накопичувачів) з КНР, що використовуються як засоби для перегляду кінофільмів, прослуховування музики. Окрім цього, в КНДР правоохоронні органи ведуть тривалу боротьбу з намаганнями побудови приватними особами “москітних мереж”, тобто мереж таких пристроїв з використанням не контрольованих державою каналів (wi-fi, Bluetooth, irDa та подібних технологій) [16], а також зі спробами використовувати мережі мобільного зв’язку КНР для доступу до Інтернету через такі пристрої в прикордонних зонах [17].

Загалом громадськими організаціями, що спеціалізуються на дослідженнях стану свободи Інтернету в різних країнах, основними аспектами державного впливу визнано

“перепони для доступу” до Інтернету, “обмеження контенту” та “порушення прав користувачів”. Усі зазначені аспекти взаємопов’язані. Як правило, державний вплив у цій сфері зумовлений метою контролю за діями громадян в інтересах держави. Тому в демократичних суспільствах рівень свободи Інтернету є вищим аніж в авторитарних. Декларовані підстави для обмежень, що зазначаються державними органами, можуть приховувати реальні їх цілі. Як правило, мова йде про боротьбу з тероризмом, злочинністю або ж із необхідністю забезпечення кібербезпеки. Відповідна риторика корелює із політичними гаслами щодо посилення державного впливу, введення обмежень прав і свобод людини для досягнення вищих цілей.

Слід зазначити, що “суверенізація” Інтернету набула досить широкого розповсюдження в аргументації на підтримку низки законодавчих новел у Російській Федерації. Насамперед мова йде про Федеральний Закон Російської Федерації “Про внесення змін до Федерального Закону “Про зв’язок” і Федерального Закону “Про інформацію, інформаційні технології і про захист інформації” від 01.05.2019 року № 90-ФЗ, що набуває чинності з 1 листопада 2019 року [18]. Основними законодавчими новаціями Закону є покладання додаткових обов’язків на операторів зв’язку щодо встановлення спеціального обладнання – технічних засобів протидії загрозам стійкості, безпеки і цілісності функціонування на території Російської Федерації мережі Інтернет. Зазначені технічні засоби є складовою системи централізованого управління мережею зв’язку загального користування. Таким чином законодавчий акт встановлює адміністративно-правові передумови створення та функціонування системи централізованого управління мережею Інтернет в межах Росії відповідним державним органом. Технічна реалізація зазначеного буде регламентована в подальшому на рівні підзаконних актів. Нова глава 7-1 Федерального Закону “Про зв’язок” присвячена відповідним заходам, спрямованим на забезпечення стійкості, безпеки і цілісності функціонування на території Російської Федерації мережі Інтернет. Координація заходів покладається на відповідний федеральний орган. Пряме централізоване управління має здійснюватись зазначеним органом в умовах “надзвичайних обставин”, які визначені вкрай широко – у випадку виникнення загроз стійкості, безпеки і цілісності функціонування мережі Інтернет.

Поняття “суверенітету” щодо Інтернету досить широко використовувалось на етапі підготовки та прийняття зазначеного Закону, оскільки законодавчі новації викликали чималу критику правозахисників. Обґрунтування прийняття Закону містилось в пояснювальній записці до законопроекту. На думку його авторів причиною прийняття Закону є агресивні дії з боку США, що нібито визначені у Стратегії національної кібербезпеки, а також необхідність забезпечення довгострокової та сталої роботи мережі Інтернет на території Росії. Для досягнення цієї мети і пропонується створити інфраструктуру, яка б мала змогу обмежити увесь трафік мережі шляхом контролю усіх точок доступу, а також за необхідності забезпечити використання мережевих ресурсів Росії в умовах відсутності зв’язку із Інтернетом [19]. Зрозуміло, що зазначені складові мети є технічними завданнями, а правовий шлях досягнення мети передбачає адміністративно-правове регулювання діяльності, у т.ч. покладання на суб’єктів господарської діяльності обов’язку встановлювати спеціальне технічне обладнання. Введення за необхідності централізованого управління за таких умов впливає із відповідних заходів, що визначаються цим Законом у межах повноважень державних органів.

Але слід зазначити, що “суверенізація” не означає встановлення централізованого управління Інтернетом. Загалом в міжнародному праві кібервійни зазначено наступне

ставлення до суверенітету в кіберпросторі. Перше правило Талліннського статуту (Tallinn Manual) щодо міжнародного права, яке може бути застосовано до кібервійни, визначає загальні підходи до суверенітету в кіберпросторі. Зокрема визначено, що держава може здійснювати контроль над кібер-інфраструктурою і діяльністю в межах своєї суверенної території [20, с. 25]. Тобто суверенітет держави щодо об'єктів, на які він розповсюджується, є похідним від суверенітету держави щодо певної території. Зазначене стосується і об'єктів кібер-інфраструктури. За таких умов держава дійсно має суверенні права щодо встановлення обмежень, у тому числі і у питанні доступу до мережі Інтернет на власній території. Питання можливого порушення суверенітету внаслідок проведення операцій в кіберпросторі (кібервійна), а також пріоритету прав людини у цьому контексті, що визначені міжнародно-правовими актами, є досить складними і комплексними, їх однозначне трактування є справою майбутнього, про що свідчить характер наукової дискусії в цьому напрямку [21, с. 211-212].

Таким чином, суверенне право держави мати контроль над об'єктами кібер-інфраструктури на своїй території під сумнів не ставиться. Але суверенітет не означає наявності права власності або необхідності розповсюдження на ці об'єкти прямого державного управління. Отже, зазначені законодавчі новели ніякої суверенізації не встановлюють. Мова йде лише про посилення державного регулювання певної сфери. Причини для такого посилення можуть бути різні, але у випадку Росії вони скоріше за все є політичними. Ефективність обраних заходів щодо протидії військовим операціям, які проводяться у кіберпросторі, зможуть оцінити відповідні технічні фахівці. Слід лише зазначити, що у Стратегії національної кібербезпеки США не передбачено проведення операцій в кіберпросторі, спрямованих на обмеження доступу до Інтернету будь-якої держави, але цілий розділ присвячений просуванню “американського впливу”. До числа цілей такого впливу Стратегія відносить забезпечення стійкості Інтернету та свободи Інтернету [22, с. 24]. Саме реалізації таких завдань фактично і протидіють заходи по встановленню централізованого управління використанням мережі Інтернет та його перетворення на територіально замкнену мережу (Інтранет). І саме такими вірогідно і були справжні цілі ухвалення в Росії законопроекту 608767-7.

### **Висновки.**

1. “Суверенізація Інтернету” загалом є політичним терміном, який відображає певні тенденції у державній політиці окремих країн. Зазначені тенденції, як правило, мають внутрішній характер, тісно пов'язані із існуючим в державі політичним режимом і відображають його характер. У правовому значенні поняття суверенітету може використовуватись як термін міжнародного права.

2. Загальне розуміння суверенітету передбачає суверенітет держави над об'єктами (у тому числі кібер-інфраструктури) за принципом території, на яку розповсюджується суверенітет. При цьому держава має право контролювати доступ до мережі та діяльність у ній відповідно до вимог законодавства, у тому числі міжнародно-правових актів щодо захисту прав людини.

3. Адміністративна діяльність щодо державного регулювання у сфері телекомунікацій регламентується національним законодавством відповідної держави. Технічні вимоги стосовно організації доступу та використання мережі Інтернет забезпечуються державою шляхом встановлення нормативно-правових вимог. Водночас питання розповсюдження суверенітету та сприйняття суверенітету (національної приналежності) щодо певних ресурсів може бути значно ускладнено з огляду на глобальний характер мережі Інтернет.

4. Перспективними у цьому контексті є подальші наукові дослідження стосовно визначення підстав для державних обмежень, що реалізуються у кіберпросторі, визначення гарантій забезпечення прав і свобод людини, які пов'язані з використанням мережі Інтернет та пошуку балансу між необхідністю реалізації цілей держави і правами людини.

### Використана література

1. Баранов А.А. Інтернет: объект правоотношений и предмет регулирования: монография. Київ: Ред.журн. "Право України"; Харків: Право, 2013. 144 с.
2. Динис Г.Г. Міжнародно-правові концепції глобального права, права Інтернету або кіберправа та трансформації міжнародного права. *Часопис Київського університету права*. 2011. № 2. С. 279-285.
3. Рассолов И.М. Право и Интернет: теоретические проблемы. 2-е изд. Москва: Норма, 2009. 383 с.
4. Серго А. Интернет и право. Москва: Бестселлер, 2003. 272 с.
5. Декларація про державний суверенітет України: Закон України від 16.07.90 р. URL: <https://zakon.rada.gov.ua/laws/show/55-12> (дата звернення 21.04.2019).
6. Комагоров В.П. Архитектура сетей и систем телекоммуникаций: учебное пособие. Томск: Изд-во Томского политехн. ун-та, 2011. 154 с.
7. Про телекомунікації: Закон України від 18.11.03 р. № 1280-IV. Дата оновлення: 04.11.2018. URL: <https://zakon.rada.gov.ua/laws/show/1280-15/stru> (дата звернення: 01.05.2019).
8. Правила домену UA. URL: <http://www.domenua.com.ua/uapolicy-ukr.php> (дата звернення: 01.05.2019).
9. Berkens M. Verisign Renews Contract With Tuvalu To Run.TV Registry Through 2021. *The Domains.com*. February, 25, 2015. URL: <https://www.thedomains.com/2012/02/25> (дата звернення: 01.05.2019).
10. Соболев С., Истомина М. Не наш YouTube: почему ФАС отказалась считать видеосервис частью Рунета? *РБК: Технологии*. 16.05.2018. URL: [https://www.rbc.ru/technology\\_and\\_media/16/05/2018/5afae6119a794735ac623eab](https://www.rbc.ru/technology_and_media/16/05/2018/5afae6119a794735ac623eab) (дата звернення: 01.05.2019).
11. Mansourov A. North Korea on the Cusp of Digital Transformation: Nautilus Institute Special Report. October, 2011. URL: [http://www.nautilus.org/wp-content/uploads/2011/12/DPRK\\_Digital\\_Transformation.pdf](http://www.nautilus.org/wp-content/uploads/2011/12/DPRK_Digital_Transformation.pdf) (дата звернення: 01.05.2019).
12. Komiyama K. The Information Technology Industry in North Korea. *Keio University Global Research Institute Working Papers*. 2019. Vol. 4. URL: <http://www.kgri.keio.ac.jp/en/docs/S180620190226.pdf> (дата звернення: 01.05.2019).
13. Гогилашвили Е. Как сидят в Интернете в Северной Корее? *BIT.UA*. 10.09.2018. URL: <https://lab.bit.ua/2018/09/north-korea-intranet/> (дата звернення: 01.05.2019).
14. Schiess N. Governmental Control of Digital Media Distribution in North Korea: Surveillance and Censorship on Modern Consumer Devices. *DPRK Tech Info*. 2017. May. URL: [https://dprktech.info/media/governmental\\_control\\_of\\_digital\\_media\\_distribution\\_in\\_north\\_korea-nschiess.pdf](https://dprktech.info/media/governmental_control_of_digital_media_distribution_in_north_korea-nschiess.pdf) (дата звернення: 01.05.2019).
15. Tushar S.D. Now The Super-Secure Red Star OS Can Be Hacked With Just A Link. *TechViral*. December, 6.2016. URL: <https://techviral.net/now-red-star-os-can-be-hacked> (дата звернення: 01.05.2019).
16. Choe Sang-Hun. North Koreans Rely On Smuggled Cellphones to Connect to the Outside World. *The New York Times*. March, 26, 2016. URL: <https://www.nytimes.com/2016/03/27/world/asia/north-korea-china-mobile-phones.html> (дата звернення: 01.05.2019).
17. Kim Joon-Ho, Lee Jiin-Jun, Lipes J. North Korea Shuts Down Illegal Cell Phone Access to Chinese Networks. *RFA*. 20.09.2018. URL: <https://www.rfa.org/english/news/korea/cellphones-09202018161614.html> (дата звернення: 01.05.2019).



18. О внесении изменений в Федеральный Закон “О связи” и Федеральный Закон “Об информации, информационных технологиях и защите информации”: Федеральный Закон Российской Федерации от 01.05.19 г. № 90-ФЗ. URL: <http://publication.pravo.gov.ru/File/GetFile/0001201905010025?type=pdf> (дата звернення: 01.05.2019).

19. О внесении изменений в Федеральный Закон “О связи” и Федеральный Закон “Об информации, информационных технологиях и защите информации”: пояснительная записка к законопроекту № 608767-7 от 14.12.18 г. URL: <https://sozd.duma.gov.ru/bill/608767-7> (дата звернення: 01.05.2019).

20. Tallinn Manual on The International Law applicable to Cyber Warfare/ Ed. Michael N. Schmitt. N.Y.: Cambridge University Press, 2013. 215 p.

21. Corn Gary, Taylor Robert. Sovereignty in the Age of Cyber. *AJIL Unbound*. 2017. Vol. 111. P. 207-212.

22. National Cyber Strategy of the USA. September, 2018. URL: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf> (дата звернення: 01.05.2019).

~~~~~ \* \* \* ~~~~~

УДК 343.9:343.346.8:004

**ГРЕБЕНЮК М.В.**, кандидат юридичних наук, доцент,  
Міжвідомчий науково-дослідний центр з проблем боротьби  
з організованою злочинністю при РНБО України  
**ЛЕОНОВ Б.Д.**, доктор юридичних наук, старший науковий співробітник,  
Національна академія Служби безпеки України

## **ПРОБЛЕМИ ПРОТИДІЇ ПОШИРЕННЮ ДЕСТРУКТИВНОЇ ПРОПАГАНДИ ТА ДЕЗІНФОРМАЦІЇ НАПЕРЕДОДНІ ВИБОРІВ: АНАЛІЗ ДОСВІДУ ЄС**

**Анотація.** У статті аналізується досвід ЄС із забезпечення протидії деструктивній пропаганді та дезінформації під час електоральних процесів. Висвітлюються проблеми боротьби з деструктивною пропагандою у вітчизняному інформаційному просторі. Аналізуються законодавчі ініціативи окремих країн ЄС у сфері інформаційного забезпечення протидії деструктивній пропаганді та дезінформації.

**Ключові слова:** протидія, інформаційна безпека, електоральні процеси, деструктивна пропаганда, дезінформація.

**Аннотация.** В статье анализируется опыт ЕС в обеспечении противодействия деструктивной пропаганды и дезинформации во время электоральных процессов. Освещаются проблемы борьбы с деструктивной пропагандой в отечественном информационном пространстве. Анализируются законодательные инициативы отдельных стран ЕС в области информационного обеспечения противодействия деструктивной пропаганды и дезинформации.

**Ключевые слова:** противодействие, информационная безопасность, электоральные процессы, деструктивная пропаганда, дезинформация.

**Summary.** The article analyzes the EU experience in providing counteraction to destructive propaganda and disinformation during electoral processes. The issue of combating destructive propaganda in the domestic information space is highlighted. The legislative initiatives of individual EU countries in the field of informational counteraction to destructive propaganda and disinformation are analyzed.

**Keywords:** counteraction, information security, electoral processes, destructive propaganda, disinformation.

**Постановка проблеми.** Напередодні проведення парламентських виборів в Україні у 2019 році тематика боротьби з пропагандою у соціальних мережах набуває надзвичайної актуальності з огляду на загрозу втручання РФ в електоральні процеси, метою якого є дестабілізація політичної ситуації. Невипадково, протягом останнього часу відзначається надмірне посилення протистояння між країнами Заходу та РФ, перш за все, в інформаційній сфері, що пов'язано з активізацією намагань останньої здійснити вплив на геополітику ЄС у вигідному для себе напрямку.

Загалом можна констатувати, що більшість інформаційних кампаній з дезінформації проводяться спецслужбами РФ проти держав Євросоюзу шляхом масованих кібератак на об'єкти критичної інфраструктури, впливу на політичні дебати, створення конфліктних контентів з метою розпалювання релігійної та іншої ворожнечі в суспільстві.

**Результати аналізу наукових публікацій.** В основу написання цієї статті покладено аналіз актів ЄС, а також чинного інформаційного законодавства окремих зарубіжних країн, які стосуються предмету дослідження, а також творчий доробок

відомих вчених, зокрема В. Брижка та М. Швеця [1], В. Горбуліна [2], В. Гурковського [3], О. Дзюбаня та В. Пилипчука [4], Д. Ланде [5], В. Панченко [6], В. Фурашева [7] та ін.

Однак в науковій літературі відсутні системні дослідження, присвячені протидії поширенню деструктивної пропаганди та дезінформації напередодні виборів.

**Метою статті** є визначення позитивного досвіду країн ЄС та РФ у сфері протидії деструктивній пропаганді та дезінформації під час електоральних процесів для його можливого запозичення та використання правоохоронними органами України.

**Виклад основного матеріалу.** В державах-членах Європейських Співтовариств відкрито декларують, що саме РФ застосовуватиме дезінформацію та пропаганду для того, щоб змінити результати виборів. Керівництво Євросоюзу прагне робити поступальні кроки для запобігання поширенню дезінформації, яка може негативно вплинути на діяльність багатьох інституцій Євросоюзу. Ще у 2017 році в ЄС був створений сайт [euvdisinfo.eu](http://euvdisinfo.eu) для боротьби з дезінформацією з боку РФ [8], де міститься згадка про те, що він створений в рамках кампанії “ЄС проти дезінформації”, спрямованої на “поліпшення прогнозування, розгляду та реагування на прокремлівську дезінформацію”.

Сьогодні ж стратегічним завданням є оновлення формату ЄС у частині протидії російській дезінформації. Йдеться про протидію дезінформації, антидемократичній пропаганді та “фейкам”. Ця діяльність є частиною безпекової стратегії ЄС, оскільки непоодинокими стають випадки стороннього впливу на політику, вибори в окремих державах ЄС шляхом застосування різного роду маніпуляцій та спотворення правдивої інформації. Для цього застосовуються значні ресурси, які є більшими за ресурси, що виділяються для захисту у відповідних інституціях країн ЄС. Це зумовлює потребу у розробці національних стратегій на рівні кожної з 27 держав-членів ЄС, зміст яких має охоплювати інструменти протидії деструктивній пропаганді та дезінформації.

Аналіз останніх подій свідчить про послідовну політику ЄС у напрямку запобігання дезінформації та деструктивній пропаганді.

25 квітня 2018 року ПАРЕ ухвалила резолюцію про протидію російській пропаганді на рівні ЄС [9], згідно з якою державам-членам Ради Європи рекомендується створити органи (observatories) для відстеження фактів поширення дезінформації і фейків російського походження.

21 січня 2019 р. Рада ЄС (на рівні міністрів закордонних справ) обговорила питання реалізації плану дій проти дезінформації, який був представлений Єврокомісією ще в грудні 2018 р. як пріоритетний з урахуванням виборів до Європарламенту. Головну увагу було зосереджено на зовнішніх аспектах плану дій проти дезінформації, ідентифікації її джерел, посиленні відповідних ресурсів ЄС шляхом обміну досвідом між країнами-членами ЄС та його інституціями, вироблення інструментів спільної протидії дезінформаційній кампанії [10].

Відповідно до нового плану Єврокомісія збільшила бюджет групи зовнішньополітичної служби ЄС із стратегічних комунікацій, яка була створена для боротьби з дезінформацією, насамперед з боку РФ. Для забезпечення діяльності цієї групи у 2019 році планується виділити 5 млн. Євро, тоді як в 2018 році її бюджет складав лише 1,9 млн. Євро. Крім того, план боротьби із дезінформацією та пропагандою передбачає створення в установах держав-членів ЄС спеціальної системи швидкого оповіщення, що працюватиме для спрощення обміну даними та оцінками кампаній дезінформації, а також повідомлятиме про загрози дезінформації в режимі реального часу. В Єврокомісії також розглядають питання вжиття додаткових превентивних заходів з метою забезпечення повної прозорості електоральних процесів та їх кінцевих результатів для держав-членів ЄС.

З огляду на це, Європейський Союз закликає світові он-лайн-платформи, такі як Facebook, Twitter, Google посилити боротьбу з дезінформацією напередодні європейських виборів. Вони будуть зобов'язані забезпечити прозорість політичної реклами, активізацію зусиль щодо закриття фейкових аккаунтів, маркувати повідомлення, які автоматично розповсюджуються ботами, та співпрацювати з академічними дослідницькими установами, які займаються перевіркою фактів виявлення дезінформації. Із січня по травень поточного року он-лайн-платформи повинні будуть щомісячно звітувати перед Єврокомісією, яка у свою чергу, готуватиме звіти для оприлюднення в ЄС [10].

29 січня 2019 р. Єврокомісар з цифрової економіки і суспільства М. Габріель під час презентації першого звіту щодо усунення політичної дезінформації напередодні виборів повідомила, що боротьба з дезінформацією і пропагандою у співпраці ЄС з Facebook, Google чи Twitter має низку недоліків. Серед недоліків було виявлено те, що:

- 1) дезінформація не знає кордонів, тому потрібен загальноєвропейський підхід, згідно з яким співпрацювати в цій сфері повинні всі країни ЄС;
- 2) має місце зволікання з реакцією, спрямованою на запобігання дезінформації, тобто важливо, щоб плани були реалізовані досить оперативно;
- 3) потрібно розширити “поле дій” у сфері прозорості в мережі Інтернет з метою виявлення реклами, яка переслідує приховані політичні цілі [11].

Оприлюднений план боротьби із дезінформацією та пропагандою мотивує соцмережі до розробки нових правил, відповідно до яких під час європейських виборів політична реклама повинна бути схвалена соцмережею, а також містити чіткий банер з назвою її замовника. Тобто нові механізми мають поширюватися не тільки на рекламу для кандидатів або політичних партій, а й на заполітизовані питання в суспільстві, наприклад, такі як, імміграція. Згадані інструменти передбачають попередню спеціальну авторизацію для рекламодавців, а також створення архіву реклами, де можна буде отримати інформацію про тих користувачів, які її переглядали, зокрема їхній вік, стать і місце розташування, а також дані про витрати на рекламу. Дані з такої бібліотеки політичної реклами зберігатимуться й будуть у загальному доступі протягом 7 років [12].

Заслугує на увагу те, що Facebook має намір:

- а) запровадити функцію, завдяки якій користувачі зможуть отримувати детальну інформацію з приводу посилань у новинній стрічці (ця інформація буде вбудована під посиланням, опція називатиметься “Про цю статтю”);
- б) скоротити кількість посилань із заголовками, що вводять в оману (клікбейтами);
- в) посилити перевірку викладених у публікаціях фактів за допомогою оновлення відповідної програми (нині вона може перевіряти контент 16-ма мовами); створити спеціальний штаб для запобігання поширенню недостовірної інформації, напередодні виборів. Як стверджують фахівці, нові механізми будуть доступні наприкінці березня і допоможуть “зробити політичну рекламу у Facebook більш прозорою” [13].

На думку Єврокомісії, Facebook має використовувати свої інструменти для розширення прав та можливостей споживачів та співпраці з органами та спеціалізованими дослідницькими установами ЄС для перевірки виявлених фактів.

Водночас, представники мережі Facebook вважають, що відносно політичної активності на Інтернет-платформах слід додержуватися “золотої середини”, а стосовно протидії дезінформації, фейкам й деструктивній пропаганді слід вживати превентивних заходів. При цьому представники компанії Facebook застерігають від надмірно суворих вказівок щодо видалення політично чутливого контенту, адже не можна, на їх думку, плутати ненависницькі пости з оціночними висловлюваннями окремих політиків, які комусь не до вподоби [14].

Політика боротьби з дезінформацією у державах-членах ЄС дедалі активніше реалізується. Фіксуються непоодинокі спроби боротьби з дезінформацією навіть за допомогою штучного інтелекту. Так, литовські програмісти навчили штучний інтелект шукати фейки в Інтернет. Спеціальну комп'ютерну програму, яка вже повноформатно працює, ще у вересні 2018 року презентували в Брюсселі оперативній робочій групі зі стратегічних комунікацій "East StratCom" та представникам Єврокомісії [15].

В основі технології знаходиться ідея, що комп'ютерні алгоритми здатні здійснювати пошук в контенті певних меседжів та наративів. Ця система щодня проводить моніторинг більше ніж 10 тисяч матеріалів з 500 литовських та російських Інтернет-доменів. У майбутньому вона зможе збільшити свою потужність до двохсот тисяч текстів на день. Нова розробка поки не потребує допомоги людей: комп'ютерні алгоритми шукають в Інтернеті підозрілі матеріали, а потім їх перевіряють волонтери та спеціалісти – "мережеві ельфи", які можуть позначити викривлення фактів чи неправдиву інформацію. Розробники сподіваються, якщо їхня програма доведе свою ефективність – у майбутньому вона може стати основою для загальноєвропейської платформи боротьби з фейками. Також політичне керівництво Литви закликає партнерів по ЄС посилити боротьбу з російською пропагандою, оскільки Європа повинна ретельніше готуватися до інформаційної війни з РФ. У 2018 році в Литві за підозрою в шпигунстві на користь Росії затримали декількох осіб, які виконували завдання російської розвідки і намагалися за допомогою своїх дій і контактів з позапарламентськими партіями впливати на політичні процеси в країні [15].

Прояви російської інформаційної пропаганди фіксують правоохоронні органи Франції, у зв'язку з чим у цій країні підготовлено проект закону з протидії фейкам на виборах. Відзначається, що минулорічна президентська кампанія у Франції ознаменувалася втручанням російських медіа, кібератаками та й загалом була "брудною" за французькими стандартами. Враховуючи масштаби загроз в інформаційній сфері, у "Стратегічному огляді" (*Revue stratégique*) Франції задекларовано, що питання дезінформації та її впливу стають одними з безпекових пріоритетів. Отже, у Франції на законодавчому рівні посилюються заходи з контролю мас-медіа, особливо напередодні виборів. Також у Франції державному регулятору надаватиметься право анулювати ліцензії телеканалів з метою протидії централізованій російській пропаганді. Це стосується також й блокування контенту в соціальних мережах, що стане додатковим, ще потужнішим інструментом протидії російському впливу [16].

У Фінляндії у 2017 році розпочав роботу центр по боротьбі з гібридними загрозами. Серед гібридних загроз засновники центру виділяють, серед іншого, поширення неправдивої інформації, атаки проти інформаційних систем, а також інші види атак за допомогою сучасних технологій [17].

Восени 2018 року у США на протидію пропаганди з боку РФ, Китаю та Ірану було виділено 40 мільйонів доларів, які мали бути спрямовані на виявлення дезінформації та взаємодію з регіональними соцмедіа, громадськими організаціями та пресою. Зазначається, що виділені кошти, зокрема, призначені для: впровадження технологій з раннього виявлення дезінформації; аналізу закордонної аудиторії, найбільш вразливої до її впливу; розвитку ефективної взаємодії із впливовими гравцями на ринку регіональних соціальних медіа, неурядовими організаціями та журналістами [18].

На саміті Великої сімки (G7), який відбувся влітку 2018 року у Канаді, країни-учасниці дійшли згоди щодо розробки нової системи захисту від поширення деструктивної пропаганди. Зокрема, країни G7 вирішили розробити систему захисту від

пропаганди і маніпуляцій за допомогою “Механізму швидкого реагування”, який покликаний скоординувати заходи з боротьби з деструктивною пропагандою. Очікується, що це дозволить оперативно і скоординовано припинити маніпуляції, пропаганду, а також інші “неприпустимі дії” і спроби дестабілізації з боку цієї країни. За допомогою нової системи захисту держави-члени G7 планують аналізувати дані про подібні інформаційні атаки, а також обмінюватися цими даними. Передбачається, що “в ідеальному випадку” відповіддю на атаку має стати скоординована реакція, яка може бути у вигляді відповідної кампанії або санкцій [19].

У внутрішній політиці інформаційна війна проявляється пропагандистським протистоянням політичних опонентів і агітацією, хоча нерідко набуває складнішого комплексно-маніпулятивного змісту ігор та інтриг, коли в хід ідуть будь-які доводи, звинувачення, компромат (зі скандалами), приховання від громадськості закулісних операцій тощо [1, с. 54].

У свою чергу, фахівці мають обґрунтовані підстави прогнозувати, що Росія втручатиметься не лише у вибори до Європарламенту, а й у виборчі процеси в Україні, Молдові та Польщі [20]. На жаль, як у світі, так і в Україні практично немає законодавства, яке б сприяло ефективній протидії гібридному впливу на виборчий процес, у зв'язку з чим зупинити маніпуляції виборами – надзвичайно складно. За таких умов для України важливими є питання забезпечення захищеності виборчих процесів від ворожих впливів, а з огляду на такий стан справ, важливим є опанування та вивчення європейського досвіду у цій сфері.

З цією метою 23 січня 2019 року керівництво Міністерства інформаційної політики України обговорило з представниками компанії Facebook питання співпраці у сфері інформаційної безпеки. За результатами домовленостей було схвалено рішення про те, що з 1 лютого 2019 року Facebook обмежує політичну рекламу для українських користувачів на час виборів. Забороняють, наприклад, розміщення передвиборчої реклами з-за кордону, щоб попередити зовнішнє втручання. Передвиборчою у компанії вважають ту рекламу, що стосується політиків, партій, мобілізації виборців та/або прагнення утримати виборців від участі у виборах. Політичні слогани і партійна символіка також охоплюються змістом такої компанії. Зазначені заходи є лише частиною нової політики компанії, метою якої є запобігання іноземному втручання у вибори та дезінформації на сторінках користувачів найбільшої світової соцмережі. У Facebook не стали коментувати, наскільки високою є загроза втручання у вибори в Україні. При цьому речник компанії пояснив, що можливість закордонного втручання є одним із факторів, який береться до уваги при плануванні особливої політики щодо певної країни, у якій наближаються вибори [21].

На думку західних експертів, поширення й розвиток інформаційно-комунікаційних технологій можуть підняти демократичні суспільства до більш високого рівня прозорості, вільного й миттєвого доступу до якісної інформації [20]. Натомість, інформаційний “бруд”, фейки та навмисно викривлені факти, які поширюють, скажімо, російські урядові ЗМІ та “фабрики тролів”, негативно впливають на суспільну думку. Тому розробка зброї проти фейків – справа нагальна як в Україні, так і в усьому світі, особливо напередодні виборів.

На думку керівника технологічного інкубатора “Google Jigsaw” Дж. Коена, в Україні відбувається дезінформаційна війна на трьох фронтах: дезінформаційні атаки, спрямовані на політичну систему, дезінформаційні атаки, спрямовані на порушення відносин України з її союзниками; інформаційні атаки, спрямовані на підтримку воєнних операцій на сході країни та в інших місцях [20].

У Комітеті виборців України також наголошують, що у період виборчої кампанії використання російських соцмереж як інформаційних джерел про діяльність та політичну позицію кандидатів суттєво збільшує ризики кіберпровокацій та дезінформації щодо суб'єктів виборчого процесу. З точки зору експертів Комітету виборців України, першочерговою проблемою залишається те, що окремі політичні сили продовжують використовувати російські соцмережі для поширення офіційної інформації про свої політичні партії [20].

Серед основних об'єктів протиправних посягань в інформаційній сфері виділяються інформаційно-телекомунікаційні системи органів державної влади України (у першу чергу МЗС, ЦВК, ДПС та МО України), державні реєстри та бази даних, а також автоматизовані системи управління технологічними процесами об'єктів критичної інфраструктури енергетичного, транспортного і фінансового секторів.

### **Висновки.**

У ЄС значна увага приділяється розробці та впровадженню ефективних механізмів протидії деструктивній пропаганді та дезінформації, особливо напередодні виборчих процесів, що передбачає модернізацію європейської стратегії запобігання інформаційному впливу з боку РФ.

Очікується, що у найближчій перспективі основною формою здійснення протиправного кібервпливу будуть цілеспрямовані довгострокові кібероперації (APT-атаки), які реалізовуватимуться шляхом застосування моделі cyber kill-chain, зміст якої передбачає проведення кібератаки у декілька етапів: сканування системи з метою виявлення її вразливостей; застосування спеціального програмного забезпечення (експлойту) або методів соціальної інженерії для проникнення в систему; інсталяція шкідливого програмного забезпечення для віддаленого управління системою; безпосередня крадіжка або модифікація даних, блокування роботи системи тощо. На кінцевому етапі зловмисником вживаються заходи щодо знищення слідів своєї протиправної діяльності.

До чинників, що негативно впливають на стан протидії кіберзлочинності, слід віднести: неповну імплементацію у національне законодавство положень Конвенції Ради Європи "Про кіберзлочинність" щодо обов'язкового зберігання та надання операторами та провайдерами телекомунікацій на вимогу правоохоронних органів інформації, необхідної для розслідування кіберзлочинів; використання провайдерами телекомунікаційних послуг механізму перетворення мережевих адрес за технологією NAT (Network Address Translation) без застосування механізмів логування, що ускладнює процес ідентифікації абонентів; використання зловмисниками Інтернет-сервісів та цифрових технологій, а також окремих послуг, що надають провайдери телекомунікацій та хостери, які унеможливають ідентифікацію злочинця або отримання іншої інформації, необхідної для розкриття злочину (використання методів TOR та I2P, криптовалют, виділених комунікаційних серверів тощо).

Разом з цим, доцільним вбачається активізація зусиль держави за такими напрямками: вжиття заходів з виявлення, запобігання та припинення спроб представників громадсько-політичних і релігійних об'єднань (насамперед, проросійських) політизувати та радикалізувати свою діяльність за підтримки закордонних центрів, інспірувати сепаратистські настрої та прояви релігійної ворожнечі серед етнічних громад, у тому числі й з використанням соціальних мереж, що може спричинити дестабілізацію суспільно-політичної обстановки, особливо у регіонах; вжиття профілактичних заходів, спрямованих на виявлення і недопущення використання закордонними недержавними організаціями та їх функціонерами можливостей вітчизняних ЗМІ, ресурсів мережі Інтернет, представників

мас-медійних громадських організацій та інших фахових об'єднань для створення механізмів впливу, у т.ч. фінансових, на вітчизняну інформаційну сферу, суспільно-політичні процеси, здійснення дискредитації діяльності органів державної влади, а також проведення антиукраїнських інформаційних акцій.

Одним з можливих чинників, що мінімізує негативні прояви пропаганди й дезінформації, є формування медійної освіти населення та розвиток якісної журналістики. Саме популяризація високоякісної незалежної журналістики дозволить зміцнити медійний простір, посилити співпрацю з державними ЗМІ. Журналісти і ЗМІ мають бути залучені до процесу ухвалення рішень, покликаних боротися з пропагандою та “фейками”.

### Використана література

1. Брижко В.М., Швець М.Я. Є-боротьба в інформаційних війнах та інформаційне право: монографія. Київ: НДЦПІ АПрН України, 2007. 234 с.
2. Горбулін В.П. “Гібридна війна” як ключовий інструмент російської геостратегії реваншу. *Стратегічні пріоритети*. 2014. № 4. С. 5-12.
3. Гурковський В. Механізми використання дезінформації в умовах російської гібридної агресії. *Освіта регіону*. URL: <http://social-science.com.ua/article/1393> (дата звернення: 12.02.2019).
4. Дзьобань О.П., Пилипчук В.Г. Інформаційне насильство та безпека: світоглядно-правові аспекти: монографія/ за заг. ред. проф. В.Г. Пилипчука. Харків: Майдан, 2011. 244 с.
5. Ланде Д.В., Бойченко А.В. Сценарний підхід при дослідженні контенту та структури соціальних мереж. *Правова інформатика*. № 1(45)/2015. С. 3-8.
6. Панченко В.М. Інформаційні операції в асиметричній війні Росії проти України. *Інформація і право*. № 3(12)/2014. С. 13-16.
7. Фурашев В.М. Питання шляхів протидії деструктивної пропаганди: матеріали науково-практичної конференції *Деструктивна пропаганда: шляхи протидії та проблеми відповідальності*, м. Київ, 21 травня 2015 р. Київ: ТОВ “ІВА”, 2015. С. 35-38.
8. В ЄС запустили новий сайт для протидії пропаганді Кремля. URL: <https://www.eurointegration.com.ua/news/2017/09/12/7070857> (дата звернення: 12.02.2019).
9. ПАРЕ прийняла резолюцію про протидію російській пропаганді. URL: <https://www.eurointegration.com.ua/news/2018/04/25/7080993> (дата звернення: 01.03.2019).
10. ЄС чекає від міністрів порад, як запобігати дезінформації перед виборами до Європарламенту. URL: <https://www.radiosvoboda.org/a/news-mogherini-propaganda-fake-news/29721836.html> (дата звернення: 27.02.2019).
11. В ЄС назвали п'ять недоліків своєї боротьби з фейками і пропагандою. URL: <https://www.radiosvoboda.org/a/news-eu-borotba-fake/29739793.html> (дата звернення: 27.02.2019).
12. Facebook зберігатиме на серверах політрекламу і дані про замовника сім років. URL: <https://www.ukrinform.ua/rubric-technology/2628698-facebook-zberigatime-na-serverah-politreklamu-i-dani-pro-zamovnika-sim-rokiv.html> (дата звернення: 27.02.2019).
13. Facebook обіцяє запобігти втручанню на виборах в Європарламент. URL: [www.ukrinform.ua/rubric-technology/2628926-facebook-obicae-zapobigti-vtrucannu-na-viborah-v-evroparlament.html](http://www.ukrinform.ua/rubric-technology/2628926-facebook-obicae-zapobigti-vtrucannu-na-viborah-v-evroparlament.html) (дата звернення: 01.03.2019).
14. Правила поведінки у Facebook, або як убезпечити свої персональні дані в соціальних мережах. URL: <http://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/pravila-povedinki-u-facebook-abo-yak-ubezpechiti-svoyi-personalni-dani-v-socialnih-merezhah.html> (дата звернення: 27.02.2019).
15. Литва закликала партнерів по ЄС посилити боротьбу з російською пропагандою. URL: <https://www.dw.com/uk> (дата звернення: 07.03.2019).
16. Якщо поглянути на Францію, то вона готує новий закон для протидії фейкам на виборах. Пропаганду забанять у Google. URL: <https://www.eurointegration.com.ua/articles/2018/03/20/7079007> (дата звернення: 09.03.2019).



17. У Фінляндії розпочав роботу центр по боротьбі з гібридними загрозами. URL: <https://dt.ua/WORLD/u-finlyandiyi-rozpochav-robotu-centr-po-borotbi-z-gibridnimi-zagroзами-253391.html> (дата звернення: 10.03.2019).

18. Розвідка США виявила спробу втручання РФ, Китаю та Ірану у вибори до Конгресу. URL: <https://glavcom.ua/world/observe/rozvidka-ssha-viyavila-sprobu-vtruchannya-rf-kitayu-ta-iranu-u-vibori-do-kongresu-555334.html> (дата звернення: 10.03.2019).

19. На саміті Великої сімки (G7) в Канаді влітку 2018 року. URL: <https://ukr.segodnya.ua/politics/sammit-g7-v-kanade-es-i-ssha-na-poroge-torgovoy-voyny-ili-v-shage-ot-primireniya-1144339.html> (дата звернення: 10.03.2019).

20. Протидія пропаганді та дезінформації напередодні виборів до Європейського парламенту. URL: [http://nbuviap.gov.ua/index.php?option=com\\_content&view=article&id=4131:protidiya-propagandi-ta-dezinformatsiji-naperedodni-viboriv-do-evropejskogo-parlamentu-2&catid=71&Itemid=382](http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=4131:protidiya-propagandi-ta-dezinformatsiji-naperedodni-viboriv-do-evropejskogo-parlamentu-2&catid=71&Itemid=382) (дата звернення: 06.03.2019).

21. МІП і Facebook обговорили протидію втручання у виборчі процеси. URL: <https://mir.gov.ua/news/2920.html> (дата звернення: 10.03.2019).

~~~~~ \* \* \* ~~~~~

УДК 351.746:007

**ГУЦАЛЮК М.В.,** доктор філософії (Ph.D.) з юридичних наук, доцент, с.н.с.,  
провідний науковий співробітник Міжвідомчого центру з проблем  
боротьби з організованою злочинністю при РНБО України

## **ОЦІНКА РЕАЛІЗАЦІЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ З УРАХУВАННЯМ ДОСВІДУ ЄВРОПЕЙСЬКИХ І СВІТОВИХ ПРАКТИК**

**Анотація.** У статті аналізується міжнародний досвід проведення оцінки Стратегії кібербезпеки. Акцентується увага на необхідності проведення такої оцінки Стратегії кібербезпеки України.

**Ключові слова:** кібербезпека, кіберзлочинність, критерії оцінки, Стратегія кібербезпеки, критична інфраструктура.

**Summary.** The article analyses the international experience of conducting an assessment of the Cybersecurity Strategy. The emphasis is placed on the need for such an assessment of the Cybersecurity Strategy of Ukraine.

**Keywords:** cyber security, cybercrime, evaluation criteria, Cybersecurity strategy, critical infrastructure.

**Аннотация.** В статье анализируется международный опыт проведения оценки Стратегии кибербезопасности. Акцентируется внимание на необходимости проведения такой оценки Стратегии кибербезопасности Украины.

**Ключевые слова:** кибербезопасность, киберпреступность, критерии оценки, Стратегия кибербезопасности, критическая инфраструктура.

**Постановка проблеми.** Після потужних кібератак на об'єкти критичної інфраструктури України з 2014 року значно активізувалася діяльність урядових інституцій щодо захисту кіберпростору. Координуючу роль у цих процесах відіграла Рада національної безпеки і оборони України, рішенням якої було схвалено, а в подальшому введено в дію Указом Президента України від 15 березня 2016 року № 96/2016 Стратегію кібербезпеки України. У Стратегії визначені загрози кібербезпеці, Національна система кібербезпеки та основні суб'єкти забезпечення кібербезпеки, а також пріоритети та напрями забезпечення кібербезпеки України [1].

Водночас у зв'язку з бурхливим розвитком інформаційних технологій та широким використанням хмарних сервісів, Інтернету речей, штучного інтелекту тощо, з'явилися нові види кіберзагроз, які здатні негативно впливати на стан кібербезпеки держави. У 2017 році був прийнятий Закон України "Про основні засади забезпечення кібербезпеки України" [2], який набрав чинності 9 травня 2018 року та став важливим етапом створення правових та організаційних основ забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, визначення основних цілей, напрямів та принципів державної політики у сфері кібербезпеки. Разом з тим багато питань у сфері кібербезпеки, у тому числі стратегічних, залишаються невирішеними.

**Результати аналізу наукових публікацій.** Проблемам стратегічного планування у сфері кібербезпеки були присвячені праці таких науковців і практиків, як С.Л. Гнатюк [3], Д.В. Дубов [4], Н.Ю. Литвинчук [5], Н.А. Ткачук [6] та інших, проте питання оцінки стратегій кібербезпеки потребують певних уточнень та подальших ґрунтовних розробок.

**Метою статті** є визначення ключових критеріїв оцінки ефективності реалізації Стратегії кібербезпеки України.

**Виклад основного матеріалу.** Кабінет Міністрів України щороку розробляє план заходів з реалізації Стратегії кібербезпеки України [7], а також зобов'язує Адміністрацію Державної служби спеціального зв'язку та захисту інформації інформувати кожні півроку про хід виконання цих заходів Раду національної безпеки і оборони України та Кабінет Міністрів України. Надзвичайно важливого значення в сучасних умовах набуває також визначення ефективності виконання запланованих заходів.

Процес оцінки рівня ефективності реалізації Стратегії кібербезпеки України методологічно пов'язаний із визначенням належного критерію і формуванням відповідної системи показників, адже критерій – це головна ознака визначення ефективності, за яким здійснюється її кількісна оцінка. Правильно сформульований критерій має найповніше характеризувати суть ефективності реалізації запланованих заходів.

Розвинені країни, зокрема держави ЄС, мають значну практику розробки відповідних Стратегій кібербезпеки (далі – Стратегії), їх практичної реалізації, а також визначення їх ефективності. Це пов'язано з тим, що в інформаційному суспільстві ЄС широко використовуються різноманітні інформаційні технології, водночас кіберінциденти можуть нівелювати досягнення економічних вигод від використання кіберпростору.

Міжнародним союзом електрозв'язку (International Telecommunication Union, ITU – міжнародна організація, що визначає стандарти в галузі телекомунікацій) у 2018 році був розроблений Посібник для розробки національних стратегій кібербезпеки, який спрямований на полегшення створення та оновлення національними органами відповідних документів [8].

У рекомендаціях, наданих у цьому посібнику, розглянуто процес розробки стратегії кібербезпеки починаючи від аналізу стану кібербезпеки до публікації документа та розробки плану дій на його виконання, а також подальшого вдосконалення.

Також в посібнику зазначається про необхідність періодичного оцінювання результатів від реалізації Стратегії кібербезпеки та порівнювати їх з поставленими цілями. Це надзвичайно важливо для розуміння того, чи реалізуються цілі Стратегії. Варто також регулярно переоцінювати існуючі кіберризики, щоб зрозуміти, чи впливають зовнішні зміни на результати реалізації Стратегії кібербезпеки.

Ця оцінка разом з запропонованими рекомендаціями щодо змін до Стратегії повинна бути підготовлена у вигляді звіту для відповідного керівного органу та включати в себе План дій по оновленню документа, щоб забезпечити необхідну зміну політики та переліку кіберризиків.

Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA), яке є центром експертиз для інформаційної безпеки ЄС, його держав-членів, приватного сектору та громадян Європи, розробляє рекомендації щодо ефективної практики інформаційної безпеки. Воно допомагає державам-членам ЄС у розробці законодавства ЄС у сфері кібербезпеки, підвищенні стійкості критичної інформаційної інфраструктури та комп'ютерних мереж в Європі.

Проаналізувавши 18 європейських Стратегій та 8 Стратегій поза межами ЄС, ENISA відзначило чотири важливі етапи: розробку, впровадження, оцінку та коригування і запропонувало систему їх оцінювання [9].

Відповідно до рекомендацій ENISA основними цілями оцінки стратегії кібербезпеки, заснованої на даному аналізі, є:

- розробка політики та можливостей кіберзахисту;
- досягнення кіберстійкості (здатність суб'єкта досягати бажаного результату незважаючи на кіберінциденти);

- зменшення кіберзлочинності;
- підтримка промисловості у сфері кібербезпеки;
- безпека інформаційної критичної інфраструктури.

Для оцінки ефективності реалізації Стратегії використовується також емпіричний метод, який зокрема передбачає огляд повідомлень у ЗМІ, щодо оцінки стану кібербезпеки. Це дозволяє дослідити роль, яку оцінювання Стратегії відіграє в складних заходах державної політики.

Також проводиться інтерв'ювання ключових експертів у сфері кібербезпеки. Метою цих інтерв'ю є вивчення основних показників оцінки кібербезпеки.

Практика визначення показників описується акронімом *SMART*. Вони повинні бути:

*Specific*: конкретні – чіткі, щоб уникнути неправильного тлумачення або двозначності;

*Measurable*: вимірні – можуть бути кількісно виміряні (хоча вони можуть бути також якісними);

*Attainable*: досяжні – цілі встановлюються досяжними, спостережуваними та виконуваними за певних умов в конкретні терміни, а також незалежно перевірені;

*Relevant*: повинні відповідати стратегії та цілі конкретного відомства;

*Time-related*: визначені конкретним терміном – існує обмеження часу для досягнення результатів.

Зацікавленість ENISA у сприянні оцінюванню та підтримці стратегічного планування Стратегій вписується в більш широку картину заохочення держав-членів та інституцій ЄС до впровадження різноманітних заходів кібербезпеки. У Європейському Союзі ці стратегії включені до “Цифрової програми Європи” (Digital Agenda for Europe – DAE [10]) для безпечного цифрового суспільства, спрямованого на сприяння економічному зростанню. Держави-члени контролюють прогрес кібербезпеки відповідно до запланованих заходів та подають щороку звіти про її моніторинг. На підставі цих звітів Європейська Комісія (ЄК) порівнює досягнення держав-членів за відповідними напрямками.

Майже всі Стратегії, розглянуті в рамках дослідження ENISA, включають положення про процес розгляду та оцінки документа. Наприклад, у Фінляндії забезпечення перегляду та оцінки Стратегії є одним із десяти стратегічних напрямів діяльності. В інших стратегіях (Великобританія, Німеччина, Франція) оцінка також слугує для того, щоб забезпечити сучасну законодавчу базу щодо останніх подій у технологічному ландшафті. У ряді стратегій частота циклу оцінювання встановлюється на щорічній (Литва, Словаччина, Нідерланди) або дворічній (Австрія) основі. Деталі процесу оцінювання включені в окремий акт або в план впровадження. Навіть там, де процеси перегляду не зазначені в самій Стратегії, делеговані акти та дії, передбачені ними, підлягають перевірці державними аудиторськими органами залежно від інституційної структури країни.

Кожна оцінка реалізації Стратегії повинна визначатися відповідним незалежним органом (наприклад, національною радою з кібербезпеки). Для цього необхідно цьому органу надати належний мандат та визначити його роль і обов'язки. Необхідно також створити схему збору даних для отримання відповідних показників для оцінки стратегії та плану дій. Процес збору даних повинен стати всеохоплюючим.

На основі аналізу даних готується аналітичний звіт про оцінку, що описує досягнуті результати та очікування щодо наступного періоду.

Для отримання об'єктивної оцінки реалізації Стратегії кожна держава повинна здійснювати моніторинг найважливіших надзвичайних ситуацій, які стосуються кіберзахисту. Успіх національної програми вимірюється кількістю кіберінцидентів, що сталися в певний період часу з мінімальними заходами безпеки. Відсутність цього типу подій концептуально означає, що всі загрози були виявлені, і їхній вплив було мінімізовано.

В країнах ЄС щорічна доповідь про діяльність у сфері захисту кіберпростору додається до щорічного звіту парламенту про стратегію та політику національної безпеки.

ENISA запропонувало перелік можливих ключових індикаторів ефективності (key performance indicators – KPI), які можуть бути обрані для вимірювання ефективності реалізації Стратегії. Ці індикатори розбиті на групи відповідно до ключових цілей оцінки стратегії кібербезпеки.

#### Ключова ціль 1: *Розвиток кіберзахисту*

| Ключове завдання                                                                                                                                                                                                                   | Доказ (що саме оцінюється)                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Наявність стратегічного національного плану з кібербезпеки                                                                                                                                                                         | Наявність і статус такого плану, звіти про діяльність, план дій та відповідальність |
| Ступінь участі в ініціативах ЄС з кіберзахисту                                                                                                                                                                                     | Індикація участі, рівень участі                                                     |
| Ідентифікація та структура військового CERT                                                                                                                                                                                        | Оцінка можливостей; політичні документи; внутрішні оперативні документи             |
| Наявність навчання персоналу                                                                                                                                                                                                       | Оцінка можливостей; політичні документи; внутрішні оперативні документи             |
| Оперативна сумісність (здатність взаємодіяти з іншими структурами)                                                                                                                                                                 | Оцінка можливостей; політичні документи; внутрішні оперативні документи             |
| Збільшення стійкості через співпрацю у протидії військовим кібератакам (швидке виявлення, відповідь і відновлення від складних кібератак, економічно ефективний розвиток, співпраця, надійні, доступні і зрозумілі канали зв'язку) | Оцінка можливостей, звіти про кіберінциденти                                        |

Ключова ціль 2: *Досягнення кіберстійкості*: розвиток потенціалу та ефективного співробітництва державного та приватного секторів

| Ключове завдання                                                                                                                          | Доказ (що саме оцінюється)                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Налагодження діяльності CERT або Національних агенцій кібербезпеки                                                                        | Існування та мандат інституційних суб'єктів (сфера діяльності, повноваження агентств/органів)        |
| Наявність державно-приватного партнерства з питань кібербезпеки                                                                           | Визначення та зміст такого партнерства, його значення, звіти про діяльність                          |
| Виявлення ризиків та загроз                                                                                                               | Аналіз ризиків, аналіз загроз (проводиться CERT або Агенцією національної безпеки)                   |
| Наявність тренувань з питань кібербезпеки                                                                                                 | Звіти про діяльність                                                                                 |
| Розширені можливості: організовані тренінги для державного та приватного секторів, взаємна навчальна діяльність (семінари та конференції) | Звіти про діяльність, назва події, компанії/зацікавлені сторони                                      |
| Координація діяльності усіх суб'єктів національної системи кібербезпеки                                                                   | Звіти про діяльність                                                                                 |
| Наявність розвинених засобів реагування (плани реагування, системи раннього попередження тощо)                                            | Плани виявлення та відновлення, раннє попередження системи та імітаційні моделі, звіт про діяльність |

|                                                    |                                                                                                                                                                                                                 |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Посилення безпеки громадських інформаційних систем | Виявлення вразливостей (звіт-CERT або Національної Агенції кібербезпеки), документування оновлення/виправлення програмного забезпечення та створення процедур, прийняття стандартів кібербезпеки для систем ІКТ |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Ключова ціль 3: *Зменшення кіберзлочинності*

| Ключове завдання                                                                                                                                                                                                                | Доказ (що саме оцінюється)                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Національна система протидії кіберзлочинності                                                                                                                                                                                   | Структура системи                                                                                                                                                                          |
| Національні інституції для протидії кіберзлочинності (правоохоронні органи, CERT тощо)                                                                                                                                          | Структури та законодавча база                                                                                                                                                              |
| Зміцнення правоохоронних органів (аналіз прогалин, визначення потреб, сучасні технічні активи, використання передового досвіду)                                                                                                 | Документація щодо виявлених проблем та заходів щодо підтримки правоохоронних органів для протидії кіберзлочинності, оцінки можливостей, реєстру кращих практик, документації щодо процедур |
| Наявність механізмів співпраці з ЕСЗ, CEPOL, Євроюстом та іншими міжнародними організаціями                                                                                                                                     | Звіти про діяльність та спільні дії                                                                                                                                                        |
| Національні рішення по справам кіберзлочинності                                                                                                                                                                                 | Статистичні дані МВС щодо кіберзлочинів (розслідування, кримінальні переслідування тощо)                                                                                                   |
| Міжнародна співпраця:<br>– посилення можливостей боротьби з кіберзлочинністю через кордони;<br>– зменшення бар'єрів для розслідувань;<br>– доступ до сучасних інструментів;<br>– зниження витрат на боротьбу з кіберзлочинністю | Процедури транскордонного співробітництва між органами влади (CERT та ін.). Статистика розслідувань і резолюцій, бюджетні звіти                                                            |
| Безпечний кіберпростір для всіх користувачів                                                                                                                                                                                    | Статистика (правоохоронні органи, опитування, національні статистичні управління)                                                                                                          |

### Ключова ціль 4: *Промислові розробки та технології для забезпечення кібербезпеки*

Концепція цієї ключової цілі полягає в тому, що промисловість та технологічні досягнення (у тому числі наукові) будуть підтримувати рівень національної кібербезпеки на ринку продуктів.

| Ключове завдання                                                               | Доказ (що саме оцінюється)                                                                                                                 |
|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Підтримка стандартизації та розробки у галузі кібербезпеки                     | Відповідність стандартам безпеки, перевіркам та механізмам сертифікації, встановленими регуляторними органами, рівнем прийняття стандартів |
| Фінансування досліджень через програми ЄС та національні дослідницькі програми | Бази даних ЄС щодо дослідницького проекту, агентства, що фінансують науку                                                                  |
| Розробка нових національних заходів кіберзахисту                               | Політичні документи, державні акти, документи щодо вимоги до ІКТ, нові політики                                                            |

|                                            |                                                       |
|--------------------------------------------|-------------------------------------------------------|
| Підтримка інновацій в електронному бізнесі | Впровадження інноваційних рішень електронного бізнесу |
| Доступ споживачів до безпечних технологій  | Звіти про дослідження ринку                           |

**Ключова ціль 5: *Забезпечити захист критичної інформаційної інфраструктури.***

Відповідно до ключового завдання щодо захисту критичної інформаційної інфраструктури ми досліджуємо такі поняття, як інформування про кіберінциденти, ідентифікацію цих структур, міжнародне співробітництво та обмін інформацією.

| Ключове завдання                                                                                                          | Доказ (що саме оцінюється)                                                                              |
|---------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Ідентифікація критично важливої інформаційної інфраструктури, тобто критичних активів, уразливостей, залежностей, ризиків | Перелік об'єктів критичної інформаційної інфраструктури                                                 |
| Оцінка ризиків та плани управління ризиками                                                                               | Розподіл обов'язків та процедури, яких необхідно дотримуватися (включаючи періодичність оновлень)       |
| Процедури інформування про кіберінциденти                                                                                 | Опис процедури, ролей та обов'язків, залучених органів, співпраці між країнами                          |
| Плани відновлення бізнесу та безперервності для критичної інфраструктури                                                  | Стратегічні програмні документи; імплементації рекомендацій, розподіл обов'язків різноманітних структур |
| Успішний обмін інформацією та надійне співробітництво між різними гравцями                                                | Довірені канали для спілкування, регулярні зустрічі, залучення зацікавлених сторін                      |
| Швидке та ефективне реагування на випадок інцидентів на національному рівні (менше часу простою у разі кіберінциденту)    | Скорочення швидкості реагування; зменшення невизначеності реакції                                       |
| Прозорість і підзвітність систем                                                                                          | Кількість та тип документації, доступної для громадськості, вимірює обізнаність людей                   |

Також для оцінки ефективності національної Стратегії та плану її реалізації слід враховувати показники загального рівня кібербезпеки. Це зокрема, відсоток виконання зобов'язань, рівень прозорості витрат для цілей кібербезпеки (необхідний фінансовий аудит з конкретними сферами діяльності щодо плану дій з кібербезпеки), співробітництво з іншими державами у кіберпросторі тощо.

Наступним кроком для проведення оцінки та об'єднання різних критеріїв для кінцевого результату повинна бути розробка відповідного автоматизованого інструменту.

Деякі інші підходи щодо оцінки ефективності Стратегії розглянемо на прикладі Канади [11]. Ця оцінка була проведена з метою виконання вимог Закону про фінансове адміністрування (Financial Administration Act [12]).

Основною метою проведення оцінки ефективності Стратегії було визначити наскільки:

була ефективною структура управління для виконання Стратегії;

департаменти та відомства, що беруть участь у забезпеченні кібербезпеки, виконували затверджену Стратегію діяльності;

заплановані заходи сприяли досягненню головних цілей Стратегії.

Для проведення оцінки використовувалася така методологія:

1. Огляд спеціальної літератури – це пошук в Інтернеті документів, пов'язаних із темами з кібербезпеки в цілому, і, зокрема, Стратегії кібербезпеки Канади.

2. Перегляд документів включав перегляд звітів про ефективність, фінансової інформації та останніх аудиторських звітів.

3. Інтерв'ю – це проведення 48 інтерв'ю з урядовими посадовцями з 11 урядових організацій Канади, а також з науковцями та іншими експертами.

При аналізі ефективності Стратегії увага приділялася питанням якою мірою досягнуто прогрес у забезпеченні кібербезпеки уряду Канади та зміцненні спроможності:

запобігання кіберінцидентам;

виявленні і захисту від кіберзагроз;

реагуванні і відновленні інфраструктури після кіберінцидентів.

Проведене дослідження виявило, що існуюча структура управління сприяла співпраці, координації та обміну інформацією між суб'єктами кібербезпеки. Проте обмін інформацією проходив на вибірковій основі, і не було чіткої політики щодо того, з ким і коли він здійснюється. На цей час не існує ефективного механізму обміну секретною інформацією, особливо в режимі реального часу.

Стратегія допомогла визначити ролі та обов'язки різних організацій та уряду Канади, запровадивши систему управління для уточнення цілей, призначення ролей та обов'язків, а також створення різних комітетів і робочих груп.

В результаті дослідження було виявлено, що Стратегія сприяє збільшенню спроможності уряду Канади запобігати, виявляти, реагувати та відновлюватися після кібернападів. Зокрема, практична реалізація Стратегії допомогла підвищити здатність урядових організацій швидко аналізувати та протидіяти кіберінцидентам, які, хоча все ще відбуваються, проте стають все рідше. Ці покращення були відзначені, незважаючи на збільшення державної та неурядової кіберактивності проти інформаційних мереж уряду Канади за останні роки. Тим не менше, респонденти відзначають, що є додаткові можливості для подальшого покращення кібербезпеки. Оцінка також виявила, що Стратегія сприяє розвитку партнерських відносин із власниками та операторами критично важливої інфраструктури, а також іншими зацікавленими сторонами приватного сектору.

Також серед більшості опитаних існує думка, що канадці сьогодні порівняно з минулим стали більш інформовані про кіберзагрози.

Враховуючи ці висновки, в оцінці було визначено ряд шляхів для вдосконалення кібербезпеки і висунуті рекомендації для їх вирішення. Як головна організація, Міністерство громадської безпеки Канади взяло на себе зобов'язання вирішувати ці питання у співпраці з партнерськими організаціями в рамках зусиль, спрямованих на поновлення стратегії кібербезпеки Канади з метою кращої підготовки до зміцнення її національної, економічної та кібернетичної безпеки.

Хоча в Україні в останні роки забезпеченню кібербезпеки надають великого значення і, як уже зазначалося, щорічно формується План заходів з реалізації Стратегії кібербезпеки України, який затверджується розпорядженням Кабінету Міністрів України, заходи, які визначені цим Планом, не завжди виконуються вчасно, а деякі залишаються взагалі не виконаними з різних причин.

Наприклад, **найбільш актуальним** на сьогодні залишається питання **формування переліку об'єктів критичної інформаційної інфраструктури, яке передбачене пунктом 2 Плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України** (далі – План). Це питання не вирішується протягом значного терміну часу (п'ятий рік). Зокрема розпорядженням Кабінету Міністрів України від 5 листопада 2014 р. № 1135-р (чинне) було затверджено План заходів щодо захисту державних інформаційних



ресурсів, яким передбачалося Адміністрації Держспецзв'язку протягом 2014 – 2015 років сформувавши перелік об'єктів, що належать до критичної інформаційної інфраструктури держави, організувати та провести оцінку стану захищеності державних інформаційних ресурсів зазначених об'єктів.

Пізніше пунктом 2 Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації”, введеного в дію Указом Президента України від 13 лютого 2017 року №32/2017, було ухвалено забезпечити у місячний строк виконання завдання, передбаченого пунктом 2 постанови Кабінету Міністрів України від 23 серпня 2016 року № 563 “Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави”, та вжити в установленому порядку заходів щодо притягнення до відповідальності осіб, які не забезпечили виконання такого завдання у визначений зазначеною постановою строк. Це рішення також не було виконано. Зазначимо, що і на даний час (написання статті) перелік об'єктів критичної інформаційної інфраструктури не сформовано.

Також Планом на 2018 рік, як і в 2017 р. (пункт 13) передбачалось здійснити “розроблення методики формування та визначення основних показників ефективності реалізації Стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик”. Але ні у 2017, ні у 2018 роках ці завдання виконані не були (відповідальний за їх виконання орган – Держспецзв'язку) [6].

Однією з можливих причин цього є те, що План був затверджений тільки у липні 2018 року, і тому терміни виконання половини (9 із 18) заходів, передбачених цим Планом, були вже закінчені на час його затвердження, а відповідні заходи об'єктивно не могли бути виконаними вчасно.

З огляду на це, слід приділити серйозну увагу формуванню Плану на 2019 рік. Адже, незважаючи на те, що відповідний проект Держспецзв'язком було розроблено у листопаді 2018 року, сам план на даний час (написання статті травень 2019) Кабінетом Міністрів України ще не затверджено.

Підкреслимо, що Законом України “Про національну безпеку” [13] запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони України, забезпечуючи у такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони. А відповідно до ст. 4 цього Закону предметом цивільного контролю з боку громадянського суспільства є зміст і стан реалізації стратегій, доктрин, концепцій, державних програм та планів у сферах національної безпеки і оборони.

Тому, на нашу думку, актуальним на сьогодні є проведення незалежного аналізу ефективності реалізації Стратегії кібербезпеки України. Такий аналіз повинен бути здійснений відповідним уповноваженим органом згідно із затвердженою Методикою на основі рекомендацій ENISA.

Зазначимо також, що відповідно до пункту 3 статті 15 Закону України “Про основні засади забезпечення кібербезпеки України” щорічно має проводитись незалежний аудит діяльності основних суб'єктів національної кібербезпеки щодо ефективності системи забезпечення кібербезпеки держави згідно з міжнародними стандартами аудиту. Проведення зазначеного аудиту потребує визначення відповідного органу та затвердження методики проведення такого аудиту.

Незалежний нагляд та контроль за діяльністю суб'єктів у сфері кібербезпеки держави здійснюється і в європейських країнах. Такий контроль може виявити низку недоліків у забезпеченні кібербезпеки та надати певні рекомендації для їх усунення.

Зокрема у своїй доповіді з питань інформаційної безпеки у державній адміністрації у 2014 році, Національне бюро аудиту Швеції вказало на необхідність посилення у першу чергу нагляду на об'єктах критичної інфраструктури [14].

Подібний аудит проводиться і в Польщі. Зокрема, у 2015 році Головне контрольно-ревізійне управління (Najwyższa Izba Kontroli, NIK) підготувало спеціальний аудит для оцінки реалізації стратегічних заходів, що здійснюються суб'єктами, відповідальними за кібербезпеку в Польщі. Загальна оцінка була критичною щодо успіху впровадження Стратегії кібербезпеки – рівень реалізації ключових заходів та рівень досягнення цілей були дуже низькими [15].

### **Висновки.**

Уряди провідних країн світу і зокрема ЄС продовжують вживати різноманітних заходів для посилення безпеки кіберпростору, як елементу глобальної міжнародної безпеки. При цьому особлива увага приділяється розробкам стратегічних документів з питань кібербезпеки, їх регулярному оновленню та контролю виконання плану заходів реалізації на основі оцінки ефективності та спроможностей.

Для своєчасного поновлення таких документів в Україні необхідно розробити критерії оцінки стану кібербезпеки в державі. А після проведення відповідної оцінки визначити ключові напрями формування нової Стратегії кібербезпеки України, розрахованої на 2020 – 2025 роки.

Враховуючи міжнародний досвід, включно з фундаментальними рекомендаціями та директивами ООН, НАТО, ЄС та ОБСЄ, основний стратегічний напрям діяльності суб'єктів національної системи кібербезпеки повинен бути спрямований на кіберзахист критичної інформаційної інфраструктури.

Тому Кабінету Міністрів України необхідно прискорити затвердження Переліку об'єктів критичної інформаційної інфраструктури, а також постанови “Про затвердження Вимог щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури” та “Порядку проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури”. Це дозволить виявити реальний стан кіберзахисту на зазначених об'єктах та вжити заходів для його посилення.

У зв'язку з тим, що відповідно до ст. 25 Закону України “Про національну безпеку України” Стратегію кібербезпеки та інші стратегічні документи, якими визначаються основні напрями і завдання державної політики у сферах національної безпеки і оборони розробляє РНБО України, яка також здійснює координацію і контроль за їх виконанням, на нашу думку, доцільно було б, щоб План заходів з реалізації Стратегії кібербезпеки України також затверджувався б Рішенням РНБО України, а його підготовку та контроль виконання здійснював Національний координаційний центр кібербезпеки, що передбачено у Положенні про Національний координаційний центр кібербезпеки [16]. Це надасть змогу більш оперативно планувати відповідні заходи та здійснювати контроль їх виконання.

### **Використана література**

1. DR Mykhaylo Gutsalyuk. Ukraine's Cybersecurity strategy and ways to implement it. *European Cybersecurity journal*. Volume 2 (2016). The Kosciuszko Institute. Poland. P. 65-69.
2. Науково-практичний коментар Закону України “Про основні засади забезпечення кібербезпеки України”: станом на 1 січня 2019 року / М.В. Гуцалюк та ін.; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.
3. Гнатюк С.Л. Кібербезпека в умовах розгортання четвертої промислової революції (industry 4.0): виклики та можливості для України. URL: <http://niss.gov.ua/doslidzhennya/analitichni-materiali/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgartannya> (дата звернення: 21.05.2019).

4. Дубов Д.В. Стратегічні аспекти кібербезпеки України. *Стратегічні пріоритети*. 2013. № 4. С. 119-127. URL: [http://nbuv.gov.ua/UJRN/spa\\_2013\\_4\\_18](http://nbuv.gov.ua/UJRN/spa_2013_4_18) (дата звернення: 21.05.2019).
5. Литвинчук Н.Ю. Формування системи забезпечення кібернетичної безпеки: збірник тез наук. доповідей X Всеукр. наук.-практ. конф. *Актуальні проблеми управління інформаційною безпекою держави*, м. Київ, 4 квіт. 2019 р. Київ: Нац. акад. СБУ, 2019. С. 240-243.
6. Ткачук Н.А. Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право*. № 1(28)/2019. С. 129-134.
7. Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 11.07.18 р. № 481-р. URL: <https://zakon.rada.gov.ua/laws/show/481-2018-%D1%80> (дата звернення: 21.05.2019).
8. Guide to Developing A National Cybersecurity Strategy. URL: [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-CYB\\_GUIDE.01-2018-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf) (дата звернення: 21.05.2019).
9. An evaluation Framework for National Cyber Security Strategies. URL: <https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies> (дата звернення: 21.05.2019).
10. Europe 2020 strategy URL: <https://ec.europa.eu/digital-single-market/en/europe-2020-strategy> (дата звернення: 21.05.2019).
11. Horizontal Evaluation of Canada's Cyber Security Strategy. URL: <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/vltcn-cnd-scrt-strtg/index-en.aspx> (дата звернення: 21.05.2019).
12. Financial Administration Act (R.S.C., 1985). URL: <https://laws-lois.justice.gc.ca/eng/acts/f-11> (дата звернення: 21.05.2019).
13. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19?find=1&text=%D1%F2%F0%E0%F2%E5%E3%B3%F%F+%EA%B3%E1%E5%F0%E1%E5%E7%EF%E5%EA%E8> (дата звернення: 21.05.2019).
14. A national cyber security strategy (Sweden). URL: <https://www.government.se/4ac8ff/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213> (дата звернення: 21.05.2019).
15. NIK o bezpieczeństwie w cyberprzestrzeni. URL: <https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.html>
16. Про Національний координаційний центр кібербезпеки: Указ Президента України від 7.06.16 р. № 242/2016. URL: <https://zakon.rada.gov.ua/laws/show/242/2016> (дата звернення: 21.05.2019).

~~~~~ \* \* \* ~~~~~

УДК 342.52

**ПЕТРОВ С.Г.**, кандидат юридичних наук, співробітник СБ України

## **ПОВНОВАЖЕННЯ СБ УКРАЇНИ ЯК СУБ'ЄКТА НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ**

**Анотація.** У статті досліджуються питання визначення повноважень Служби безпеки України як суб'єкта національної системи кібербезпеки з урахуванням процесів реформування державного органу спеціального призначення з правоохоронними функціями, що забезпечує державну безпеку.

**Ключові слова:** Служба безпеки України, кібербезпека, повноваження, функція, державні електронні інформаційні ресурси.

**Summary.** The article deals with defining of the authority of the Security Service of Ukraine as a subject of national cybersecurity system regarding the reformation of the special governmental body with law enforcement functions ensuring state security.

**Keywords:** Security Service of Ukraine, Cybersecurity, Authority, Function, State Electronic Information Recourses

**Аннотация.** В статье исследуются вопросы определения полномочий Службы безопасности Украины как субъекта национальной системы кибербезопасности с учетом процессов реформирования государственного органа специального назначения с правоохранительными функциями, который обеспечивает государственную безопасность.

**Ключевые слова:** Служба безопасности Украины, кибербезопасность, полномочия, функция, государственные электронные информационные ресурсы.

**Постановка проблеми.** Концепція розвитку сектору безпеки і оборони України, яка визначає шляхи формування національних безпекових та оборонних спроможностей, зорієнтована серед іншого на створення національної системи реагування на кризові ситуації, своєчасне виявлення, запобігання та нейтралізацію зовнішніх і внутрішніх загроз національній безпеці, гарантування особистої безпеки, конституційних прав і свобод людини і громадянина, забезпечення кібербезпеки [1].

Реформування Служби безпеки України відповідно до зазначеної Концепції спрямовуватиметься на посилення її спроможностей протидіяти сучасним зовнішнім і внутрішнім загрозам національній безпеці та здійснюватиметься у напрямі оновлення доктринальних і концептуальних підходів до організації діяльності Служби безпеки України, функціональної оптимізації її організаційної структури та вдосконалення матеріально-технічного забезпечення. Значна частина повноважень СБ України буде спрямована на вирішення завдань попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством; протидії кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога стосовно захисту якої встановлена законом, критичної інформаційної інфраструктури та її окремих об'єктів; здійснення тестування готовності захисту об'єктів критичної інформаційної інфраструктури до можливих кібератак та кіберінцидентів; забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки [1; п. 3.9].

Тому вирішення питання щодо наділення СБ України окремими повноваженнями в означеній сфері потребує ґрунтовного наукового аналізу чинного законодавства України, а також місця СБ України у національній системі кібербезпеки.

**Результати аналізу наукових публікацій** свідчать про те, що питання діяльності СБ України у сфері забезпечення інформаційної безпеки держави було предметом досліджень багатьох українських учених, а саме М.М. Галамби, М.В. Гребенюка, О.Д. Довганя, О.О. Климчука, А.І. Марущака, В.В. Остроухова, В.М. Панченко, В.Г. Пилипчука, В.І. Польового, О.Б. Розвадовського, В.Б. Хлевицького, О.М. Юрченка та інших. Однак розкриття функцій та повноважень СБ України як суб'єкта національної системи кібербезпеки були предметом досліджень тільки частково.

**Метою статті** є розкриття повноважень СБ України як суб'єкта національної системи кібербезпеки.

**Виклад основного матеріалу.** Закон України “Про національну безпеку України” від 21 червня 2018 року визначив СБ України державним органом спеціального призначення з правоохоронними функціями, що забезпечує державну безпеку, здійснюючи з неухильним дотриманням прав і свобод людини і громадянина:

- 1) протидію розвідувально-підбивній діяльності проти України;
- 2) боротьбу з тероризмом;
- 3) контррозвідувальний захист... кібербезпеки... та інформаційної безпеки держави, об'єктів критичної інфраструктури [2, ст. 19].

Відповідно до Закону України “Про основні засади забезпечення кібербезпеки України” національну систему кібербезпеки становлять суб'єкти забезпечення кібербезпеки та взаємопов'язані заходи політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури [3, ст. 8].

Словосполучення “контррозвідувальний захист кібербезпеки” при визначенні відповідної функції СБ України видається не зовсім коректним. Вважаємо, що кращим для використання і позначення функції СБ України буде термін “контррозвідувальне забезпечення кібербезпеки” як складової національної безпеки.

Служба безпеки України визначена одним із основних суб'єктів національної системи кібербезпеки разом з Державною службою спеціального зв'язку та захисту інформації України (Держспецзв'язку України), Національною поліцією України, Міністерством оборони України та Генеральним штабом Збройних Сил України, розвідувальними органами, Національним банком України [3, ст. 8].

Завданнями основних суб'єктів національної системи кібербезпеки відповідно є:

- 1) Держспецзв'язку забезпечує – захист у кіберпросторі державних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури, створення та функціонування Національної телекомунікаційної мережі; здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформування про кіберзагрози та методи захисту від них; забезпечення впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури; забезпечення функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA тощо. Варто відзначити, що впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення та функціонування основних

складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань [3, ст. 8].

2) Національна поліція України – захист від злочинних посягань у кіберпросторі; здійснення заходів із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі;

3) Міністерство оборони України, Генеральний штаб Збройних Сил України – здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); впровадження заходів із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану тощо.

4) розвідувальні органи України – здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;

5) Національний банк України – опікується питаннями забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів; створює центр кіберзахисту НБУ, забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України.

Служба безпеки України в свою чергу здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки [3, ст. 8].

Безумовно, значну частину заходів щодо забезпечення кібербезпеки здійснює Держспецзв'язку України поряд із забезпеченням функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань [2, ст. 22].

Національна система кібербезпеки України на сьогодні перебуває у стадії свого формування, а тому існують питання, які потребують нагального вирішення. Так, наприклад, Закон України “Про національну безпеку України” передбачає здійснення комплексного огляду сектору безпеки і оборони, зокрема й огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. Однак на сьогодні такий огляд не проведено. Більше того, Кабінет Міністрів України не затвердив порядок проведення комплексного огляду сектору безпеки і оборони у сфері кібербезпеки. У документах, які датуються 2015 роком і стосуються плану заходів з проведення комплексного огляду сектору безпеки і оборони України та методичних

рекомендацій щодо його проведення [4] відсутні питання огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. На нашу думку, такий огляд має стати основою для оновлення Стратегії кібербезпеки України, яка на сьогодні вже не повною мірою відповідає вимогам часу.

Для її оновлення існують й інші аргументи. Так, Закон України “Про національну безпеку України” визначає, що Стратегія кібербезпеки України є основою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України [2, ст. 31].

Разом з тим, варто відзначити, що в Україні Стратегія кібербезпеки України як “документ довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, підвищення ефективності основних суб’єктів забезпечення кібербезпеки, насамперед суб’єктів сектору безпеки і оборони, щодо виконання завдань у кіберпросторі, а також потреби бюджетного фінансування, достатні для досягнення визначених цілей і виконання передбачених завдань, та основні напрями використання фінансових ресурсів” [2, ст. 31] прийнята до закріплення відповідного визначення у Законі України “Про національну безпеку України” від 21.06.18 р., а саме Указом Президента України від 15.03.16 р. № 96/2016 [5]. Це об’єктивно призвело до того, що сучасна Стратегія кібербезпеки України не містить закріплення концептуальних підходів до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, а також, що найголовніше, – потреб бюджетного фінансування, достатніх для досягнення визначених цілей і виконання передбачених завдань, та основних напрямів використання фінансових ресурсів.

Законодавство України про контррозвідувальну діяльність [6] на сьогодні не містить норм щодо здійснення СБ України контррозвідувальних заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством. І хоча до підстав для проведення контррозвідувальної діяльності віднесено виконання визначених законом завдань щодо контррозвідувального забезпечення економічного, інформаційного, науково-технічного потенціалу, оборонно-промислового і транспортного комплексів та їх об’єктів, національної системи зв’язку, Збройних Сил України та інших утворених відповідно до законів України військових формувань, військово-технічного співробітництва [6, ст. 6], вважаємо за необхідне додатково передбачити такі підстави у Законі України “Про контррозвідувальну діяльність” саме у частині боротьби з кібертероризмом та кібершпигунством, а також протидії кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави.

Закон України “Про Службу безпеки України” також не передбачає повноважень СБ України як суб’єкта національної системи кібербезпеки, хоча передбачає функціонування підрозділів контррозвідувального захисту інтересів держави у сфері інформаційної безпеки [7]. У новій редакції зазначеного Закону безумовно будуть передбачені повноваження, визначені законодавством про кібербезпеку.

Враховуючи наукову і практичну проблему неімплементованості у чинне законодавство України положень Конвенції про кіберзлочинність у частині обов’язкового зберігання та надання операторами та провайдерами телекомунікацій інформації на вимогу правоохоронних органів, необхідної для розслідування кіберзлочинів [8], не зможуть бути ефективно реалізованими функції СБ України щодо

протидії злочинам проти миру і безпеки людства, які вчиняються у кіберпросторі, кібертероризму, кібершпигунству та кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України.

Крім того, за чинним кримінальним процесуальним законодавством СБ України не має повноважень щодо розслідування кібератак на критичну інформаційну інфраструктуру та державні електронні інформаційні ресурси, як передбачає законодавство України про кібербезпеку. Тому цей напрям удосконалення повноважень СБ України також вважаємо перспективним, особливо з урахуванням відсутності на даний час переліку об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури України.

Розслідування кіберзлочинів є важливою складовою забезпечення кібербезпеки держави. Однак, на сьогодні СБ України фактично позбавлена повноважень щодо оперативної і цілодобової підтримки від іноземних партнерів при запобіганні, виявленні, припиненні та розкритті злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі, а також кібертероризму та кібершпигунства. Адже в Україні органом, на який покладаються повноваження щодо “створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України” [9]. Безумовно, при закріпленні повноважень СБ України у процесі її реформування мають бути передбачені можливості для оперативної і цілодобової підтримки відповідних розслідувань.

### **Висновки.**

Підсумовуючи викладене, зазначимо, що у процесі реформування СБ України функція контррозвідального забезпечення кібербезпеки має бути закріплена однією з пріоритетних з огляду на загрози і виклики національній безпеці в інформаційній сфері.

При удосконаленні повноважень СБ України як суб'єкта національної системи кібербезпеки, відповідального за запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі, здійснення контррозвідальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, негласну перевірку готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидію кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечення реагування на кіберінциденти у сфері державної безпеки мають бути враховані наступні пропозиції автора.

В Україні варто створити нормативно-правову основу для огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. Такий огляд стане основою для оновлення Стратегії кібербезпеки України, яка на сьогодні не тільки не повною мірою відповідає вимогам часу, а й не містить окремих положень, передбачених Законом України “Про національну безпеку України” щодо формування та реалізації державної політики з безпечного функціонування кіберпростору і потреб бюджетного фінансування та основних напрямів використання фінансових ресурсів.

У роботі обґрунтовано необхідність внесення змін до законів України “Про контррозвідальну діяльність” та “Про Службу безпеки України” саме у частині



боротьби з кібертероризмом та кібершпигунством, а також протидії кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави.

Вказано на доцільність внесення змін до кримінального процесуального законодавства України щодо наділення СБ України повноваженнями із розслідування кібератак на критичну інформаційну інфраструктуру та державні електронні інформаційні ресурси, як передбачає законодавство України про кібербезпеку.

Актуалізовано також необхідність наділення СБ України повноваженнями щодо оперативної і цілодобової підтримки від іноземних партнерів при запобіганні, виявленні, припиненні та розкритті злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі, а також кібертероризму та кібершпигунства через контактну мережу, яка на сьогодні функціонує лише у Міністерстві внутрішніх справ України.

**Перспективами подальших наукових пошуків** визначаємо питання повноважень інших суб'єктів національної системи кібербезпеки.

### Використана література

1. Про рішення Ради національної безпеки і оборони України від 4.03.16 р. “Про Концепцію розвитку сектору безпеки і оборони України”: Указ Президента України від 14.03.16 р. № 92/2016. *Офіційний вісник України*. 2016. № 23. Ст. 898.
2. Про національну безпеку України: Закон України від 21.06.18 р. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.
3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.
4. Про затвердження плану заходів з проведення комплексного огляду сектору безпеки і оборони України та методичних рекомендацій щодо його проведення: Розпорядження Кабінету Міністрів України від 25.02.15 р. № 139-р. *Урядовий кур'єр*. 2015. № 41.
5. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”: Указ Президента України від 15.03.16 р. № 96/2016. *Офіційний вісник України*. 2016. № 23. Ст. 899.
6. Про контррозвідальну діяльність: Закон України від 26.12.02 р. № 374-IV. *Відомості Верховної Ради України*. 2003. № 12. Ст. 89.
7. Про Службу безпеки України: Закон України від 25.03.92 р. № 2229-XII. *Відомості Верховної Ради України*. 1992. № 27. Ст. 382.
8. Марущак А.І. Проблеми розслідування кіберзлочинів в Україні. *Економіка. Фінанси. Право*. 2018. № 1. С. 23-27.
9. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.05 р. № 2824-IV. *Відомості Верховної Ради України*. 2006. № 5. Ст. 71.

~~~~~ \* \* \* ~~~~~

УДК 355.402

**КРАВЧЕНКО Р.М.**, кандидат юридичних наук

**ЩОДО ДЕЯКИХ ПІДХОДІВ ДО ВДОСКОНАЛЕННЯ  
КОНТРРОЗВІДУВАЛЬНОГО ПОШУКУ ОРГАНІВ ВІЙСЬКОВОЇ  
КОНТРРОЗВІДКИ СБ УКРАЇНИ З УРАХУВАННЯМ  
АНАЛІЗУ ЗАКОНОДАВСТВА США**

**Анотація.** У статті проведено аналіз окремих нормативно-правових актів, що регулюють суспільні відносини в сфері контррозвідувального забезпечення Армії США, з метою виявлення правових рішень, які можуть бути адаптовані до національного законодавства в інтересах підвищення ефективності контррозвідувального пошуку органів військової контррозвідки СБУ.

**Ключові слова:** контррозвідувальне забезпечення, військова контррозвідка, структура, повноваження, розслідування, збройні сили США, контррозвідувальний пошук, контррозвідувальна обізнаність, інструктаж.

**Summary.** The article analyzes individual legal acts regulating public relations in the field of counterintelligence provision of the US Army in order to identify legal solutions that can be adapted to national legislation in order to increase the effectiveness of the counterintelligence search of the SSU military counterintelligence units.

**Keywords:** counterintelligence support, military counterintelligence, structure, authority, investigation, US armed forces, counterintelligence search, counterintelligence awareness, instruction.

**Аннотация.** В статье проведен анализ отдельных нормативно-правовых актов, которые регулируют общественные отношения в сфере контрразведывательного обеспечения Армии США, с целью выявления правовых решений, которые могут быть адаптированы к национальному законодательству в интересах повышения эффективности контрразведывательного поиска органов военной контрразведки СБУ.

**Ключевые слова:** контрразведывательное обеспечение, военная контрразведка, структура, полномочия, расследование, вооруженные силы США, контрразведывательный поиск, контрразведывательная осведомленность, инструктаж.

**Постановка проблеми.** Згідно із Законом України “Про контррозвідувальну діяльність”, Службі безпеки України надано право здійснювати контррозвідувальний пошук з використанням гласних контррозвідувальних заходів, які передбачають використання відкритих (офіційних) форм і методів роботи у сфері забезпечення державної безпеки, та негласних контррозвідувальних заходів, які здійснюються із залучення осіб, які конфіденційно співпрацюють з контррозвідувальними органами і підрозділами, а також з використанням оперативних, оперативно-технічних та спеціальних сил і засобів [1].

Контррозвідувальний пошук є невід’ємною складовою контррозвідувальної діяльності, в ході якої виявляються ознаки зовнішніх та внутрішніх загроз безпеці України тоді, коли ще не встановлено причетності до них конкретних осіб [2]. Одним зі способів підвищення ефективності контррозвідувального пошуку органів військової контррозвідки (далі – ВКР) СБ України є створення нових можливостей добування інформації про ознаки або факти розвідувальної, терористичної та іншої діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб,

спрямованої проти Збройних Сил України. Правові норми законодавств іноземних країн, що регулюють контррозвідувальний захист військових формувань, містять приклади вдалого вирішення цього завдання.

**Результати аналізу наукових публікацій.** Питання вдосконалення законодавчих основ здійснення контррозвідувальної діяльності в сучасному правовому суспільстві, в тому числі з урахуванням іноземного досвіду, постійно знаходяться в полі зору вітчизняних науковців і практиків. С.С. Кудінов, досліджуючи питання правового регулювання забезпечення СБ України антитерористичної безпеки, довів потребу підготовки населення до виявлення ознак терористичної діяльності та вдосконалення правового регулювання запобігання тероризму, як основоположний складник профілактики тероризму в Україні, що має знайти відображення у відповідних законодавчих та підзаконних нормативно-правових актах [3].

І.В. Авдошин, аналізуючи шляхи оптимізації контррозвідувальної системи США з попередження загроз підривного характеру, констатував, що зміна парадигми протидії розвідувально-підривним загрозам супроводжувалася прийняттям низки законів і інструкцій, уніфікацією вимог, підходів і процедури в сфері контррозвідувальної діяльності [4].

Сучасний стан правового регулювання контррозвідувального пізнання, як важливої складової контррозвідувальної діяльності, вивчав А.В. Ватраль і дійшов висновку, що усунення прогалин правового регулювання пізнавального процесу у контррозвідці є запорукою успішного вирішення завдань у сфері забезпечення державної безпеки України [5].

Водночас слід зазначити, що дослідження питань вдосконалення законодавчого врегулювання контррозвідувального пошуку, що здійснюється в межах контррозвідувального забезпечення Збройних Сил та інших військових формувань, створених відповідно до законодавства України, наразі не проводилося.

**Метою статті** є аналіз окремих нормативно-правових актів, що регулюють суспільні відносини в сфері контррозвідувального забезпечення Армії США, з метою виявлення правових рішень, які можуть бути адаптовані до національного законодавства в інтересах підвищення ефективності контррозвідувального пошуку органів військової контррозвідки СБУ.

**Виклад основного матеріалу.** Аналіз іноземних нормативно-правових актів свідчить про наявність прикладів суттєвого розширення можливостей отримання органами військової контррозвідки інформації, що належить до їх компетенції, за рахунок правового закріплення обов'язку кожного військовослужбовця, працівника та найманого співробітника збройних сил проходити контррозвідувальні інструктажі й навчання, а також повідомляти відповідним підрозділам ВКР інформацію про факти та ознаки розвідувальної, терористичної та іншої підривної діяльності. При цьому такий обов'язок підкріплюється функцією командирів всіх рівнів здійснювати контроль за його виконанням, а також можливістю настання для порушників правових наслідків у вигляді адміністративної та дисциплінарної відповідальності. Таким чином, в результаті реалізації вказаного механізму забезпечується систематичний профілактичний вплив на весь особовий склад збройних сил, а кожний його представник в обов'язковому порядку стає джерелом надходження контррозвідувальної інформації.

“Програма контррозвідувальної обізнаності та інструктажу”, яка була введена в дію Інструкцією Департаменту оборони США № 5240.6, вперше ввела в обіг термін “контррозвідувальна обізнаність” (Counterintelligence Awareness) [6]. Зі змісту цієї Програми вбачається, що контррозвідувальна обізнаність передбачає, по-перше,

проведення підрозділами, що виконують функції військової контррозвідки в Департаменті Оборони та Армії США, інструктажів всього особового складу, а також суб'єктів господарювання, які виконують роботи чи надають послуги оборонного характеру, з метою доведення інформації про загрози в сфері протидії іноземній розвідувальній і терористичній діяльності, а по-друге обов'язок військовослужбовців та працівників надавати до вказаних підрозділів передбачену інструктажами інформацію.

Безпосереднє формулювання терміна “контррозвідувальна обізнаність” містить Директива Департаменту оборони № 5240.06, яка визначає її як рівень усвідомлення особою інформації про загрози, методи та ознаки діяльності іноземних розвідувальних служб, а також вимоги доповідати про таку інформацію [7].

Інструкція № 5240.6 встановлює, що військовослужбовці дійсної служби та резерву, а також цивільні працівники Армії США повинні доповідати командуванню та до органів військової контррозвідки інформацію про всі контакти та події, які можуть становити загрозу особовому складу, майну, таємній та чутливій інформації. Суб'єкти господарської діяльності, що виконують контракти в сфері оборони, також зобов'язані повідомляти таку інформацію до ФБР або Служби розслідувань Департаменту оборони.

Весь особовий склад Армії повинен проходити періодичні інструктажі стосовно загроз з боку іноземних спецслужб, іноземних підприємницьких структур, терористичних організацій, незаконного втручання в роботу комп'ютерів та розголошення інформації. В межах цих інструктажів доводиться інформація стосовно іноземних розвідувальних служб, цілей їхньої діяльності, методів проведення розвідувальних операцій, кадрових співробітників, способів підтримання зв'язку, фінансування, міжнародного тероризму та споріднених загроз безпеці особового складу, майну збройних сил та інформації військового характеру.

Особовий склад Армії повинен надавати (усно чи письмово) до органів військової контррозвідки інформацію стосовно власних контактів (у формі зустрічей, особистого спілкування, з використанням радіо-, телефонного зв'язку, листування, чи в інший спосіб, незалежно від того, хто започаткував контакт, а також його соціальної, офіційної чи приватної основи) з особами (незалежно від громадянства), які пропонували: співробітництво з іноземною спецслужбою чи терористичною організацією з метою участі у проведенні ними розвідувальної діяльності, надання несанкціонованого доступу до таємної чи іншої інформації з обмеженим доступом; з встановленими чи ймовірними співробітниками розвідки будь-якої країни; з членами іноземних дипломатичних представництв в будь-якій країні на офіційній чи приватній основі. Також підлягає доповіді інформація про діяльність, що стосується шпигунства, тероризму, незаконної передачі технологій, саботажу, антиурядової агітації, диверсії, зради, розголошення таємної чи нетаємної контрольованої інформації, несанкціонованого втручання в автоматизовані інформаційні системи.

В разі невиконання вказаних вимог, до винних осіб можуть бути застосовані норми, які передбачають юридичну та/або адміністративну відповідальність згідно з Кодексом військової юстиції.

За результатами аналізу повідомлень, що надійшли від особового складу, щорічно органами військової контррозвідки здійснюється аналіз та узагальнення інформації за наступними категоріями:

Категорія І. Доповіді про контакти чи запити інформації, причетність до яких іноземної розвідувальної служби підтверджена.

Категорія ІІ. Доповіді про контакти чи запити інформації, причетність до яких іноземної розвідувальної служби є ймовірною (імовірність ґрунтується на даних про

прізвище особи, яка встановила контакт, зовнішній опис, застосовані методи, характер інформації, до якої проявлений інтерес).

Категорія III. Доповіді про намагання отримати таємну чи іншу інформацію з обмеженим доступом поза офіційними каналами чи встановленими процедурами, причетність до яких іноземної розвідувальної служби є мало ймовірною.

Категорія V. Доповіді про міжнародні чи внутрішньодержавні терористичні групи чи окремих терористів, які становлять загрозу особовому складу та майну збройних сил.

Категорія VI. Доповіді про навмисну компрометацію таємної інформації військовослужбовцями чи працівниками збройних сил, а також її передачу стороннім особам.

Інформація, отримана за вказаними категоріями підлягає обліку для забезпечення контролю та оцінки ефективності реалізації Програми, в тому числі проведених на підставі неї контррозвідувальних розслідувань та операцій. Результати аналізу та узагальнення річних підсумків реалізації програми повинні доповідатися керівництву Контррозвідки Армії.

Як бачимо, отримана в порядку виконання Інструкції № 5240.6 інформація складає ґрунтовну і, що найважливіше, достатню об'єктивну сукупність емпіричних даних для проведення контррозвідувального аналізу. При цьому Директива Департаменту оборони № 5240.02 визначає, що контррозвідувальний аналіз – це процес вивчення та оцінки інформації, спрямований на визначення природи, функцій, взаємозв'язків, учасників та намірів, що стосуються можливостей іноземних розвідувальних служб [8].

Іншим нормативно-правовим актом, який передбачає участь усього особового складу Армії США у своєчасному виявленні та попередженні розвідувально-підривної діяльності, є Інструкція № 381-12 “Диверсія та шпигунство, спрямовані проти Армії США” [9]. Цим документом регламентується проведення контррозвідувальних тренувань, а також встановлюються обов'язки командирів щодо контролю за виконанням вимог Інструкції підлеглими. Дається визначення, що контррозвідувальний пошук – це систематичне отримання інформації, що стосується шпигунства, саботажу, тероризму та споріднених видів діяльності, що здійснюються іноземними державами, організаціями чи особами і спрямовані проти інтересів оборони.

Згідно з Інструкцією, діючі військовослужбовці Армії, Національної гвардії, Резервної армії США, цивільний персонал, працівники суб'єктів господарювання, які виконують контракти оборонного призначення, та наймані іноземні працівники підрозділів та установ Армії США за кордоном повинні проходити контррозвідувальне тренування принаймні один раз на рік. Зміст тренування може варіюватись у залежності від категорії осіб, з якими він проводиться, та географічного положення, в умовах якого відбувається несення військової служби. В ході тренування може використовуватись нетаємна інформація для широкої аудиторії, а також таємні відомості для визначених категорій осіб.

Тренування повинно містити наступні складові:

1) Доведення, що іноземні розвідувальні служби вважають особовий склад Армії цінним джерелом таємної і чутливої інформації. Пояснення про те, як це стосується підрозділу чи виду діяльності, до якої мають відношення учасники тренування;

2) Роз'яснення видів кримінального покарання за шпигунство, передбачених Кодексом США та Об'єднаним кодексом Військової юстиції; наведення прикладів засудження осіб за шпигунство, призначених покарань, у тому числі допустимості смертної кари;

3) Розкриття, зокрема, на конкретних прикладах, методів і технік, які застосовуються іноземними розвідками для втягування осіб у залежність, збирання інформації про спроможності, бойове застосування, особовий склад і технології; специфіка підходів під “чужим прапором”;

4) Види ситуацій (обставин) про які необхідно доповідати та ознаки шпигунства;

5) Характер збитків, які можуть бути завдані внаслідок шпигунства;

6) Попередження про дисциплінарну відповідальність, яка може бути застосована до особи в разі недотримання вимог Інструкції;

7) Доведення порядку надання доповіді про виявлені факти і ознаки;

8) Роз'яснення загроз внутрішнього та міжнародного тероризму щодо особового складу та членів родин, методи попередження та уникнення шкідливих наслідків;

9) Визначення розвідувальних загроз, які можуть становити недержавні розвідувальні служби та організації, що здійснюють міжнародний наркотрафік.

Інструкція визначає категорії інформації або ситуацій, які потребують доповіді:

1) Спроби неуповноважених осіб отримати таємну чи нетаємну інформацію щодо спроможностей, персоналу, діяльності, технологій збройних сил шляхом опитування, вивідування, введення в оману, підкупу, погроз, шантажування, фотографування, спостереження, збирання документів чи матеріалів, проникнення до комп'ютерів;

2) Відомі, підозрілі чи ймовірні шпигунські дії представника особового складу Армії США;

3) Контакти військовослужбовців та працівників збройних сил або членів їх родин з особами, підозрюваними у причетності до іноземних спецслужб чи терористичних організацій;

4) Контакти представників особового складу Армії з будь-якими іноземними громадянами, якщо вони виявляють надмірне володіння інформацією чи невинуватий інтерес до представників особового складу Армії або їх обов'язків, американських технологій, досліджень, випробувань, систем озброєння чи наукової інформації; намагаються отримати таємну чи нетаємну інформацію; створити умови залежності представника особового складу Армії США через особливе ставлення, надання переваг, подарунків, грошей чи в інший спосіб; започатковують будь-які підприємницькі відносини, що виходять за межі їх офіційних обов'язків;

5) Випадки, коли під час перебування за кордоном військовослужбовцям або членам їх родин пропонують розповісти про свої службові обов'язки, надати інформацію військового характеру, розпочати співробітництво з іноземним урядом чи розвідкою із застосуванням погроз або тиску будь-якого характеру;

6) Інформація стосовно будь-якої внутрішньодержавної чи міжнародної терористичної діяльності чи саботажу, незаконної передачі за кордон американських технологій;

7) Відомі або ймовірні факти зради з боку військовослужбовців Армії США, заклики до захоплення державної влади неконституційним шляхом;

8) Відомі або ймовірні факти несанкціонованого втручання у військові таємні або нетаємні автоматизовані інформаційні системи;

9) Використання родичів, що мешкають за кордоном з метою здійснення впливу чи тиску на військовослужбовців Армії США;

10) Виявлення в приміщеннях, де запроваджені заходи безпеки, підозрілих підслуховуючих пристроїв чи інших засобів технічного спостереження;

11) Безпідставна відсутність за місцем служби (роботи) військовослужбовців, які мали доступ до інформації з обмеженим доступом, криптографічних даних;

12) Самогубства чи спроби покінчити з життям з боку військовослужбовців, які протягом останнього року мали доступ до інформації з обмеженим доступом;

13) Порухення заходів комп'ютерної безпеки;

14) Факти та наміри військовослужбовців, працівників збройних сил здійснити перехід на бік ворога в період воєнного стану або в умовах збройного конфлікту.

Також Інструкція вимагає надання доповідей у разі виявлення ознак шпигунства:

1) Будь-які спроби отримати розширений доступ до таємної інформації шляхом наполегливого намагання зайняти відповідну посаду чи виконання обов'язків понад встановлений обсяг, а також спроби ознайомитися з відомостями, що виходять за межі наданого доступу;

2) Безпідставне переміщення таємних матеріалів з робочого місця, або їх зберігання в особистому автотранспорті та за місцем мешкання;

3) Використання копіювальної, факсимільної або комп'ютерної техніки для розмноження чи передачі таємних матеріалів, що не пов'язано зі службовою необхідністю;

4) Повторне і не викликане потребою залишення на роботі понад норми робочого часу, особливо наодинці;

5) Підписання документів про анулювання таємних матеріалів без фактичної присутності при їх знищенні;

6) Занесення засобів реєстрації інформації (відеокамер, записуючих пристроїв, комп'ютерів чи модемів) у приміщення, де зберігається, обробляється чи обговорюється таємна інформація;

7) Немотивоване різке покращення майнового стану (придбання нерухомості, транспортних засобів, коштовного відпочинку, покриття великих боргів, кредитів), намагання пояснити це отриманням спадку, виграшом, прибутковим бізнесом;

8) Відкриття декількох банківських рахунків зі значними сумами коштів, без об'єктивного пояснення їх походження;

9) Часті, нетривалі виїзди до іноземних країн;

10) Намагання запропонувати додатковий дохід від імені сторонньої зацікавленої особи військовослужбовцю, який має доступ до чутливої інформації, або втягування його в кримінальну ситуацію, яка може призвести до підкупу;

11) Неодноразові порушення заходів безпеки;

12) Жартування на тему співробітництва з іноземною спецслужбою, відвідання іноземних дипломатичних установ, консульств, торгових чи прес-офісів.

Закріплена Інструкцією процедура надання доповіді передбачає наступний порядок.

1. Особи, які є учасниками або володіють інформацією про випадки, описані Інструкцією, повинні негайно доповідати до найближчого контррозвідального офісу. Якщо це не є представляється можливим, то інформація повинна надаватись офіцеру безпеки чи командуванню, які зобов'язані протягом 24-х годин передати її до підрозділу контррозвідки.

2. Доповідь повинна містити максимально деталізовану інформацію, ні за яких обставин не дозволяється проводити власне розслідування чи переслідувати підозрюваного. В разі надходження особі пропозиції про співробітництво, відповідь повинна бути ухильною, не містити ні згоди, ні відмови.

3. В період перебування за кордоном, особи, в разі термінової потреби (наявності загрози життю чи майну), повинні надавати інформацію найближчій військовій посадовій особі, офіцеру розвідки чи безпеки, військовому аташат, до американського

посольства чи консульства. В іншому випадку, доповідь повинна надаватися до контррозвідувального підрозділу після повернення з-за кордону.

Заслуговує на увагу, що в межах реалізації Інструкції № 381-12 на командирів всіх рівнів покладаються наступні обов'язки:

1) Забезпечувати надання підлеглим особовим складом доповідей до відповідних контррозвідувальних підрозділів щодо фактів та ознак шпигунства, диверсії, інших визначених Інструкцією ситуацій;

2) Вживати належних заходів, аби інформація за визначеними Інструкцією категоріями надходила безпосередньо до контррозвідувальних підрозділів, а не по лінії військового командування, аби не зашкодити можливому проведенню подальшого розслідування;

3) Включати контррозвідувальні тренування до всіх інших тренувальних програм, в тому числі поєднувати їх з тренуваннями з питань безпеки. Забезпечувати щорічне проходження контррозвідувального тренування військовослужбовцями та працівниками Армії;

4) Здійснювати моніторинг якості та ефективності контррозвідувальних тренувань.

За результатами виконання Інструкції складається щорічний звіт, який містить наступну інформацію:

1) Кількість представників особового складу, які пройшли щорічне контррозвідувальне тренування;

2) Кількість доповідей, що надійшли за визначеними Інструкцією категоріями;

3) Кількість розслідувань, які були розпочаті на підставі наданих доповідей;

4) Кількість розслідувань, які мали результатами:

- Планування і проведення контррозвідувальних операцій;
- Підтверджені випадки шпигунства;
- Підтверджене несанкціоноване розголошення інформації з обмеженим доступом;
- Призначення кримінальних та адміністративних покарань особам, винним у здійсненні шпигунства чи пов'язаних з ним правопорушень;
- Призначення адміністративних чи іншого роду покарань за ненадання передбачених Інструкцією доповідей;
- Призначення адміністративних чи іншого роду покарань за інші порушення, які були виявлені в результаті доповідей, наданих згідно Інструкції;

5) Кількість доповідей щодо терористичних загроз Армії США та іншим національним інтересам;

6) Кількість спроб та фактів несанкціонованого втручання в автоматизовані системи Армії.

Американське законодавство в сфері оборони також містить норми, які встановлюють вимоги щодо надання доповідей до контррозвідувальних підрозділів Армії про ознаки, контакти, поведінку та діяльність, пов'язані з тероризмом, а також кіберзагрози, до яких можуть бути причетні іноземні спецслужби. Зокрема, Директива Департаменту оборони № 5240.06 зобов'язує доповідати про наступне [7].

1) Виправдування насильства, погроз насильства, або застосування сили для досягнення цілей в інтересах відомих чи підозрюваних міжнародних терористичних організацій, прояви підтримки цих організацій;

2) Надання фінансової чи іншої матеріальної підтримки відомим чи підозрюваним міжнародними терористичним організаціям чи міжнародним терористам;

3) Передача обладнання чи знаряддя, придбання складових для виготовлення бомб, отримання інформації про конструкцію вибухових пристроїв в інтересах відомих чи підозрюваних міжнародних терористичних організацій;



- 4) Підтримання контактів з терористичними організаціями, в тому числі через соціальні мережі, збір інформації в їх інтересах;
- 5) Спроби завербувати інших осіб для участі в терористичній діяльності;
- 6) Родинні або інші зв'язки з членами терористичних організацій;
- 7) Відвідання веб-сайтів міжнародних терористичних організацій, які пропагують насильство, не пов'язане з виконанням службових обов'язків;
- 8) Злам паролів, акаунтів, розмежування доступу, криптозахисту;
- 9) Витік чи компрометація комп'ютерної інформації;
- 10) Впровадження в інформаційні системи непередбачених програмних чи технічних елементів;
- 11) Несанкціоноване завантаження чутливої комп'ютерної інформації, а також впровадження несанкціонованих комп'ютерних програм;
- 12) Несанкціонований мережевий доступ, електронне листування на адреси, розташовані на іноземних серверах;
- 13) DOS-атаки чи підозрілі мережеві помилки;
- 14) Передача даних до недозволених доменів;
- 15) Безпідставне накопичення криптованої інформації;
- 16) Соціальний інжиніринг, фішінг, підлаштування хибних електронних адрес;
- 17) Виявлення вірусів, комп'ютерних хробаків, троянів, логічних бомб, інших шкідливих програм.

### **Висновки.**

Таким чином, у теперішній час військовослужбовці Збройних Сил України та інших військових формувань фактично не мають нормативно визначених обов'язків у сфері контррозвідувального режиму, крім зобов'язань, які виникають в зв'язку з отриманням допуску до державної таємниці. Водночас нині існує необхідність вжиття дієвих заходів щодо вдосконалення загальнодержавної системи забезпечення контррозвідувального режиму в Україні, про що свідчить затвердження Указом Президента України від 6 жовтня 2017 року № 310/2017 Концепції забезпечення контррозвідувального режиму в Україні [10]. Відтак вбачається, що одним з напрямків підвищення ефективності контррозвідувального режиму є внесення змін до законодавчих актів України в частині визначення завдань, повноважень та функцій суб'єктів системи забезпечення контррозвідувального режиму в Україні, а також посилення юридичної відповідальності фізичних та юридичних осіб за порушення у сфері дії окремих елементів контррозвідувального режиму в Україні.

Упровадження норм, аналогічних вищевизначеним, у законодавство України, зокрема у відомчі нормативні акти Міністерства оборони, Збройних Сил та Служби безпеки України, а також накази та розпорядження, які мають міжвідомчий характер, може мати суттєве значення для посилення контррозвідувального режиму та підвищення ефективності контррозвідувального пошуку органами військової контррозвідки СБ України.

### **Використана література**

1. Про контррозвідувальну діяльність: Закон України. *Відомості Верховної Ради України*. 2003. № 12. Ст. 89.
2. Про внесення змін до законів України, що регулюють оперативно-розшукову та контррозвідувальну діяльність: пояснювальна записка до проекту Закону України. URL: <http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=54666&pf35401=336780>

3. Кудінов С.С. Шляхи удосконалення правового регулювання забезпечення Службою безпеки України Антитерористичної операції. URL: <http://pgp-journal.kiev.ua/archive/2019/2/45.pdf>
4. Авдошин І.В. Оптимізація контррозвідувальної системи США з попередження загроз підривного характеру. URL: <http://science.univ.kiev.ua/sbu.pdf>
5. Ватраль А.В. Сучасний стан правового регулювання контррозвідувального пізнання. URL: [http://pravoisuspilstvo.org.ua/archive/2017/5\\_2017/part\\_2/53.pdf](http://pravoisuspilstvo.org.ua/archive/2017/5_2017/part_2/53.pdf)
6. Department of Defense INSTRUCTION NUMBER 5240.6 July 16, 1996 Counterintelligence (CI) Awareness and Briefing Program. URL: [www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/524006p.pdf](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/524006p.pdf)
7. Department of Defense DIRECTIVE NUMBER 5240.06. URL: [https://fas.org/irp/doddir/dod/d5240\\_06.pdf](https://fas.org/irp/doddir/dod/d5240_06.pdf)
8. Department of Defense DIRECTIVE NUMBER 5240.02. URL: [https://fas.org/irp/doddir/dod/d5240\\_02.pdf](https://fas.org/irp/doddir/dod/d5240_02.pdf)
9. Army Regulation 381-12. Subversion and Espionage Directed Against the U.S. Army (SAEDA). URL: <https://fas.org/irp/doddir/army/ar381-12-1993.pdf>
10. Про рішення Ради національної безпеки і оборони України від 13 вересня 2017 року “Про Концепцію забезпечення контррозвідувального режиму в Україні”: Указ Президента України від 6.10.17 р. № 310/2017. URL: <http://zakon4.rada.gov.ua>

~~~~~ \* \* \* ~~~~~

УДК 342.9

**КУЛЕШОВ М.В.**, перший заступник начальника  
ДКІБ Служби безпеки України

## **СУТНІСТЬ ТА ЗМІСТ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ ТА КІБЕРАТАК ПІДРОЗДІЛАМИ СБ УКРАЇНИ**

**Анотація.** У статті здійснено аналіз змісту діяльності з розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури, проведено відмежування такого розслідування від досудового слідства, а також визначено загальний обсяг повноважень співробітників СБ України, залучених до цього процесу.

**Ключові слова:** забезпечення кібербезпеки, розслідування кіберінцидентів та кібератак, повноваження підрозділів СБ України.

**Summary.** The article analyzes the nature of the investigation of cyberincidents and cyberattacks on state electronic information resources, information the protection of which is required by law, critical information infrastructure, delimitates such an investigation from the pre-trial investigation, and also determines the total amount of responsibilities of the SSU officers involved in this activity.

**Keywords:** ensuring cybersecurity, investigation of cyberincidents and cyberattacks, the responsibilities of the officers of the Security Service of Ukraine.

**Аннотация.** В статье осуществлён анализ содержания деятельности по расследованию киберинцидентов и кибератак государственных электронных информационных ресурсов, информации, требование по защите, которой установлено законом, критической информационной инфраструктуры, проведено отграничение такого расследования от досудебного следствия, а также определён общий объём полномочий сотрудников СБ Украины, вовлечённых в эту деятельность.

**Ключевые слова:** обеспечение кибербезопасности, расследование киберинцидентов и кибератак, полномочия подразделений СБ Украины.

**Постановка проблеми.** У зв'язку із прийняттям Закону України "Про основні засади забезпечення кібербезпеки України", формуванням системи суб'єктів забезпечення кібербезпеки й розподілом відповідних функцій та повноважень між ними, законодавцем було введено ряд понять та категорій, які потребують інтегрування у вже існуючу модель правоохоронної діяльності. Наразі визначення сутності та змісту потребує діяльність з розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури, оскільки завдання щодо здійснення таких розслідувань були поставлені Службі безпеки України відносно недавно, а процесуальна форма цієї діяльності ще не була сформована. Окремим проблемним аспектом є визначення загального змісту повноважень співробітників СБ України, які проводять такі розслідування.

Відсутність нормативного регулювання процесу розслідування кіберінцидентів та кібератак підрозділами СБ України не дозволяє повною мірою застосовувати наявний потенціал сил та засобів з протидії зазначеним негативним явищам в кіберпросторі, що негативно позначається на виконанні завдань щодо захисту інформаційної безпеки та її складової – кібербезпеки. А, як зазначає І.П. Бахновська, нині національна безпека

значною мірою залежить від забезпечення інформаційної безпеки, оскільки захищеність інформації та її повнота впливають на стабільність у суспільстві, забезпечення прав і свобод громадян, правопорядок і навіть на збереження цілісності держави [1, с. 106].

**Результати аналізу наукових публікацій.** Наразі наукові публікації, які стосуються саме сутності, змісту й нормативно-правового регулювання розслідування кіберінцидентів та кібератак відсутні, що свідчить про актуальність дослідження обраної тематики. Окремі аспекти досліджуваної теми розкриті в наукових працях наступних вчених.

Так, технічні питання забезпечення кібербезпеки України досліджували О.Ю. Козлова, В.Г. Кононович, І.В. Кононович, М.Г. Романюков, Л.М. Тимошенко. Соціальні, правові та інші аспекти забезпечення кібербезпеки розкрито І.П. Бахновською, С.А. Вітер, І.В. Діордіцею, М.М. Присяжнюком, І.І. Світличним, О.В. Ставицьким, Є.І. Цифрою та А.Ю. Шинкаренком та ін.

Проте, незважаючи на значний масив наукових розвідок в сфері забезпечення інформаційної безпеки та кібербезпеки, питання сутності та змісту, а також нормативно-правового регулювання розслідування кіберінцидентів та кібератак залишились поза увагою науковців, що обумовлює важливість обраної теми.

**Метою статті** є науково-практичний аналіз сутності розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури, виділення сутності та визначення загального змісту дій співробітників СБ України в контексті такого розслідування.

**Виклад основного матеріалу.** Згідно розділу 2 Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96/2016, сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах критичної інфраструктури. Більшого поширення набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні веб-сайти в мережі Інтернет. При цьому дедалі частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій. Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для скоєння принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації.

Враховуючи реалії сьогодення та характер існуючих загроз у сфері кібербезпеки, з метою практичного виконання завдань з реалізації курсу України на європейську та євроатлантичну інтеграцію, впровадження в систему планування єдиних процедур та правил, необхідних для підвищення ефективності сектору безпеки і оборони, для нейтралізації реальних та потенційних загроз національній безпеці України, дотримання цілісності, узгодженості та системності в опрацюванні документів за сферами національної безпеки, а також вжиття комплексу невідкладних заходів, спрямованих на підвищення обороноздатності держави з урахуванням наявних державних ресурсів, Кабінету Міністрів України, окрім іншого, доручено:

- забезпечити проведення оборонного огляду, огляду громадської безпеки та цивільного захисту, огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом;

- затвердити до 30 червня 2019 року порядки проведення огляду громадської безпеки та цивільного захисту і огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом [2].

Наведене вище свідчить про усвідомлення необхідності захисту кібербезпеки як складової інформаційної безпеки та спрямування зусиль суб'єктів національної системи кібербезпеки на виконання першочергових завдань, визначених нормативними актами, що регулюють забезпечення національної безпеки.

Відповідно до ст. 8 Закону України “Про основні засади забезпечення кібербезпеки України” (надалі – Закон), Служба безпеки України є одним із основних суб'єктів національної системи кібербезпеки, який, відповідно до Конституції і законів України виконує в установленому порядку такі основні завдання: здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки.

В сучасному кіберпросторі кібератаки використовуються вже не тільки приватними особами, але й спецслужбами іноземних держав. І тут необхідно погодитись з І.В. Логіновим, Н.А. Ткачук та В.М. Удовиченком в тому, що “кібератаки, вмотивовані державою та спрямовані на викрадення інформації з обмеженим доступом, знищення, викривлення важливих для інших країн інформаційних ресурсів або блокування доступу до них з метою отримання політичних, економічних, військових переваг у зовнішньоекономічних стосунках, у мирний час становлять одну з сучасних форм розвідувально-підривної діяльності, а після оголошення стану війни можуть перетворитися на форму військових дій” [3, с. 105].

Окремо необхідно зазначити, що кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури, можуть здійснюватися в межах спеціальних інформаційних операцій, які проводяться країною-агресором останні роки. Досліджуючи інформаційно-правове забезпечення спеціальних інформаційних операцій, О.О. Верголяс визначив наступні прийоми протидії в інформаційній війні: одержання інформації про супротивника як у результаті аналізу відкритої інформації, що циркулює в ЗМІ, інформаційних системах тощо, так і в результаті її перехоплення, несанкціонованого доступу з наступним викривленням, знищенням, “перекодуванням” з метою формування оцінки, наміру й орієнтацій населення й осіб, що ухвалюють стратегічні рішення; придушення елементів інфраструктури державного й військового управління; радіоелектронна боротьба тощо. Методи інформаційної війни надзвичайно різноманітні: дезінформація, пропаганда, наклеп, неправда, приховування істотної інформації, зсув понять, відволікання уваги, інформаційне табування й інші [4, с. 128].

Фактично, враховуючи наведені вище обставини, діяльність, яка полягає в розслідуванні кіберінцидентів та кібератак і встановлення їх механізму, обставин, засобів, знарядь та виконавців, не може здійснюватись в межах захисту інформації штатними співробітниками підприємств, установ та організацій, а результати їх

діяльності в подальшому досить складно використати в межах розслідування кримінального провадження. Так, наприклад, С.А. Вітер та І.І. Світличин, досліджуючи модель існування спецслужби з кібербезпеки, яку можуть представляти фахівці з організації інформаційної безпеки та проведення тестування на проникнення, інспектори з організації захисту секретної інформації, аналітики проектів із кібербезпеки, системні адміністратори, адміністратори комп'ютерних мереж, менеджери систем з інформаційної безпеки, аналітики систем забезпечення кібербезпеки, відносять до обов'язків таких фахівців наступне:

- виявлення уразливих місць системи та моделювання можливої ситуації стороннього кібервпливу з позиції загроз і пов'язаних із ними ризиків;
- контроль надійності функціонування системи захисту облікової інформації, розроблення заходів безпеки на випадок непередбачуваних подій;
- віднесення облікової інформації до категорії обмеженого доступу (службової і комерційної таємниць, іншої конфіденційної інформації);
- розроблення положень, політики і процедур у рамках системи безпеки облікової інформації;
- упровадження розроблених заходів безпеки та випробування системи з оцінкою її результативності, за необхідності внесення коригувань;
- встановлення користувачам комп'ютерної системи бухгалтерського обліку необхідних реквізитів захисту;
- навчання користувачів комп'ютерної інформаційної системи правилам безперервної обробки інформації;
- контроль за дотриманням користувачами комп'ютерної інформаційної системи та персоналом підприємства встановлених правил роботи з обліковою інформацією, що захищається у процесі її автоматизованої обробки [5, с. 501]

Як бачимо, повноваження чи обов'язки щодо розслідування кіберінцидентів та кібератак в наведеній моделі відсутні. Окрім того, внаслідок дій системних адміністраторів безпеки можуть бути втрачені чи перекручені дані і сліди протиправної діяльності, що унеможливить притягнення до відповідальності винних осіб чи подальше використання інформації про кіберінцидент чи кібератаку в оперативних та контррозвідальних цілях.

Що ж стосується кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури, то вони здатні спричинити реальну шкоду охоронюваним законом інтересам у сфері державної безпеки, з огляду на що важливість первинної діяльності, спрямованої на виявлення слідів протиправних дій та належного документування, складно переоцінити. Іншими словами, коли інтереси держави опиняються під загрозою спричинення значної шкоди особою, яка вчиняє протиправні дії у кіберпросторі, протидію такій діяльності та її розслідування повинен здійснювати суб'єкт забезпечення кібербезпеки.

Визначення кіберінцидентів та кібератак закріплено в п. 3 та 4 ст. 1 Закону. Так, кіберінцидентом визнається подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи,

та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Кібератака ж визначається як спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту. Як зазначає Р.В. Киричок, кібератака або хакерська атака (у вузькому розумінні) – це спроба реалізації загрози кіберзловмисниками (хакерами). Використовуючи різноманітні комбінації виявлених вразливостей, недоліки конфігураційних файлів систем та прогалини визначеної в корпорації політики безпеки, в залежності від своїх цілей, зловмисники можуть реалізувати різноманітні сценарії та навіть цілі стратегії нападу, при цьому залишившись непоміченими. Дані стратегії можуть бути спрямовані на різні ресурси КІС та включати багатоетапні ланцюги атакуючих дій, які в більшості випадків розпочинаються з імпортування та встановлення вірусів чи троянів на комп'ютери компаній через мережу Інтернет або надсилання шкідливих сценаріїв за допомогою електронної пошти, що дозволяє зловмисникам практично з легкістю заражати свої бажані цілі [6, с. 53-54].

Враховуючи, що здійснення кібератак та виникнення кіберінцидентів пов'язане з кваліфікованими діями осіб, які спеціалізуються на використанні кіберпростору, супроводжується застосуванням спеціалізованого технічного обладнання та шкідливого програмного забезпечення, процес розслідування зазначених кіберподій має складатись із взаємопов'язаних дій та заходів, спрямованих як на збирання конкретних даних, припинення шкідливої дії кіберінцидента чи кібератаки, так і удосконалення існуючої моделі та системи захисту з метою недопущення вчинення аналогічних дій в майбутньому. Саме в цьому контексті процес розслідування кібератак та кіберінцидентів відрізняється від процесу розслідування в кримінальному процесуальному розумінні.

Згідно п. 5 ч. 1 ст. 3 Кримінального процесуального кодексу України, досудове розслідування – стадія кримінального провадження, яка починається з моменту внесення відомостей про кримінальне правопорушення до Єдиного реєстру досудових розслідувань і закінчується закриттям кримінального провадження або направленням до суду обвинувального акта, клопотання про застосування примусових заходів медичного або виховного характеру, клопотання про звільнення особи від кримінальної відповідальності. Цілком очевидним є той факт, що досудове розслідування і розслідування кіберінцидентів та кібератак – це не тотожні поняття, оскільки не кожен кіберінцидент містить ознаки кримінального правопорушення, та не кожна кібератака може стати предметом розслідування.

Проаналізуємо відмінності процесу досудового розслідування та розслідування кібератак та кіберінцидентів.

1. Суб'єктом, який здійснює досудове слідство, є слідчий, суб'єктом здійснення розслідування кіберінцидентів та кібератак може бути співробітник функціонального підрозділу з контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБ України.

2. Не кожен кіберінцидент містить ознаки кримінального правопорушення. В залежності від обставин, механізму виникнення та наявності людського фактору кіберінциденти умовно можна поділити на наступні категорії: 1) прості кіберінциденти – подія або ряд несприятливих подій ненавмисного характеру, настання яких виключає дію людського фактору (КІК-4); 2) ускладнені кіберінциденти – подія або ряд несприятливих подій, настання яких супроводжувалось умисними чи необережними діями осіб поза кіберпростором (КІК-3) або у кіберпросторі (КІК-2), за відсутності ознак кібератаки; 3) кібератаки – активна та цілеспрямована форма кіберінцидента, механізм виникнення якої включає умисні та цілеспрямовані дії осіб, вчинені з метою досягнення результату, передбаченого п. 4 ст. 1 Закону (КІК-1).

При цьому кіберінциденти категорії КІК-4 взагалі виключають наявність суб'єкта злочину, кіберінциденти КІК-3 та КІК-3 можуть містити ознаки тих або інших кримінальних правопорушень, а можуть і не містити. Разом з тим вимога законодавця щодо розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури, є прямою, з огляду на що процес такого розслідування має бути розпочатий в кожному випадку отримання інформації про кіберінцидент.

3. Навіть у випадку, коли наявні ознаки вчиненого кримінального правопорушення, не кожна інформація про кіберінцидент чи кібератаку може бути внесена до ЄРДР, оскільки, наприклад, у випадку, коли фактично вчинені дії утворюють склад злочину, передбаченого ч. 1 ст. 361 КК України, відповідно до вимог ч. 1 ст. 477 КПК України, провадження може бути розпочате слідчим, прокурором лише на підставі заяви потерпілого щодо кримінального правопорушення (кримінальне провадження у формі приватного обвинувачення). При цьому, як і в попередньому випадку, існує вимога закону щодо розслідування такого кіберінцидента чи кібератаки.

4. Пріоритетним аргументом в прийнятті рішення щодо початку розслідування в разі отримання інформації про кіберінцидент або кібератаку є не вимоги щодо підслідності злочинів, передбачені ч. 2 ст. 216 КПК України, а саме характер об'єкта, на який здійснюється злочинне посягання, або предмета посягання. Розслідування співробітниками СБ України розпочинається лише у випадку, коли кіберінциденти та кібератаки здійснювались щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури

Наведені відмінності свідчать про те, що розслідування кіберінцидентів та кібератак здійснюється поза межами досудового слідства, тобто поза кримінальним процесом. Причиною цьому є те, що, як правильно підкреслюють автори коментаря Закону України “Про основні засади забезпечення кібербезпеки України”, “деякі види розвідувально-підривної діяльності у кіберпросторі (наприклад, добування розвідувальної інформації шляхом перехоплення й аналізу телекомунікаційного трафіку кіберрозвідками іноземних держав з позицій закордону, космічного простору, нейтральних вод) не можуть кваліфікуватись як протиправні діяння, і разом з тим несуть істотні загрози кібербезпеці держав, що розвідуються” [3, с. 105]. Саме цим пояснюється те, що діяльність з розслідування кіберінцидентів та кібератак зазначених об'єктів здійснюється саме в межах контррозвідувальної діяльності.

Разом з тим, якщо в ході розслідування буде встановлено, що виявлені події категорії КІК-3, КІК-2 та КІК-1 містять ознаки кримінального правопорушення, службова особа, яка призначила розслідування, має невідкладно повідомити про це орган досудового розслідування і вжити заходів щодо завершення розслідування,



складання висновку за його результатами та передачі матеріалів для прийняття процесуального рішення про внесення даних про виявлене кримінальне правопорушення у Єдиний реєстр досудових розслідувань.

Отже, задля встановлення змісту та обсягу повноважень суб'єктів, які здійснюють розслідування кіберінцидентів та кібератак, визначимо сутність цієї діяльності. Так, розслідування кібератак та кіберінцидентів – структурована сукупність дій та заходів, які здійснюються в межах забезпечення кібербезпеки України поза кримінальним процесом уповноваженими суб'єктами та спрямовані на встановлення механізму, обставин, засобів і знарядь та виконавців кіберінцидентів і кібератак, мінімізацію їх негативного впливу та шкідливих наслідків, а також вжиття заходів з попередження кіберінцидентів та кібератак у майбутньому.

Проведення розслідування кіберінцидентів та кібератак поза межами кримінального процесу означає, що особи, які його проводять, не можуть застосовувати інструментарій процесуальних, слідчих та негласних слідчих (розшукових) дій. Аналіз нормативно-правових актів, які регулюють оперативно-службову діяльність органів СБ України, дає підстави стверджувати, що з метою встановлення обставин, які підлягають з'ясуванню під час розслідування кібератак та кіберінцидентів, співробітники СБ України мають право: 1) здійснювати опитування осіб (за їх згодою отримуючи від них усні або письмові пояснення), які можуть повідомити будь-яку інформацію, що має значення для досягнення відповідних цілей розслідування; 2) отримувати від очевидців кіберінцидента чи кібератаки, службових осіб підприємства, установи, організації або інших громадян речі і документи, що мають значення для встановлення відповідних обставин кіберподії, яка є предметом розслідування; 3) отримувати у встановленому порядку дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків; 4) у порядку, погодженому із керівником підприємства, установи, організації, проводити візуальний і технічний огляд комп'ютерної та периферійної техніки, яка містить сліди кіберподії; 5) ознайомлюватись з документами та даними, що характеризують діяльність підприємств, установ та організацій, вивчати їх, за рахунок коштів, що виділяються на утримання підрозділів, які здійснюють оперативно-розшукову діяльність, виготовляти копії з таких документів, на вимогу керівників підприємств, установ та організацій – виключно на території таких підприємств, установ та організацій; 6) застосовувати спеціальне програмне забезпечення або технічні пристрої з метою отримання, збирання та накопичення інформації, необхідної для встановлення обставин кіберінцидента чи кібератаки; 7) залучати до проведення окремих заходів фахівців СБ України, проводити з ними консультації та отримувати від них письмові висновки щодо предмета розслідування; 8) здійснювати комп'ютерно-технічне дослідження а) зразків цифрової інформації, отриманої у ході ознайомлення з документами та даними, що характеризують діяльність підприємств, установ та організацій, б) комп'ютерної техніки, мережових апаратних засобів та їх комплектуючих, залучати до таких досліджень відповідних фахівців; 9) за наявності підстав, передбачених ст. 207 КПК України, затримувати особу, в діях якої вбачаються ознаки кримінального правопорушення, та тимчасово вилучати її майно з метою подальшої передачі затриманої особи та вилученого майна уповноваженій службовій особі для вирішення питання про внесення даних про виявлене кримінальне правопорушення в ЄРДР та оформлення процесуального затримання особи в порядку ст. 208 КПК України.

Необхідно враховувати також, що розслідування кіберінцидентів та кібератак підрозділами СБ України носить відкритий характер і здійснюється в межах захисту кібербезпеки України. Результати окремих заходів можуть використовуватись в оперативній і контррозвідувальній діяльності, якщо їх зміст відповідає таким потребам. Проте сам процесуальний порядок не визначений ні нормативно-правовими актами СБ України, ні чинним законодавством, що ускладнює реалізацію окремих повноважень та знижує ефективність протидії кіберзагрозам.

### **Висновки.**

В сучасних умовах законодавцем вживаються кроки щодо розширення механізму захисту кібербезпеки України як складової її інформаційної безпеки. Діяльність з розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури віднесена до завдань СБ України як суб'єкта національної системи кібербезпеки.

Проте, навіть поверхневий аналіз загального змісту прав та обов'язків співробітників СБ України дає підстави стверджувати, що, незважаючи на специфічну сферу, в якій проводиться розслідування кіберінцидентів та кібератак, та важливість забезпечення інформаційної безпеки як складової національної безпеки, законодавчі ініціативи в частині надання суб'єктам забезпечення кібербезпеки додаткових повноважень явно не відповідають потребам сьогодення. Тому подальші наукові розвідки, спрямовані на пошук альтернатив та перспектив розширення правоохоронних можливостей СБ України в частині забезпечення кібербезпеки, є актуальними та необхідними.

### **Використана література**

1. Бахновська І. П. Аналіз основних принципів забезпечення кібербезпеки в проекті Закону України “Про основні засади забезпечення кібербезпеки України”. *Науковий вісник Ужгородського національного університету. Серія “Право”*. Ужгород, 2016. Вип. 40(2). С. 106-109.
2. Про організацію планування в секторі безпеки і оборони України Рішення Ради національної безпеки і оборони України від 16 травня 2019 року: Указ Президента України від 16.05.19 р. № 225/2019. URL: <http://www.rnbo.gov.ua/documents/502.html>
3. Науково-практичний коментар Закону України “Про основні засади забезпечення кібербезпеки України”; станом на 1 січня 2019 року / М.В. Гуцалюк та ін.; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.
4. Верголяс О.О. Інформаційно-правове забезпечення спеціальних інформаційних операцій. *Інформація і право*. № 4(27)/2018. С. 126-133.
5. Вітер С.А., Світличин І.І. Захист облікової інформації та кібербезпека підприємства *Науковий вісник Мукачівського державного університету. Серія “Економіка і суспільство”*. 2017. Вип. 11. С. 497-502.
6. Киричок Р.В. Тест на проникнення як імітаційний підхід до аналізу захищеності корпоративних інформаційних систем. *Сучасний захист інформації*. 2018. № 2(34). С. 53-58.

~~~~~ \* \* \* ~~~~~

УДК 37.014:355.233.11

САНДУЛ В.С., вчитель предмету “Захист Вітчизни” середнього загальноосвітнього закладу “Слов’янська гімназія”

## УДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА ТА НАВЧАЛЬНОЇ ПРОГРАМИ ВИКЛАДАННЯ ПРЕДМЕТА “ЗАХИСТ ВІТЧИЗНИ” В СЕРЕДНІХ ЗАГАЛЬНООСВІТНІХ ЗАКЛАДАХ

**Анотація.** Щодо удосконалення законодавства та навчальної програми викладання предмету “Захист Вітчизни” в середніх загальноосвітніх закладах, в умовах воєнного чи надзвичайного стану, гібридної війни та тимчасової окупації Автономної Республіки Крим.

**Ключові слова:** предмет “Захист Вітчизни”, інформаційна війна, гібридна війна.

**Summary.** Regarding the improvement of legislation and the curriculum of studying the subject “Defense of the Motherland” in secondary educational institutions, in conditions of emergency, hybrid warfare and temporary occupation of the Autonomous Republic of Crimea.

**Keywords:** the item “Defense of the Motherland”, information war, hybrid war.

**Аннотация.** Относительно усовершенствования законодательства и учебной программы изучения предмета “Защита Отчизны” в средних общеобразовательных учреждениях, в условиях чрезвычайного положения, гибридной войны и временной оккупации Автономной Республики Крым.

**Ключевые слова:** предмет “Защита Отчизны”, информационная война, гибридная война.

**Постановка проблеми.** Події останніх чотирьох років, що призвели до соціальної нестабільності в Україні, спровокували збройну агресію з боку Росії на Сході України, анексію Криму та подальше розгортання Росією гібридної війни на усіх можливих напрямках, виявили певну недосконалість вітчизняного законодавства та як наслідок, виникла необхідність внесення змін до навчальної програми предмета “Захист Вітчизни” в середніх загальноосвітніх закладах України.

Для врегулювання зазначених відносин необхідно провести відповідні роботи з аналізу й оцінки чинного законодавства України та вжити заходів з його удосконалення в тій частині, що відповідає сучасній політичній, економічній, військово-політичній та міжнародній ситуаціях.

**Метою статті** є удосконалення чинного законодавства України у галузі освіти щодо викладання предмета “Захист Вітчизни” у середніх загальноосвітніх закладах України.

**Виклад основних положень.** Стаття 17 Конституції України [1] встановлює, що захист Вітчизни є обов’язком громадян України та найважливішою функцією держави.

Оборона України, захист її суверенітету, територіальної цілісності і недоторканності покладаються на Збройні Сили України. Водночас Збройні Сили України потребують підготовленого резерву.

Згідно частини третьої статті 1 Закону України “Про військовий обов’язок і військову службу” (далі – Закон) [2], військовий обов’язок включає в тому числі – підготовку громадян до військової служби.

Частиною першої статті 9 Закону встановлено, що допризовна підготовка включається до Державного стандарту повної середньої освіти загальноосвітніх та

професійно-технічних навчальних закладів у разі, якщо певний освітньо-кваліфікаційний рівень здобувається на основі базової середньої освіти та проводиться за програмами, погодженими з Міністерством оборони України.

В сучасній школі, забезпечення виконання завдань допризовної підготовки покладається на програмний курс навчального предмета “Захист Вітчизни”.

Навчальна програма шкільного предмета “Захист Вітчизни” введена наказом Міністерства освіти і науки України від 23.10.17 р. № 1407 [3] включає вісім розділів, деякі з них не повною мірою відповідають вимогам сьогодення.

Дуже ґрунтовне та фахове дослідження щодо адекватної реакції змісту навчальної програми “Захист Вітчизни” на військову агресію проти України, проведено колишнім вчителем предмету Романом Кучеренко в оглядовій статті [4]. Розглянемо деякі із таких.

1. У розділі першому зазначається, що функціонування Збройних Сил України на сучасному етапі спрямовано на формування у молоді ідеалу людини-патріота, захисника Вітчизни на прикладах героїчної боротьби українського народу за незалежність. Проте, на жаль, відсутня акцентація на необхідності надання прикладів героїчної боротьби та навіть самопожертв таких Героїв, які сьогодні захищають незалежність Держави на Сході України.

Р. Кучеренко в своїй статті ставить справедливе питання: “А де сам захист Вітчизни нашими воїнами, тобто хід військового конфлікту? Де захоплення героїзмом та успіхами нашого війська: де аналіз прикрих поразок та приклади героїзму наших воїнів: курган Савур-Могила (липень – серпень 2014 р.), втрата Ізвариного (липень 2014 р.), Амвросіївки та Оленівки (серпень 2015 р.), Іловайський (серпень 2015 р.) та Дебальцівський (січень – лютий 2015 р.) котли? ”

Також автор підкреслює, що “в жодному разі не применшуючи історичних досягнень минувшини, поставимо собі питання: що цікавіше молодій людині – визвольна війна під проводом Богдана Хмельницького 1648 – 1657 років чи війна на сході України (АТО, ООС) 2014 р.? Хто цікавіший – кошовий отаман Петро Конашевич-Сагайдачний чи Герой України Михайло Забродський? А може, цікавіше знати молоді про місцевих героїв, які проживають поруч, вчилися в їхній школі, були поранені або ж не повернулися живими?.” І таку позицію Р. Кучеренка можна вважати дуже справедливою.

Таким чином, вважаємо, є потреба включення до програми предмету “Захист Вітчизни” як обов’язок вчителя – інформування учнів про щоденну обстановку в зоні проведення операції об’єднаних сил.

2. У розділі другому – Статути Збройних Сил України, розглядаються основні положення організації внутрішньої служби, повсякденної життєдіяльності військ. Водночас відсутня складова, щодо життєдіяльності військ в умовах ведення противником гібридної війни.

Р. Кучеренко у темі “Військовослужбовці та відносини між ними” пропонує більше уваги приділяти особливостям військового виховання, іншим елементам взаємовідносин у районі бойових дій, використанню знаків розрізнення та інше. У темі “Військова дисципліна” є необхідність висвітлення питання покарань та заохочень в зоні бойових дій, а також найбільш розповсюджених дисциплінарних та кримінальних правопорушень у війську на сьогодні та їхні наслідки.

3. Основні положення щодо підготовки та ведення сучасного бою механізованим відділенням, прийоми і способи дій солдата в основних видах бою у складі відділення, вивчаються в п’ятому розділі – “Тактична підготовка”. Як стверджує Р. Кучеренко: “Майже не приділяється увага вивченню сучасних засобів та методів зв’язку, а без нього решта втрачає сенс”. Окрім того, слід роз’яснити учням сутність та призначення

таких елементів оборони, управління та забезпечення, як спостережний пост (СП), блокпост, взводний та ротний опорні пункти (ВОП та РОП), командно-спостережний пункт (КСП), тиловий пункт управління (ТПУ), а також їхню взаємодію. Особливу увагу слід приділити наданню знань ефективного спостереження за супротивником. В першу чергу це стосується використання тепловізорів, відстанемірів, сучасних приладів нічного бачення. Також варто не оминати увагою поняття безпілотних літальних апаратів, їх основні види, маскування від них та боротьба з ними, особливості доповіді про їхній проліт. На жаль, зазначеним розділом не передбачене ознайомлення з новими тактичними прийомами, які з'явилися під час ведення так званої “гібридної війни”.

Гібридна війна є новим суспільно-політичним явищем, притаманним сьогоденню. Світовою спільнотою вона визнана як один із видів війни.

Попович К.В. у роботі [5] підкреслює, що гібридна війна – це війна, основним інструментом якої є створення державою-агресором в державі, обраній для агресії, внутрішніх протиріч та конфліктів з подальшим їх використанням для досягнення політичних цілей агресії, які звичайно досягаються звичайною війною.

Майже аналогічним за суттю, але більш об'ємним за формою є визначення терміну “гібридна війна” (англ. hybrid warfare) як воєнної стратегії, яка об'єднує звичайну війну, малу війну і кібер- війну. Термін “гібридна війна” використовують також для опису атак із застосуванням ядерної, біологічної та хімічної зброї, саморобних вибухових пристроїв та інформаційних технологій.

Проблеми застосування інформаційної зброї детально висвітлено в монографічному дослідженні “е-боротьба в інформаційних війнах та інформаційне право” [6], де надано ґрунтовний аналіз видів, змісту, зброї, засобів нападу та захисту інформаційних ресурсів, систематизовано уявлення про інформаційну боротьбу у зв'язку з розвитком електронно-інформаційного середовища та поширенням кіберзлочинності, активним застосуванням деструктивних інформаційних маніпуляцій людиною, громадською думкою і масовою свідомістю, та науково доведено, що найефективнішим способом захисту людини, суспільства та держави щодо захисту знань та інформаційних ресурсів від небажаного інформаційного впливу є необхідність подальшого активного вдосконалення, зокрема, інформаційного законодавства держави. Як зазначається у дослідженні: *“Невід'ємною та обов'язковою у військовій боротьбі (та гібридній війні – від Авт.) є інформаційна складова, яка завжди присутня не тільки у період ведення бойових дій, але й у мирний час. Ця складова пронизує політичну, ідеологічну, економічну і, власне, всю збройну боротьбу. За всіх часів підготовка до війни та її ведення супроводжувались бажанням отримати якомога більше інформації про супротивника та, одночасно, забезпечити захист інформації щодо свого стану, намірів, дій тощо. ...Брехня, обман та дезінформація є головними чинниками маніпуляцій свідомістю людини”*.

Доктор філологічних наук, професор, експерт з інформаційної політики та комунікаційних технологій Г. Почепцов стверджує, що *“сьогоднішня гібридна війна розгорнута на всіх можливих напрямках, це не лише інформаційна війна. Це одночасно економічна, репутаційна, смислова, людська... На неї повинні працювати всі, хто має вплив на населення: актори, співаки, письменники, режисери. Військові дії задають лише фон для більш масштабної війни в людському розумі. Це скоріше гуманітарна війна, в якій військові дії є другорядними. Коли ми в першу чергу звертаємо увагу на них, ми робимо помилку”* [7].

Виходячи з вищезазначеного, як ніколи зростає роль шкільного виховання, щодо нейтралізації впливу засобів гібридної війни на свідомість молодого покоління українців.

Видання “Трибуна” [8], наводить ознаки гібридної війни. Ось деякі із них:

1. Гібридну війну не оголошують. Це дає змогу країні – агресору маніпулювати міжнародною думкою, а країні, на яку здійснюється агресія, неможливо адекватно реагувати на загрозу, бо юридичної підстави нібито нема.

2. Гібридна війна планується під стратегію інформаційної війни, за якою здійснюється побудова такої зомбі-реальності, за якою противника оголошують “нелюдом”, “фашистом”, приреченим на знищення.

3. Метою гібридної війни є не стільки завоювання як таке, скільки створення хаосу, безперервного конфлікту, постійне генерування провокацій, умов, непридатних для життя, руйнування інфраструктури.

4. Використовуються постановочні воєнні дії, виконувані акторами, призначені для зйомок картинок для показу в зомбі-ЗМІ.

5. Суть гібридної війни – знищення національно-державної громадянської ідентичності країни-суперника.

Україна одна з небагатьох держав світу, яка на протязі останніх п’яти років, захищаючи свою територіальну цілісність та недоторканість кордонів, зіткнулась з усіма проявами та реаліями гібридної війни, але до цієї пори не визначила такого виду війни на законодавчому рівні.

В діючих Законах України, що регламентують діяльність Міністерства Оборони України, а саме:

В пункті 1 частини 1 статті 1 Закону України “Про національну безпеку України” [9], визначено, що воєнний конфлікт – форма розв’язання міждержавних або внутрішньодержавних суперечностей із двостороннім застосуванням воєнної сили; основними видами воєнного конфлікту є війна та збройний конфлікт. В той же час не передбачено такого виду війни, як “гібридна війна”.

Статтею 1 Закону України “Про оборону України” [10], визначені такі терміни як: збройна агресія, вторгнення або напад збройних сил іншої держави або групи держав на територію України, а також окупація або анексія частини території України, блокада портів, узбережжя або повітряного простору, порушення комунікацій України збройними силами іншої держави або групи держав, засилання іншою державою або від її імені озброєних груп регулярних або нерегулярних сил, що вчиняють акти застосування збройної сили проти України, застосування підрозділів збройних сил іншої держави або групи держав, які перебувають на території України відповідно до укладених з Україною міжнародних договорів.

Як вважаємо, сукупність усіх вищезазначених термінів можуть складати предмет поняття “гібридна війна” та бути об’єднані єдиним терміном – “гібридна війна”.

Положення абз. 6 статті 1 Закону України “Про Збройні Сили в Україні” [11] декларує: “Ніякі надзвичайні обставини, накази чи розпорядження командирів і начальників не можуть бути підставою для будь-яких незаконних дій по відношенню до цивільного населення, його майна та навколишнього середовища”.

Враховуючи, що дії деяких цивільних осіб, що підтверджується досвідом бойових дій в гібридній війні, підпадають під визначення учасника бойових дій на стороні супротивника, зазначене положення втрачає актуальність та потребує внесення змін, що розширюють права військовослужбовців щодо можливості силового впливу на учасників гібридної війни.

Котенко А. в статті “Гібридна війна як форма сучасного міжнародного конфлікту” [12] стверджує, що на даний час у військовій та політичній науці відсутні загальновизнане визначення “гібридної війни”. Офіційно ухвалювати цей термін не поспішає і Міністерство оборони США, яке наразі обмежується терміном “гібридна загроза”. Деякі дослідники, у тому числі у Росії, також ставлять під сумнів обґрунтованість терміну “гібридна війна”.

Звичайно, Україна повинна поважати позицію міжнародної спільноти, але сучасні виклики вимагають в першу чергу захищати інтереси Держави Україна.

Іде шостий рік гібридної війни. При цьому Міністерством оборони України, як органом центральної влади, що має право законодавчої ініціативи, не здійснюється ніяких дій, щодо удосконалення нормативно-правової бази та приведення такої до вимог сьогодення, особливо в тій частині, яка стосується проявів гібридної війни.

Враховуючи вищезазначене, можна дійти висновку, що деякі положення чинного законодавства України не відповідають сучасним викликам. Виникає необхідність приведення у відповідність реаліям сьогодення норм чинних Законів України а саме:

1. В пункті 1 частини 1 статті 1 Закону України “Про національну безпеку України” надати визначення такому виду війни як “гібридна війна”.

Такому визначенню, як одному із видів війни, по суті відповідає визначення наведене Поповичем К.В., яке після доопрацювання може бути прийняте за основу.

2. Терміни, що визначені в статті 1 Закону України “Про оборону України”, а саме: “збройна агресія, вторгнення або напад збройних сил іншої держави або групи держав на територію України, а також окупація або анексія частини території України, блокада портів, узбережжя або повітряного простору, порушення комунікацій України збройними силами іншої держави або групи держав, засилання іншою державою або від її імені озброєних груп регулярних або нерегулярних сил, що вчиняють акти застосування збройної сили проти України, застосування підрозділів збройних сил іншої держави або групи держав, які перебувають на території України відповідно до укладених з Україною міжнародних договорів”, об’єднати єдиним терміном – “гібридна війна”.

3. Ствердження О. Джолоса [13]: “державна, яка веде гібридну війну, здійснює операцію з недержавними виконавцями-бойовиками, групами місцевого населення, організаціями, зв’язок з якими формально повністю заперечується”, ставить за доцільне внести зміни до абз. 6 статті 1 Закону України “Про Збройні Сили в Україні” в частині, що дозволить військовослужбовцям приймати заходи силового впливу до учасників бойових дій, в тому числі і груп місцевого населення, які діють на стороні супротивника.

### **Висновки.**

Враховуючи вищезазначене, потреби часу та досить складну внутрішньополітичну, міжнародну та військово-політичну ситуацію, зусилля держави мають бути спрямовані на вдосконалення національного законодавства, шляхом внесення змін до:

1) пункту першого частини першої статті 1 Закону України “Про національну безпеку України” стосовно надання визначення терміну “гібридна війна” у такому формулюванні:

***гібридна війна** – це війна, яку розпочинають без оголошення, основним інструментом якої є стратегія інформаційного впливу на населення, для створення державою-агресором в державі, обраній для агресії, внутрішніх протиріч та конфліктів з подальшим їх використанням, з метою знищення національно-державної громадянської ідентичності країни-суперника, оволодінням людськими, матеріальними та інформаційними ресурсами;*

2) статті 1 Закону України “Про оборону України” щодо об’єднання різних видів озброєного насильства для досягнення політичних, економічних та соціальних цілей єдиним терміном – “гібридна війна”, та абзацу шостого статті 1 Закону України “Про Збройні Сили в Україні” в частині, що розширить повноваження військовослужбовців щодо можливості силового впливу на цивільне населення, яке бере участь у війні на стороні противника.

Зазначені пропозиції щодо внесення змін до законодавства, згідно вимог частини першої статті 9 Закону України “Про військовий обов’язок і військову службу”, можуть стати підставою для удосконалення Міністерством освіти і науки України навчальної програми предмета “Захист Вітчизни” в закладах середньої освіти до вимог сьогодення, що буде сприяти створенню умов підвищення рівня викладання предмета “Захист Вітчизни” в середніх загальноосвітніх закладах, підготовки громадян до військової служби та забезпечення безпеки держави Україна, зокрема під час ведення проти неї гібридної війни.

### Використана література

1. Конституція України: Закон України від 28.06.96 р. № 254/96-ВР. URL: [www.rada.gov.ua](http://www.rada.gov.ua).
2. Про військовий обов’язок і військову службу: Закон України від 25.03.92 р. № 2233-ХІІ. *Відомості Верховної Ради України*. 1992. № 27. Ст. 386.
3. Навчальна програма шкільного предмета “Захист Вітчизни”: Наказ МОН України: від 23.10.17 р. № 1407. URL: <https://mon.gov.ua/ua/osvita/zagalna-serednya-osvita/navchalni-programi/navchalni-programi-dlya-10-11-klasiv>
4. Роман Кучеренко. Предмет “Захист Вітчизни”: проблеми змісту. Ч. 2. URL: <http://education-ua.org.ua/articles/1161-predmet-zakhist-vitchizni-problemi-zmistu-chastina-druga>
5. Попович К.В. Гібридна війна як сучасний спосіб ведення війни: історичний та сучасний виміри. *Науковий вісник Ужгородського університету. Серія “Історія”*. Вип. 2 (35). 2016.
6. Брижко В.М. та ін. е-боротьба в інформаційних війнах та інформаційне право: монографія / за ред. М. Швеця, чл.-кореспондента АПрН України; рецензенти: М. Сегай, академік АПрН України, О. Крупчан, чл.-кореспондент АПрН України. Київ: Вид. ТОВ “Пан-Тот”, 2007 р. 236 с.
7. Почепцов Г. Гібридна війна: інформаційна складова. URL: [http://www.ji-magazine.lviv.ua/2015/Pochepcov\\_Gibr\\_vijna\\_inf\\_skladova.htm](http://www.ji-magazine.lviv.ua/2015/Pochepcov_Gibr_vijna_inf_skladova.htm)
8. П’ять ознак “Гібридної війни”. URL: <https://tribuna.pl.ua/news/5-oznak-gibridnoyi-vijni>
9. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.
10. Про оборону України : Закон України від 06.12.91 р. № 1933-ХІІ. *Відомості Верховної Ради України*. 1992. № 9. Ст. 107.
11. Про Збройні Сили в Україні: Закон України від 06.12.91 р. № 1935-ХІІ(1935-12). *Відомості Верховної Ради України*. 1992. № 9. Ст. 109.
12. Котенко А. “Гібридна війна як форма сучасного міжнародного конфлікту”. URL: [https://www.google.com/search?q=%D0%B3%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%B0+%D0%B2%D1%96%D0%B9%D0%BD%D0%B0+%D0%B2%D0%B8%D0%B7%D0%BD%D0%B0%D1%87%D0%B5%D0%BD%D0%BD%D1%8F&rlz=1C1AWFA\\_enUA837UA837&oq=%D0%B3%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%B0+%D0%B2%D1%96%D0%B9%D0%BD%D0%B0%2C&aqs=chrome.5.69i57j0l5.15888j1j8&sourceid=chrome&ie=UTF-8](https://www.google.com/search?q=%D0%B3%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%B0+%D0%B2%D1%96%D0%B9%D0%BD%D0%B0+%D0%B2%D0%B8%D0%B7%D0%BD%D0%B0%D1%87%D0%B5%D0%BD%D0%BD%D1%8F&rlz=1C1AWFA_enUA837UA837&oq=%D0%B3%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%B0+%D0%B2%D1%96%D0%B9%D0%BD%D0%B0%2C&aqs=chrome.5.69i57j0l5.15888j1j8&sourceid=chrome&ie=UTF-8)
13. Олег Джолос. Інформаційна складова гібридної війни. Погляд з Донбасу. URL: <http://novosti.dn.ua/article/4889-informaciyna-skladova-gibrydnoi-viyny-poglyad-z-donbasu>

~~~~~ \* \* \* ~~~~~



**Інформація за іншими предметними напрямками досліджень за спеціалізаціями в галузі знань 08 – “Право”**

УДК 340:374.3

**БЕЛАНЮК М.В.**, кандидат юридичних наук, в.о. ученого секретаря  
НДІ інформатики і права НАПрН України

**ВРОНСЬКА Т.В.**, доктор історичних наук, головний науковий  
співробітник НДІ інформатики і права НАПрН України

**ПЕРШІ КРОКИ ВІДНОВЛЕННЯ РОБОТИ ОРГАНІВ ЮСТИЦІЇ НА  
ВИЗВОЛЕНІЙ ВІД НАЦИСТІВ ТЕРИТОРІЇ УКРАЇНИ (1943 – 1944 рр.)**

**Анотація.** У статті досліджуються перші кроки відновлення роботи органів юстиції після звільнення окупованих територій України у 1943 – 1944 рр. Спираючись на унікальні архівні документи, висвітлюються особливості діяльності цих органів, аналізуються організаційно-функціональні питання, зокрема і вирішення кадрової проблеми в особливих умовах воєнного часу, наближеності лінії фронту та бойових дій на головному театрі Другої світової війни.

**Ключові слова:** війна, окупація, евакуація, реевакуація, юстиція, судочинство, суд, трибунал.

**Summary.** The article examines the first steps of the restoration of the work of the justice bodies after the liberation of the occupied territories of Ukraine in 1943 – 1944. Based on unique archival documents, the peculiarities of the activities of these bodies are analyzed, organizational and functional issues are analyzed, in particular, the solution of personnel problems in special conditions of wartime, proximity front line and fighting at the main theater of the Second World War.

**Keywords:** war, occupation, evacuation, reevacuation, justice, court proceedings, court, tribunal.

**Аннотация.** В статье исследуются первые шаги по восстановлению работы органов юстиции после освобождения оккупированных территорий Украины в 1943 – 1944 гг. Опираясь на уникальные архивные документы, освещаются особенности деятельности этих органов, анализируются организационно-функциональные вопросы, в том числе решение кадровой проблемы в особых условиях военного времени, вблизи линии фронта и боевых действий на главном театре Второй мировой войны.

**Ключевые слова:** война, оккупация, эвакуация, реевакуация, юстиция, судопроизводство, суд, трибунал.

**Постановка проблеми.** Дотепер у більшості праць з історії радянського правосуддя найбільшою тематичною лакуною залишається період Другої світової війни, особливо той її етап, який стосується евакуації, окупації та перших кроків відновлення роботи державних інституцій, зокрема й юстиції на очищеній від нацистів території УРСР. Це пояснюється не відсутністю інтересу з боку істориків чи правників, а, передусім, браком відповідних матеріалів у вітчизняних архівосховищах. Серед авторів, які побіжно торкались проблеми відновлення роботи судових органів на території України у 1943 – 1944 рр. В. Гончаренко, О. Зайчук, О. Копиленко, Д. Сусло, Б. Потильчак [1].

Більшість документів, дотичних до функціонування інститутів радянської Феміди, була знищена під час відступу Червоної армії. Лише незначну частку документів вдалося евакуювати до Москви, де вони й донині зберігаються. Але для українських

вчених ці документи є недоступними і такий стан речей, вірогідно, триватиме ще протягом невизначеного періоду. Виявлені раніше матеріали (у 2010 – 2011 рр.) у Державному архіві Російської Федерації (далі – ДАРФ), передусім ті, що зберігаються у фонді 9492 “Радянська юстиція”, в якому містяться звіти про роботу органів юстиції, доповіді про їх кадрове забезпечення, резолюції нарад тощо; а також відповідний комплекс документів фонду 1 (“Центральний комітет Комуністичної партії України (1918 – 1991)”) Центрального державного архіву громадських об’єднань України (далі – ЦДАГО) дозволяють підняти завісу і реконструювати перші заходи республіканської влади, керівництва правоохоронних й інших органів з відновлення та налагодження функціонування окремих установ радянської системи права. У контексті згаданого процесу особлива увага прикута до специфіки кадрової політики тієї доби, а також об’єктивних й суб’єктивних чинників, що впливали на організаційну та ідеологічну складову ухвалюваних рішень. Все це сприяє глибшому розумінню своєрідності функціонування інституцій радянської юстиції у республіці, тих вад та недоліків, що згодом позначилися не лише на подальшій практичній роботі органів юстиції, а й на долях людей, які потрапляли до лещат їх механізму.

**Метою статті** є виявлення особливостей роботи органів юстиції на очищеній від нацистів території України, зокрема, у 1943 – 1944 рр., що сприятиме врахуванню негативних уроків минулого в ході реформи судової системи та органів юстиції України на шляху до Європейської інтеграції. Досвід “реанімаційних” процесів у сфері юстиції воєнної доби також може бути корисним для врахування при відновленні роботи державних органів, зокрема й правосуддя, після звільнення окупованих та анексованих територій України.

**Виклад основного матеріалу.** Найголовніший орган в системі радянського судочинства, який мав оперативно відновити свої повноваження спочатку у придатній для цього місцевості, а згодом і у столиці України, це Верховний Суд – найвищий судовий орган у системі судів загальної юрисдикції, на який покладено обов’язки щодо здійснення правосуддя та забезпечення застосування законодавства усіма судами загальної юрисдикції.

Цей організаційний процес у загальних рисах, з певними застереженнями можна було б порівняти із становленням судової гілки влади на інкорпорованих територіях Західної України у 1939 – 1941 рр. Там теж все відбувалося прискореними темпами та в умовах браку кадрів. Але таке уявлення є спрощеним, оскільки радянська влада пішла шляхом насадження нових структур, забезпечуючи їх кадрами, рекрутованими зі східних областей України, Росії та інших республік. Володіння українською мовою не було пріоритетним серед вимог до кандидатів на заміщення відповідних посад.

Натомість у досліджуваній період на визволеній від супротивника території бракувало найголовнішого: фахівців і матеріальної бази. Непорушними залишалися лише закони та радянська свідомість, якою мав керуватися суддівський корпус.

Ще до визволення столиці України, де мав дислокуватися головний офіс найвищої судової інституції, 10 червня 1943 р. виконуючим обов’язки голови цієї установи М. Розановим була підготовлена перша доповідь “Про організацію та роботу Верховного суду УРСР”. У ній він інформував наркома юстиції СРСР М. Ричкова про початок роботи найвищого судового органу республіки з 1 квітня 1943 р. у Старобільську на Донбасі [2, с. 31]. Це стало можливим вже після прибуття туди двох членів суду. Ще до реєвакації цих осіб і заступника наркома юстиції УРСР Титаренка, за дорученням ЦК КП(б)У та РНК УРСР М. Розанов, відповідно до своїх повноважень опікувався організацією народних та обласних судів у визволених областях УРСР.

Отже Верховний суд Української РСР станом на 1 квітня 1943 р. складався з трьох осіб: тимчасово виконуючого обов'язки голови Верховного суду М. Розанова і двох членів суду К. Маркіяновича і А. Бобриньової, які о тій порі одночасно із своєю основною роботою змушено (за відсутності інших кадрів) виконували й функції співробітників канцелярії [2, с. 31].

26 квітня 1943 р. наказом Наркома юстиції СРСР № 230-л на посаду голови Верховного Суду УРСР було призначено його довоєнного керівника К. Топчія, який обіймав цю посаду з червня 1938 р., але упродовж перших років війни виконував обов'язки заступника голови військових трибуналів Південно-Західного, Сталінградського, Донського і Центрального фронтів. Але, як видно з аналізу архівних документів, все ж до серпня 1943 р. обов'язки голови Верховного Суду УРСР виконував М.Г. Розанов [3, с. 127].

20 травня 1943 р. до цього невеличкого колективу приєднався й виконувач обов'язки заступника голови Верховного суду з кримінальних справ Д. Сусло, а на початку другого півріччя 1943 р. на посаду управляючого справами була зарахована В. Пономарьова [2, с. 31].

Як вже зазначалося вище, навесні 1943 р. Верховний суд УРСР тимчасово розташовувався у м. Старобільську Ворошиловградської області, але згодом переїхав до м. Калач Воронежської області, потім в с. Кабичівка Марківського району Ворошиловградської області, у липні – до селища міського типу Дворічна Харківської області [2, с. 31]. 23 серпня 1943 р. від німецьких військ було визволено Харків, а наступного дня разом із іншими республіканськими урядовими установами до колишньої столиці УРСР переїхав і Верховний Суд УРСР, розташувавшись у приміщенні на вулиці Юрївській 2. Тоді ж до безпосереднього керівництва судом став прибулий з Москви К. Топчій [3, с. 128]. Згодом, відповідно до рішення ЦК КП(б)У та РНК УРСР від 12 січня 1944 р., Верховний суд УРСР перебрався до Києва і почав свою роботу в будинку (вул. Воровського, 16), де у 1941 році містилося окупаційне управління у справах фольксдойче.

До кінця 1943 р. організаційна структура Верховного Суду УРСР була практично повністю відновлена. До складу вищого судового органу республіки входили: голова К. Топчій, заступник – Д. Сусло, виконувач обов'язки заступника з кримінальних справ В. Стеценко, заступник з цивільних справ М. Розанов та вісім членів: К. Маркіянович, А. Бобриньова, А. Сахаров, Є. Кирилюк, А. Ішутін, Д. Чорпіта, А. Трубецька та К. Шабаліна. Окрім згаданих осіб лави Верховного суду поповнили член Миколаївського облсуду А. Мамчур, народний суддя Рівненської області Г. Чарська. Згадані особи були рекомендовані НКЮ УРСР, але ще не були обрані у встановленому законом порядку [2, с. 31].

За доволі короткий час штат суддівського корпусу та персоналу, що його обслуговував, збільшився. Станом на 1 січня 1944 р. в апараті Верховного суду УРСР працювало 43 особи, у тому числі: оперативних судових працівників – 14, консультантів – 5, завідувач спецчастини – 1, керуючий справами – 1, секретарі колегій – 3, технічний та обслуговуючий персонал – 19. Незабаром, у лютому, його штат зріс до 105 осіб, 33 з яких становили: голова, заступники та члени Верховного суду. У діючій армії залишалось 5 колишніх членів вищого судового органу республіки – Глущенко, Баранов, Лисів, Сірош і Федотьев [2, с. 31]. Вже у липні 1944 р., відповідно до ініційованих К. Топчієм організаційних змін, в апараті Верховного суду УРСР залишилась працювати 41 особа, у тому числі 16 членів суду [4, с. 42]. Звертає на себе увагу та обставина, що служителям республіканської Феміди визнавали такий кількісний склад “достатнім для забезпечення роботи” цієї найвищої судової інституції. Вірогідно,

такі заяви робилися з огляду на воєнний стан та розуміння реальної ситуації, адже відновити повнокровну роботу цієї інституції, як і інших державних установ, у той час було практично неможливо.

Не менш цікавим видається реконструювання “територіального поля” роботи Верховного суду України у перші дні після очищення території республіки від противника, а також процес відновлення функціонування Наркомату юстиції (НКЮ) УРСР.

У червні 1943 р. Верховний суд “обслуговував” територію УРСР, що охоплювала 22 райони Ворошиловградської області, м. Ворошиловграда та 13 районів Харківської області [2, с. 24]. Поступово, зі звільненням нових населених пунктів, масштаби та обсяги цієї роботи неухильно розширялися.

Окрім Верховного суду, інший важливий орган виконавчої влади, який входив до складу уряду УРСР, – Наркомат юстиції також пройшов нелегкий шлях повернення до роботи після окупації.

Відповідно до “Положення про Народний комісаріат юстиції СРСР” від 8 грудня 1936 р. НКЮ мав керувати організацією судової системи, виборами суддів і організаційно-господарським обслуговуванням судів на всій території СРСР, здійснювати ревізію і інструктування судових установ, керувати системою юридичної освіти і вищими юридичними навчальними закладами та науково-дослідними інститутами, вести роботу з кодифікації, юридичного консультування, вести облік судової статистики тощо.

Оскільки територія УРСР під час війни повністю була окупована, весь апарат судових органів та НКЮ був розформований і залишалася лише оперативна група цього наркомату з 3-х осіб. Архів та більшість матеріалів діловодства перед відступом Червоної армії, як і документи Верховного суду, були знищені або частково евакуйовані у східні області РРФСР. Тому на визволеній території Наркомюсту республіки довелося відновлювати практично повністю як кадрову складову, так і матеріально-технічну базу.

Як впливає з доповідної Наркома юстиції УРСР М. Бабченка, адресованої у вересні 1943 р. своєму союзному керівництву, до середини березня 1943 р. робота НКЮ УРСР обмежувалася лише встановленням місцезнаходження колишніх працівників судових органів. Перші доручення, які вони отримували о тій порі, полягали у звичайному впорядкуванні приміщень, де мали функціонувати суддівські установи. Їх зусиллями у стислі терміни вже у середині квітня до роботи стали обласні управління НКЮ УРСР та суди у Ворошиловградській та Харківській областях [4, с. 42].

Питому вагу серед співробітників, зарахованих на роботу до Наркомату юстиції УРСР восени – взимку 1943 р., становили реевакуйовані зі східних районів Радянського Союзу. Незначна кількість кадрів була тимчасово відряджена з інших республік [5, с. 33].

Відновлення роботи Наркомюсту відбувалося у два етапи.

**Перший етап** тривав з лютого до серпня 1943 р., коли була звільнена ще незначна частина Ворошиловградської та Харківської областей. Тоді проводилася робота з обліку кадрів НКЮ, створення з них оперативних груп Управлінь НКЮ та облсудів для областей Лівобережної частини Дніпра. За цей період були організовані оперативні групи Наркомюсту республіки у складі шести осіб, Верховного Суду – з п’яти осіб. З певними труднощами, але розпочали роботи й були укомплектовані кадрами народні суди у визволених районах.

Судова діяльність в цей час була обмеженою за всіма напрямками функціональних обов’язків. Самі працівники наркомату юстиції визнавали, що належної організаційної роботи вони у той час не здійснювали. Не було налагоджено ні якісного обліку кадрів,

ані діловодства. Останнє через обставини об'єктивного та суб'єктивного характеру перебувало у хаотичному стані.

Упродовж травня – червня 1943 р. наркоматом юстиції Української РСР здійснювалися ревізії обласних та народних судів, за наслідками яких суддівський корпус продовжили орієнтувати на “неослабно суворих заходах покарання, особливо стосовно розкрадачів соціалістичної власності та спекулянтів” [4, с. 43].

*Другий етап* веде свій відлік з кінця серпня 1943 р., коли Червона армія звільнила низку областей та міст України і республіканський уряд, у тому числі і Наркомат юстиції, переїхали до Харкова. Перед Наркомюстом в цей час постало конкретне завдання – створення судового апарату у визволених населених пунктах. Таким чином, початком фактичної діяльності Наркомату юстиції України і всієї судової системи слід вважати другу половину серпня 1943 р. Організаційна робота в цей час розгорталася дуже повільно.

Станом на 20 листопада 1943 р. в УРСР були повністю очищені від нацистів Ворошиловградська, Сталінська, Харківська, Полтавська, Сумська, Дніпропетровська, Чернігівська, Київська і частково Запорізька область. І на цей час штат Наркомату юстиції УРСР вже налічував 24 керівних та оперативних працівників [2, с. 31]. Цієї кількості для того часу, як виявилось, цілком вистачало, оскільки обсяг роботи був незначним. Останнє пояснювалося тим, що більшість місцевостей знаходилася у прифронтовій смузі, а воєнний стан передбачав прерогативу військових трибуналів щодо більшості справ, які виникали на тій території.

Станом на 1 липня 1944 р. кількість працюючих в апараті НКЮ УРСР становила 60 осіб при потребі (за штатним розписом) 81 особа [4, с. 42].

Слід зауважити, що у населених пунктах, де відновлювалася робота суддівського корпусу, організовувалися відповідні наради, на яких розглядалися найактуальніші питання. Вони відбувалися за безпосередньої участі працівників обласних управлінь юстиції, виконуючого обов'язки прокурора республіки Р. Руденка та виконуючого обов'язки голови Верховного суду М. Розанова. За рішенням цих зібрань для секретарів судів та судових виконавців було організовано та проведено низку триденних семінарів [4, с. 43].

Як вже наголошувалося, звітна документація Верховного суду та Наркомату юстиції є цінним джерелом реконструювання всього широкого спектру організаційно-функціональних питань: від, власне, поточної роботи до найбанальніших складових побутового облаштування, які виявилися не менш важливими у постокупаційних умовах.

Так, реальний стан організаційної та практичної діяльності з відновлення роботи органів юстиції на очищеній від ворога території республіки можна встановити з доповідної до Наркомату юстиції, підписаної тимчасово виконуючим обов'язки голови Верховного суду УРСР М. Розановим за 1 – е півріччя 1943 р. Як вже зазначалося, до 1 квітня 1943 р. Верховний суд УРСР займався лише організаційними питаннями. Тому цей рапорт віддзеркалював перебіг подій не за перше півріччя, а лише за другий квартал першого півріччя 1943 р.

Вищий судовий орган України, з огляду на реальний стан речей, доволі бадьоро доповідав, що мав всі більш-менш прийнятні умови для нормальної роботи (приміщення, світло, побутові умови для співробітників). Але вже далі у документі викладалися цілком реальні труднощі, пов'язані з браком найнеобхідніших для функціонування речей. Наголошувалося, що в умовах збільшення навантаження гостро відчувалася нестача паперу та іншого канцелярського обладнання. До речі, така ситуація

була в усіх інших установах. Навіть продуктові картки о тій порі друкували на зворотному боці німецьких листівок.

Одна друкарська машинка, що була у розпорядженні технічного персоналу, аж ніяк не могла задовольнити потреб суду, що своєю чергою позначалося на якості роботи. Часто-густо затримувався розгляд скарг й іншої “поточної чи профільної” роботи. У зв’язку з цим Верховний суд вимушено звертався до Наркомату юстиції республіки з проханням отримання друкарських машинок з інших республік “в порядку надання братерської допомоги” [2, с. 50].

До 1 червня 1943 р. Верховний суд встиг розглянути у наглядовому порядку 5 кримінальних і 43 цивільних справи, а також 67 скарг. Окрім цієї роботи відповідав на запити з місць позбавлення волі та з інших установ [2, с. 2].

Тривала війна і це не могло не позначитися на роботі Верховного суду УРСР. З великим запізненням потрапляли, а іноді й не доходили зовсім, директивні вказівки та постанови Пленуму Верховного суду СРСР, що значно ускладнювало роботу органів правосуддя. Для покращення якості практичної повсякденної роботи Верховний суд УРСР зажадав від НКЮ СРСР роз’яснень з конкретних питань, серед яких превалювали ті, що стосувалися кваліфікації справ, пов’язаних зі спекуляцією, крадіжками, вирішення суперечок навколо повернення житлової площі та вилученого майна тощо.

Щодо народних судів, то станом на 1 грудня 1943 р. на території України їх налічувалося 200 одиниць, на 1 липня 1944 р. їх кількість зросла більше ніж утричі і становила 700 одиниць [4, с. 42].

Слід зазначити, що вже у ті перші дні у визволених районах республіки почали готувати резерв кадрів для наступного направлення у західні регіони. Вже незабаром – у 1944 році з Сумської області туди було відряджено 15 прокурорсько-слідчих працівників [6]. Цей кадровий потенціал входив до складу оперативних груп, які формувалися у прифронтовій смузі перед входженням частин Червоної армії до кожного населеного пункту.

У першому півріччі 1944 р. комплектування органів юстиції та судів УРСР, як і раніше, відбувалося за рахунок відкликання колишніх працівників цієї системи з тилкових районів СРСР. На цей час до роботи стало 655 осіб, які перед війною та у її перші дні працювали на різних посадах у цьому відомстві. Тоді ж до штату органів юстиції було включено: 88 демобілізованих з лав Червоної армії і 33 колишніх партизани, 24 особи – з радянсько-партійного активу і з НКЮ СРСР – 97 осіб. Окрім цих кадрів, які вже мали певний досвід роботи, приходило поповнення щойно отримавши профільну освіту: з юридичної школи НКЮ СРСР – 97 осіб, випускників юрінститутів – 11, юкурсів – 164 особи [7, с. 43].

Окрім згаданих осіб, до роботи в республіканських органах юстиції залучили й 152 особи, які перебували на окупованій території. Слід зазначити, що зарахування таких кадрів відбувалося лише у винятковому порядку, позаяк тавро “життя під німцями” дуже важко було змити і воно надовго закарбувалося у відповідних графах анкет радянських людей. Лояльне ставлення стосувалося лише тих, які, залишаючись у тилу ворога, вели активну боротьбу з нацистами – у партизанських загонах чи підпіллі.

Хоча колишні партизани й не викликали особливих нарікань та застережень, втім серед них траплялися люди, які за своїм психічним станом навряд чи могли прислужитися радянській Феміді у справі правосуддя. Деякі вдавалися до свавілля й позасудових розправ з особами, запідозреними у співпраці з окупантами. Так, начальник Управління НКЮ по Чернігівській області, який під час війни перебував у партизанських лавах, у листопаді 1943 р. в с. Табаєвці Чернігівського району брав

участь у затриманні та допиті старости цього села. Не упоравшись з емоціями, він застрелив підозрюваного у той час, коли його допитував уповноважений відділу контррозвідки. Такі випадки були непоодинокими. Про них інформував секретаря ЦК КП(б)У М. Хрущова виконуючий обов'язки прокурора СРСР Р.Руденко [8, с. 5].

Проблема “засміченості” органів юстиції УРСР тими, хто перебував на окупованій території, була серед головних у довідці, складеній НКЮ СРСР за результатами перевірки роботи судів та НКЮ УРСР у вересні 1944 р. Зокрема, зазначалося, що до штату керівних, оперативних і технічних кадрів зараховано 22 особи, які залишалися на окупованій території УРСР. Ще більше таких “непевних” осіб було серед нотаріусів. З 138 осіб, зарахованих на роботу у визволених районах, 82 становили ті, хто за тих чи інших обставин не встигли евакуюватися в тил. І перше місце у цьому небезпечному реєстрі посідали адвокати. Перевіркою було встановлено, що у 14 визволених областях республіки восени 1944 р. працювало 437 адвокатів, з яких 244 залишалися на окупованій території. Зокрема по Київській області з 99 таких спеціалістів 39 продовжували жити в столиці при німцях. Деякі з них працювали “правовими співробітниками при районних, міських управах, чи адвокатами “Бюро обслуговування населення”, – констатували “контролери” з Москви [7; 45].

Незважаючи на суворі застереження, трьох осіб з “темним минулим” перебування на окупованій території все ж взяли на роботу: двох – ревізорами до Харківського Управління НКЮ та одного у якості консультанта – до Верховного Суду УРСР. Всі згадані новопризначені спеціалісти працювали за німців реєстраторами на міській біржі праці. Керівництво наркомату юстиції СРСР рекомендувало звільнити цих та інших “заплямованих” осіб з роботи [5, с. 33].

Підбираючи кадри для роботи у судах визволених районів УРСР, відповідний наголос робився і на їх національній належності. Перевага віддавалася українцям та росіянам. В одній з доповідних на ім'я наркома юстиції СРСР М. Ричкова, датованої вереснем 1943 р., серед іншого зазначалося: *“Питання національного підбору кадрів нами не випускається з повсякденної практичної роботи. Так, наприклад: у Ворошиловградській області з працюючих 28-ми народних суддів – 16 осіб українці і 12 – росіяни, до того ж ці 12 товаришів – уродженці України, знають місцеві особливості та українську мову”* (тут і далі курсив наш. – Авт.) [4, с. 4]. Це співвідношення станом на травень 1944 р. виглядало наступним чином: з 744 працюючих у народних судах у визволених областях республіки 364 – українці, 198 – росіяни, решта належали до інших національностей [4, с. 44].

Проаналізувавши проблему кадрового забезпечення органів юстиції Української РСР, союзний наркомат розкритикував тамтешнє керівництво не лише за прорахунки при зарахуванні на роботу сумнівних осіб, а й охарактеризував зусилля з укомплектування штатів як “безініціативні” та “споживацькі”. Така неприємна для керівників республіканської юстиції кваліфікація її роботи пояснювалася, передусім, відсутністю перспективних планів кадрової роботи, а також тим, що очільники Наркомюсту УРСР переклали всі турботи з укомплектування кадрів на союзне начальство. Зрештою, останнє й визначило найближчі перспективи, вказавши, що, враховуючи вже заповнені вакансії, належить найближчим часом, після повного визволення УРСР від нацистів, підготувати та взяти на роботу 1500 – 1600 осіб, без урахування адвокатів.

Управління кадрів Наркомату юстиції СРСР, гостро критикуючи своїх українських колег, вишукували можливості й резерви для вирішення проблеми браку кадрів в республіці, зокрема, і шляхом відкликання колишніх працівників судів України, які о тій

порі перебували в інших районах Радянського Союзу (100 осіб), надання допомоги кадрами юстиції з союзних республік (200 осіб), за рахунок випуску юридичних інститутів, відповідно профільних шкіл і короткотермінових курсів у травні – червні 1944 р. (960 осіб).

На пришвидшену підготовку кадрів для українських судів були зорієнтовані відповідні курси у Саратові, Уфі, Казані. У Харкові такі курси розпочали свою роботу з 10 грудня 1943 р. [5, с. 34].

Паралельно кадрову проблему намагалися вирішити й на республіканському рівні. Рішенням Ради Народних Комісарів (РНК) України від 4 листопада 1943 р. відновив діяльність Харківський юридичний інститут, в якому восени 1944 р. навчалося 215 осіб, але лише 17 з них – на випускному курсі. На юридичному факультеті Київського державного університету, евакуйованого до Кзил-Орди, після повернення до столиці УРСР у 1944 р. навчалося 30 осіб, а на випускному курсі лише 5 осіб [4, с. 46].

У грудні 1943 р. у Харкові відкрилися 3-місячні курси з підготовки судово-прокурорських працівників, де відповідну профільну освіту отримували майже 100 осіб. Тривало налагодження навчального процесу в одному з найстаріших державних судово-експертних закладів України та СРСР – Інституті судово-медичної експертизи ім. М. Бокаріуса. Слід відзначити, що підготовка до відкриття цих навчальних закладів розгорталася надто повільно. Асигновані урядом 100 тис. крб. не освоювалися належним чином [5, с. 33].

Незважаючи на намагання вирішити кадрове питання як з резерву, так і за допомогою підготовки молодих фахівців у галузі права, забезпечити органи юстиції та суду належною кількістю кадрів не вдалося.

Вже у липні 1944 р. нарком юстиції УРСР М. Бабченко інформував своє союзне керівництво про те, що комплектування штату республіканських органів юстиції тимчасово припинено, оскільки вичерпався резерв. На цей час згадані підрозділи радянської Феміди відновили свою роботу у 20 визволених областях УРСР. В інших чотирьох ці функції виконували оперативні групи: у Дрогобицькій – 8 осіб, Ізмаїльській – 14, Львівській – 21 і Станіславській – 16 осіб [7, с. 42].

Незадовільне вирішення кадрового питання призвело до того, що в 90 самостійних адміністративних районах влітку 1944 р. не вдалося організувати народних судів.

Натомість комплектування обласних судів було завершено раніше ніж народних. Їх кадровий склад комплектувався досвідченими працівниками, відкликаними з тилкових районів. Щоправда, їх практична діяльність навесні та влітку 1943 р. залишалася досить обмеженою за обсягом. Вони розглядали окремі справи, підсудні військовим трибуналам, зокрема за ст.ст. 56 – 20 Кримінального кодексу (далі – КК) УРСР про ухилення від оборонних робіт і 54 – 14 “контрреволюційний саботаж” наказів командування щодо здачі зброї та трофейного майна [4, с. 43]. Скласти вичерпне уявлення щодо різних категорій справ, розглянутих у 1943 – на початку 1944 рр. не видається можливим, оскільки судова практика тоді не узагальнювалася належним чином.

Більш-менш упорядкованою виглядала звітність Верховного суду УРСР, який вже восени – взимку 1943 р. розпочав розгляд скарг в наглядовому порядку. О тій порі не видавалося можливим робити будь-які серйозні виважені узагальнення щодо кримінальних справ, котрі проходили через Верховний суд республіки, оскільки вони, як зазначалося у доповідній, надісланій на ім'я наркома юстиції СРСР, “були різноплановими” і супроводжувалися порушенням підсудності та кваліфікації [2, с. 2]. Втім, останній закид адресувався не Верховному суду, а народним судам республіки,



які, порушуючи встановлений порядок приймали до розгляду справи поза своєю компетенцією. Це стосувалося в першу чергу справ про самовільне залишення роботи у вугільній промисловості, які народні суди кваліфікували за Указом Президії Верховної Ради СРСР від 26 червня 1940 р. У той час на згадану галузь народного господарства розповсюджувався Указ Президії Верховної Ради СРСР від 16 грудня 1941 р. [2, с. 3], який передбачав суворіші санкції. Якщо за Указом від 26 червня 1940 р. самовільне залишення роботи каралося тюремним ув'язненням від 2 до 4 місяців, то вже відповідно до Указу від 26 грудня 1941 р. ці ж дії кваліфікувалися як дезертирство і строк позбавлення волі зростав від 5 до 8 років [9, с. 118]. Так, до провадження народним судом Свердловського району Ворошиловградської області була прийнята справа громадянина Соколова, який самовільно залишив роботу на вугільній шахті. Його вчинок кваліфікували за Указом від 26 червня 1940 р. Верховний суд УРСР опротестував такий присуд у зв'язку з порушенням підсудності та неправильної кваліфікації [2, с. 3]. Слід зазначити, що зазначена категорія справ у роки війни була віднесена до компетенції військових трибуналів. Втім, вже наприкінці 1943 – на початку 1944 рр. такого роду правопорушення паралельно розглядалися і в народних судах. Що далі відсувалася прифронтна смуга, то більше ставало навантаження судів загальної юрисдикції.

У 1944 – 1945 рр. традиційним напрямком роботи Верховного Суду УРСР був контроль місцевих судів загальної юрисдикції. Найвищий судовий орган намагався виправити помилки, яких припустилися у своїй повсякденній роботі народні суди: опротестовувалися вироки, уточнювалася кваліфікація “злочинів”, визначення міри покарання тощо.

Про інтенсивність організаційно-контрольної та ревізійної роботи вищого органу в системі судів загальної юрисдикції Української РСР свідчить аналіз періодичності та географії відряджень суддів у 1944 р. Зокрема, перевірки здійснювалися: у Дніпропетровську з 12 по 24 лютого, Кам'янці – Подільському з 21 серпня по 26 вересня; у Полтаві з 29 квітня по 6 травня та з 6 по 12 вересня; в Сталіно з 1 по 18 грудня; у Києві та Полтаві з 14 квітня по 17 травня і з 21 липня по 15 серпня; у Чернігові – у лютому; в Сумах – у травні; в Херсоні – у серпні; в Житомирі – у грудні; у Харкові і Сталіно – чотири рази протягом року. Також заступник голови Верховного Суду УРСР Д. С. Сусліс з листопада 1944 р. по вересень 1945 р. працював у Закарпатті, де займався організацією місцевих органів юстиції [3, с. 134-135].

Верховний Суд УРСР й сам неодноразово ставав об'єктом інспекторських ревізій НКЮ СРСР у 1943 – 1944 рр. За результатами однієї з таких перевірок колегія союзного наркомату юстиції звернула увагу на те, що *“судді не мають належної кваліфікації та підготовки, виїжджають на ревізії без серйозної попередньої підготовки, обмежуються констатацією недоліків, не приймаючи на місці необхідних заходів щодо їх усунення. Та й недоліки розкриваються поверхово, без необхідного глибокого аналізу їх причин”*. Продовжуючи свій критичний вердикт, “ревізори”, здебільшого слушно, зазначали: *“Як наслідок це впливає зокрема й на низьку якість оформлення судових ухвал у багатьох справах касаційного та наглядового провадження, відсутність контролю за виконанням рішень суду на місцях, а також фактичне ігнорування роботи з узагальнення судової практики. Такий стан пояснюється, зокрема, недостатнім контролем органів юстиції з порушеннями законів у судах. Сам Ричков, вважає неправильними такі оцінки, як масові порушення законів суддями. Під час бесіди у листопаді ц.р. в ЦК ВКП (б) він заявив, що немає підстав говорити про масовий характер порушень суддями законів оскільки до загальної кількості справ, що розглядаються суддями, скасування вироків за*

кримінальними справами складають незначний відсоток. Однак Ричков забуває, що [за] незначним відсотком скасованих вироків у кримінальних справах в дійсності [безвинно] страждають сотні тисяч незаконно засуджених громадян, з яких десятки тисяч перебувають у в'язницях" [10, с. 32].

Народними судами України лише за I кварталі 1944 р. було розглянуто 17629 справ. Більшість з них (9764) були пов'язані з порушенням трудової дисципліни в надзвичайних умовах воєнного часу. Пояснюючи таке співвідношення, керівництво НКЮ УРСР наголошувало: *"Процес відновлення промисловості та велика потреба робочої сили диктує необхідність проведення мобілізації працездатного міського населення на період воєнного часу для роботи на виробництві та будівництві і тому боротьба з особами, які ухиляються від мобілізації набуває в Україні особливого значення"* [4, с. 46].

З огляду на судову практику військових трибуналів військ НКВС Українського округу за квітень – вересень 1944 р. впливає, що справи про порушення трудової дисципліни та інші, регламентовані Указом Президії Верховної Ради СРСР від 26 грудня 1941 р., слухалися у військових трибуналах Кам'янець-Подільської, Одеської, Чернівецької та інших щойно визволених областей. Але їх кількість була незрівнянно меншою, ніж у народних судах решти областей [11, с. 29].

В умовах карткової системи, гострого дефіциту продовольчих та промислових товарів суди надзвичайно принципово ставились і до т.зв. "порушень правил радянської торгівлі", спекуляції, розбазарювання державного майна, крадіжок. За крадіжки у першому кварталі 1944 р. було засуджено 1786 осіб, за привласнення майна з використанням посадового становища – 84 особи [4, с. 48].

Серед справ про крадіжки переважали справи про привласнення майна евакуйованих. Так, в останні дні перебування окупантів у Києві, коли внаслідок оголошення відповідних частин міста забороненими зонами, без догляду опинилося чимало квартир. Цим скористалися нечисті на руку особи. Вони грабували помешкання киян, коли ті не встигли повернутися додому.

Реагуючи на такого роду злочинні дії, органи юстиції звернули увагу суддів на необхідність їх правильної кваліфікації, рекомендувавши розцінювати їх не як звичайні крадіжки, а за аналогією – як мародерство та бандитизм, вчинені за обтяжливих обставин, застосовуючи ст. 59-8 Кримінального кодексу (КК) РРФСР та аналогічні статті республіканських КК [4, с. 48].

На тлі загального прагнення до встановлення справедливості та суворого застосування закону до дійсних злочинців, непоодинокими були вирoki невинувато жорстокі. Людей, які через матеріальну скруту продавали на базарах свої власні носильні речі або продукти, отримані за картками, карали позбавленням волі. Так, 23 серпня 1943 р. мешканка Вовчанського району Харківської області за вирок народногo суду отримала 5 років позбавлення волі лише за те, що продала два стакани солі й три шматки мила, накопичені спільно з рідним братом упродовж тривалого часу. У жовтні того ж року згаданий суд виніс ухвалу покарати трирічним позбавленням волі й 72-річного чоловіка за продаж поношених речей та продуктів, отриманих у межах нормованого постачання. Стара людина на суді у розпачі пояснювала, що на такий крок пішла змушено, через скруту й прагнення надати допомогу рідній дочці. Та суддя залишився невблаганним [5, с. 35].

Ці та решта непоодиноких випадків несправедливого застосування суворих санкцій були спричинені не лише якимись суб'єктивними обставинами. Саме керівництво союзних та республіканських органів правосуддя змушено визнавало те, що судді

“погано знали закони”. До того ж служителі Феміди у переважній більшості не мали жодного примірника кримінального, кримінально-процесуального й цивільного кодексів, а також не знали змісту багатьох постанов Пленуму Верховного суду СРСР, вкрай необхідних при вирішенні складних колізій. Тим часом у судовій практиці виникало чимало важких для розв’язання питань, на які не знаходили відповіді навіть у найвищих судових інстанціях України.

Лише у червні 1944 р. більшість народних судів на визволеній території були забезпечені кримінальними кодексами [4, с. 52], а до цього керувалися власним сумлінням.

Ця судова практика – лише незначна частка тогочасної правозастосовної практики. Але й вона свідчить не лише про характер тогочасної Феміди та про якість роботи суддівського корпусу, а й про наслідки швидкого і тому не завжди якісного добору кадрів на посади. На них часто-густо потрапляли люди, для яких доля інших не мала щонайменшого значення.

Найвищі органи судової влади були віддзеркаленням існуючого режиму.

### **Висновки.**

1. Відновлення роботи органів юстиції та суду на звільнених територіях України відбувалося у два етапи:

- лютий – серпень 1943 р. пошук та обладнання приміщень і підбір кадрів;
- кінець серпня 1943 р. до кінця 1944 р. – створення судового апарату та організація роботи у визволених територіях України.

2. Комплектування органів юстиції та суду УРСР відбувалося за рахунок: відкликання колишніх працівників з тилових районів СРСР, підготовки кадрів в навчальних закладах, і, як виняток, за рахунок осіб, які перебували на окупованій території. Склад прокурорсько-слідчих працівників для роботи у західних областях України формувався у східних областях. Через незадовільне укомплектування штатів до кінця 1944 р. у 90 самостійних адміністративних районах не було створено народних судів.

3. Серед справ, які розглядали судові органи на звільнених територіях України – порушення трудової дисципліни, правил торгівлі; спекуляція; розбазарювання державного майна; крадіжки; посадові злочини; мародерство, бандитизм та інші. Під час дії воєнного стану в порушення встановленого порядку, народні суди приймали до розгляду справи, які мали розглядати військові трибунали.

4. Директивні вказівки Наркомату юстиції та постанови Пленуму Верховного суду СРСР потрапляли до судових органів з великим запізненням, а іноді й не доходили зовсім, що значно ускладнювало роботу та призводило до неправильної кваліфікації злочинів. Не сприяло якості роботи суддів залучення до роботи працівників з низькою кваліфікацією через нестачу кадрів.

5. Дослідження особливостей відновлення роботи органів юстиції на визволеній від нацистів території України у 1943 – 1944 рр. показало, що кадрова політика, як і правозастосовна практика, були віддзеркаленням існуючого режиму.

### **Використана література**

1. Сусло Д.С. Історія суду Радянської України (1917 – 1967 рр.): монографія. Київ: Вид-во Київського університету, 1968. 236 с.; Копиленко О.Л., Гончаренко В.Д., Зайчук О.В., Становлення і розвиток Верховного Суду України. *Вісник Верховного Суду України*. 2003. № 1. С. 2-11.; Потильчак Б.О. Кадрове забезпечення діяльності Верховного Суду Української РСР у 1943 – 1945 рр. *Ученые записки Таврического национального университета имени В.И. Вернадского. Серия “Юридические науки”*. Симферополь: ТНУ им. В.И. Вернадского, 2013. Т. 26 (65). № 2-1 (Ч. 1). С. 106-115.

2. Державний архів Російської Федерації. Ф. 9492. Оп.1. Спр. 298. Арк. 31.
3. Потильчак Б.О. Верховний суд УРСР у 1944 – 1945 рр.: організаційна діяльність і структурна розбудова. *Науковий часопис НПУ імені М.П. Драгоманова. Серія “Економіка і право”*. 2014. Вип. 25. С. 127-137.
4. ДАРФ. Ф. 9492. Оп.1. Спр. 479.
5. ДАРФ. Ф. 9492. Оп.1. Спр. 452.
6. Історія прокуратури Сумської області. URL: [//www.prokuratura.sumy.ua/Inf/4.html](http://www.prokuratura.sumy.ua/Inf/4.html)
7. ДАРФ. Ф. 9492. Оп.1. Спр. 497.
8. Центральний архів громадських об’єднань України. Ф.1. Оп. 23. Спр. 918.
9. Ветров І. Репресивні методи забезпечення робочою силою вугільної промисловості УРСР (1943 – 1945 рр.). URL: <http://enpuir.npu.edu.ua/bitstream/123456789/11396/1/Vetrov.pdf>
10. Постановление Наркомюста и отчет о работе Верховного суда УССР (17 июля 1944 г. – 19 июля 1944 г.). Центральний державний архів громадських об’єднань України. Ф. 1. Оп. 23. Спр. 1371.
11. Центральний державний архів громадських об’єднань України. Ф. 1. Оп. 23. Спр. 1364.

~~~~~ \* \* \* ~~~~~

УДК 351.751

НИЖНИК А.І., аспірант НДІП НАПрН України

## НЕДОТОРКАННІСТЬ НАРОДНОГО ДЕПУТАТА УКРАЇНИ – КОНСТИТУЦІЙНО-ПРАВОВА ГАРАНТІЯ НЕЗАЛЕЖНОГО ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ: ІНФОРМАЦІЙНО-ПРАВОВИЙ АСПЕКТ

**Анотація.** У статті, яка присвячена дослідженню відповідних аспектів інституту депутатської недоторканності, проводиться ідея, що він є конституційно-правовою гарантією незалежного парламентського контролю. У зв'язку з цим на основі існуючих наукових досліджень та відповідних стандартів Ради Європи робиться висновок про доцільність удосконалення обсягу та змісту депутатського імунітету, а не його скасування.

**Ключові слова:** депутатська недоторканність, свобода висловлювань, парламентський контроль.

**Summary.** In this article, which is devoted to the research of the issues of aspects of members' immunity institute, the idea that parliamentary immunity is a constitutional and legal guarantee of independent parliamentary control is proved. In this regard, in the article on the basis of different scientific researches is concluded that it is reasonable not to cancel parliamentary immunity but to limit its scope.

**Keywords:** parliamentary immunity, freedom of speech, parliamentary control.

**Аннотация.** В статье, которая посвящена исследованию соответствующих аспектов института депутатской неприкосновенности, проводится идея, что он является конституционно-правовой гарантией независимого парламентского контроля. В связи с этим на основе существующих научных исследований делается вывод о целесообразности усовершенствования объема и содержания депутатского иммунитета, а не его отмены.

**Ключевые слова:** депутатская неприкосновенность, свобода высказываний, парламентский контроль.

**Постановка проблеми.** Упродовж останніх 20-ти років вітчизняний політикум, як правило напередодні виборчої кампанії, нав'язує українському суспільству думку про необхідність скасування депутатського імунітету. При цьому лунають різні аргументи на користь такої ідеї, в тому числі, що саме це політичне рішення дозволить притягати народного обранця до кримінальної відповідальності на загальних засадах, незалежно від його фракційної належності та перебування у парламентській більшості (коаліції) чи парламентській меншості (опозиції). Дещо штучна абсолютизація самої ідеї позбутися депутатського імунітету робить другорядними важливі проблеми формування в Україні сучасної політичної системи, виборчого процесу, політичної культури, незалежних правоохоронних органів, судової влади тощо.

Періодичні ж опитування громадськості за існуючого низького рівня довіри до владних інституцій свідчать про наявність суспільного запиту щодо доцільності скасування депутатської недоторканності (очевидно, імунітету?). Так, згідно з проведенням з 9 по 14 квітня 2019 року Київським міжнародним інститутом соціології всеукраїнським опитуванням громадської думки 35,5 % респондентів хотіли б, щоб наступний Президент у свої перші 100 днів подав до парламенту законопроекти про зняття едоторканності з депутатів, суддів, Президента України [1]. Отже, наразі маємо

достатньо високий рівень очікувань громадянського суспільства з приводу скасування статусної недоторканності зазначених категорій посадових осіб.

Для подібної емоційної реакції у суспільстві, очевидно, є відповідні підстави, оскільки існуючий на сьогодні обсяг імунітету народних обранців викликає нарікання громадськості та критику з боку науковців і експертного середовища. Зокрема, в експертному середовищі висловлюються застереження щодо скасування парламентського імунітету, а науковці схиляються до доцільності його обмеження.

**Результати аналізу наукових публікацій.** Питанням щодо правового статусу народного депутата України та гарантій його діяльності присвятили свої праці такі вчені, як: Бисага Ю.М., Колодій А.М., Погорілко В.Ф., Георгіца А.З., Сіренко В.Ф., Шемшученко Ю.С., Шаповал В.М. та інші.

Проблематиці гарантій депутатської недоторканності приділяли увагу Ю. Барабаш, О. Задорожній, М. Козюбра, С. Конончук, М. Погорецький, Ю.Тодика, В. Федоренко, О. Ярош та інші.

Натепер серед вітчизняних науковців існує два різних бачення щодо подальшої долі депутатського імунітету. Дехто схиляється до повного скасування депутатського імунітету, а переважна частина вчених – до його суттєвого обмеження.

Разом з тим, аналізуючи сучасну правову дійсність та політико-правові процеси в нашій державі, М.В. Костицький констатував відсутність чіткого розуміння на рівні громадської свідомості змісту та меж депутатської недоторканності [2]. Видається, що таке оціночне судження може бути гіпотетично прийнятним і стосовно громадсько-політичних діячів, які заради своєї популярності ігнорують існуючі наукові здобутки, а також застереження експертів і політологів щодо цього питання, сприяючи тим самим формуванню дещо хибного уявлення щодо соціально-політичного призначення інституту депутатської недоторканності.

Традиційно тема депутатських привілеїв актуалізується в Україні напередодні президентської чи парламентської виборчих кампаній і пропагується у вітчизняному публічному дискурсі під різним кутом зору. При цьому прихильники протилежних точок зору (повного скасування депутатського імунітету чи його суттєвого обмеження) знаходять ті чи інші аргументи на підтримку своєї позиції.

Так, у преамбулі угоди про коаліцію депутатських фракцій “Європейська Україна” зазначено: “Ми забезпечимо рівність усіх посадових осіб держави перед законом, обмежимо всі види імунітетів від кримінального переслідування ..., ми скасуємо депутатську недоторканність та будемо нести повну відповідальність за свої дії перед Українським народом” [3].

Тему скасування депутатського імунітету вкотре як передвиборче гасло використали кандидати в Президенти України у 2019 році. Принаймні у виборчих програмах кандидатів у Президенти України В. Зеленського<sup>2</sup> та Ю. Тимошенко<sup>3</sup> ця тема також проходить червоною стрічкою як відповідна публічна обіцянка.

Отже, вкотре сформовано консолідований суспільно-політичний запит щодо скасування депутатського імунітету в нинішніх реаліях.

Як не дивно, але все це є свідченням того, що питання гарантії незалежності депутатської діяльності й досі не втратило своєї суспільної, законодавчої та наукової актуальності.

<sup>2</sup> URL: <https://www.cvk.gov.ua/pls/vp2019/wp005pt021f01=233pt001f01=720.html>

<sup>3</sup> URL: <https://www.cvk.gov.ua/pls/vp2019/wp005pt021f01=225pt001f01=720.html>

**Мета статті.** Зважаючи на те, що наразі у науковому середовищі та в юридичних колах не обговорюється питання можливих негативних наслідків у разі скасування депутатського імунітету, у цій статті пропонується розглянути депутатську недоторканність не лише як невід’ємний сучасний атрибут конституційно-правового статусу парламентарія, а й з точки зору її суспільно-політичного призначення щодо забезпечення незалежного й ефективного парламентського контролю. Під таким кутом зору це питання дотепер ретельно не досліджувалося. Політична чи інша мотивація маніпулювання темою щодо скасування депутатського імунітету винесена за межі цього дослідження.

З метою дослідження запропонованого способу розв’язання проблеми визначено такі основні завдання: описати основні сутнісні характеристики сучасного інституту депутатської недоторканності; дослідити його складові елементи (індемнітет та імунітет) та суспільно-політичне призначення; виявити та узагальнити критичні застереження щодо скасування депутатського імунітету; знайти адекватний науково-обґрунтований спосіб розв’язання проблеми та запропонувати авторський підхід щодо подальшого удосконалення інституту депутатської недоторканності.

**Виклад основного матеріалу.** Передусім варто зробити короткий історичний екскурс щодо періодичності закидання українському суспільству ідеї про необхідність скасування депутатського імунітету та появи цього питання у порядку денному законодавця.

Першим про необхідність зняття депутатської недоторканності заговорив ще другий Президент України Л.Д. Кучма. Це питання було одним із пунктів його передвиборчої кампанії у 1999 році.

Як відомо, серед питань проведеного у 2000 році всеукраїнського референдуму було і питання скасування депутатського імунітету. За підсумками цього референдуму Центральною виборчою комісією повідомлено, що більшість виборців (89 %) проголосували за його скасування [4]. Проте Європейська спільнота у квітні 2000 року сприйняла Всеукраїнський референдум, яким пропонувалося визначитися стосовно скасування депутатської недоторканності, як загрозу парламентаризму. Цей референдум викликав негативну реакцію ПАРЄ, яка навіть порушувала питання про виключення України зі свого складу. У резолюції від 4 квітня 2000 року Парламентська Асамблея Ради Європи наголосила на особливому значенні депутатської недоторканності для нових демократій – країн, які перебувають на початковому етапі конституційного будівництва, до того ж в умовах, коли не завершено процес формування незалежної судової влади [5].

Певне занепокоєння перспективою подальшого повного скасування депутатського імунітету висловила і Європейська Комісія “За демократію через право” (Венеціанська Комісія). У висновку, затвердженому на її 44-му пленарному засіданні 13 – 14 жовтня 2000 року, зазначалося, що *“існують західні демократії, особливо в межах правової системи звичаєвого права, які не визнають принципу абсолютного імунітету членів парламенту від арешту та затримання, а тільки передбачають імунітет щодо заяв, зроблених у парламенті. В той же час, у цих країнах історично досить давно склалася традиція, за якою свавільний арешт опозиційних політиків є немислимим. Це не збігається з ситуацією в Україні, де демократія є досить молодого та де опозиційні політики висловлюють побоювання щодо їх арешту, якщо вони не будуть захищені цим положенням Конституції України. Це, звичайно, є ситуація, коли свобода думки та волевиявлення парламентаріїв може бути поставлена під загрозу”* [6].

Незважаючи на ці застереження, питання щодо перегляду депутатського імунітету після 2000 року неодноразово порушувалося в українському парламенті різними суб'єктами права законодавчої ініціативи.

Зокрема, Конституційний Суд України наголошував, що пропонувані відповідними законопроектами зміни щодо скасування недоторканності народних депутатів України стосуються лише їхнього спеціального статусу і не впливають на зміст конституційних прав і свобод людини і громадянина (їх скасування чи обмеження), а отже, не суперечать вимогам частини першої статті 157 Конституції України (висновки від 27 червня 2000 року № 1-в/2000, від 11 липня 2000 року № 2-в/2000, від 5 грудня 2000 року № 3-в/2000, від 10 вересня 2008 року № 2-в/2008, від 1 квітня 2010 року № 1-в/2010, від 10 липня 2012 року № 1-в/2012, від 27 серпня 2012 року № 2-в/2012, від 16 червня 2015 року № 1-в/2015). Жоден із цих законопроектів не пройшов повної законодавчої процедури через брак політичної волі.

Наразі подібні проекти законів опинилися у порядку денному українського парламенту поточного скликання.

Так, законопроект за реєстр. № 6773 “Про внесення змін до Конституції України (в частині скасування депутатської недоторканності)” було внесено групою з більш ніж 150 народних депутатів з різних політичних таборів 19 липня 2017 року. Передбачено, що у разі його прийняття як закону він набере чинності відразу після опублікування. За його включення до порядку денного і направлення до Конституційного Суду України проголосували 328 народних депутатів.

Законопроект за реєстр. № 7203 “Про внесення змін до статті 80 Конституції України (щодо недоторканності народних депутатів України)” був внесений 17 жовтня 2017 року Президентом України П. Порошенком як невідкладний, що вимагає його позачергового розгляду парламентом. При цьому у пояснювальній записці до нього наголошено, що “питання вдосконалення інституту суддівської недоторканності на сьогодні врегульовано Конституцією України (зі змінами, внесеними Законом України “Про внесення змін до Конституції України (щодо правосуддя)”). Питання ж щодо скасування недоторканності народних депутатів України й досі залишається невирішеним і за час, що минув з 16 січня 2015 року – дня внесення на розгляд парламенту законопроекту (реєстр. № 1776), не втратило актуальності. Суспільна думка з цього приводу й зараз свідчить, що гарантії недоторканності народних обранців в існуючому обсязі є не виправданими та по суті перетворилися у гарантії безкарності. На цьому наголошувалося і в Посланні Президента України до Верховної Ради України “Про внутрішнє та зовнішнє становище України в 2017 році”.

Як вбачається з пояснювальної записки до зазначеного законопроекту, позиція глави держави ґрунтується на суспільній думці, що сформована на основі відповідного рівня свідомості громадськості, внаслідок чого запропоновано концептуально хибний спосіб розв'язання проблеми, що не враховує вітчизняних наукових здобутків, а також застереження експертів, про які йтиметься далі.

У разі прийняття ініціативи у версії глави держави, цей Закон набере чинності з 1 січня 2020 року. За включення до порядку денного сесії і направлення до Конституційного Суду України законопроекту № 7203 віддали свої голоси 336 народних обранців, що є проявом наявності політичної волі цілком достатньої кількості парламентаріїв для ухвалення остаточного рішення.

Згідно з інформацією, що розміщена на веб-сайті Верховної Ради України [7], президентський законопроект з 20 вересня 2018 року перебуває на доопрацюванні в



профільному комітеті у зв'язку із застереженнями, що містяться у Висновку Конституційного Суду України від 19 червня 2018 року № 2-в/2018.

Зокрема, Постановою Верховної Ради України від 20.09.2018 р. № 2557-VIII Комітету Верховної Ради України з питань правової політики та правосуддя доручено опрацювати пропозиції та поправки до законопроекту та організувати надання народним депутатам України документів, передбачених частиною третьою статті 150 Регламенту Верховної Ради України, у період до 21 листопада 2018 року. Ця дата давно минула, а через невиконання цього доручення подальша процедура розгляду зазначеного законопроекту та його остаточного ухвалення не може відбутися. У такий спосіб реалізацію публічного зобов'язання щодо скасування необмеженого депутатського імунітету пригальмовано на рівні парламентського комітету, чим позбавлено виборця можливості переконатися у щирості продемонстрованих політиками намірів.

Разом з тим, судячи з кількості голосів на підтримку цих законопроектів, народні обранці, нехтуючи аргументами проти такої ініціативи, виявилися готовими до такого радикального кроку, незважаючи на настання тих закономірних наслідків в українських реаліях, від яких застерігали ПАРЕ та Венеціанська Комісія. Фактично йдеться про пошук належного балансу між двома по суті суперечливими суспільними інтересами – гарантування незалежності парламенту від інших гілок влади та запобігання зловживанню парламентським імунітетом.

Отже, аби уникнути чергової законодавчої помилки, хочеться сподіватися, що наступні голосування з цього питання відбуватимуться з повною відповідальністю кожного народного депутата України як державного діяча та усвідомлення наслідків такого політичного рішення.

Депутатській недоторканності як органічній складовій конституційно-правового статусу парламентарія присвячено багато вітчизняних досліджень, де обґрунтовується необхідність наявності обох елементів депутатської недоторканності – індемнітету та імунітету, що зумовлені розвитком парламентаризму.

Завдяки вітчизняним дослідженням розроблено фундаментальні теоретико-правові засади конституційного статусу народного депутата України та з'ясовано особливості національного інституту депутатської недоторканності, порівняно з конституційними практиками інших країн, у тому числі й сталих демократій. При цьому жоден вчений-конституціоналіст не зробив категоричного висновку про необхідність скасування депутатського імунітету на сучасному етапі державотворення.

Разом з тим, у контексті суворості законності та невідворотності покарання за скоєне Ю.О. Фрицький схиляється до доцільності зняття депутатського імунітету і зазначає: "...Оскільки на сучасному етапі демократизації держави, суспільства, органів державної влади, на жаль, побажання політиків не збігаються з їхніми справами, спостерігається падіння довіри народу до всіх інститутів влади, політичних партій і блоків, які захищають і вирішують у стінах парламенту, органах виконавчої та судової влади перш за все власні, особисті, а не загальнодержавні інтереси, що пояснюється зрощенням великого капіталу безпосередньо через його представників із законодавчою, виконавчою і судовою владою. Єдиним виходом з цього становища є застосування заходів безпосередньої відповідальності всіх без винятку посадових осіб, починаючи з Президента України, за свою діяльність, що повинно відобразитися у знятті депутатської недоторканності з депутатів усіх рівнів і державних службовців, починаючи з Прем'єр-міністра та міністрів, суддів усіх рівнів на підставі рівності всіх

без винятку перед законом та основоположних принципів, які, на жаль, не здобули свого закріплення у Конституції України, – суворості законності та невідворотності покарання за скоєне” [8, с. 343].

У результаті ж порівняльного аналізу конституційного регулювання інституту недоторканності парламентарія дослідниками, зокрема В.І. Борденюком, обґрунтовується висновок про необхідність перегляду та обмеження існуючого імунітету народного депутата України [9].

Подібний висновок міститься також і у дослідженні, проведеному спільно Інститутом міжнародних відносин Київського національного університету імені Тараса Шевченка та організацією Democracy Reporting International. При цьому використано звіт Венеціанської Комісії Ради Європи, у якому зазначено, що у країнах із ще не зміцнілою демократією є вищі ризики арешту чи обвинувачення депутатів на фальшивих та політично вмотивованих підставах. Отже, Україна не зовсім відповідає тим вимогам, що сприяють чи обґрунтовують скасування недоторканності. Зберігається ризик переслідування з політичних мотивів, якого може зазнати будь-який депутат, що виступить проти чийхось потужних інтересів. Але все ж таки, всі громадяни України, незалежно від матеріального і соціального статусу, повинні бути рівні перед законом. Під таким кутом зору депутатська недоторканність може бути якщо не скасована повністю (оскільки тією чи іншою мірою вона існує в більшості цивілізованих, демократичних держав), а хоча б істотно обмежена [10].

У контексті цього дослідження варто також взяти до уваги представлений Міжнародним інститутом демократії та сприяння виборам (International IDEA) порівняльний аналіз щодо наявності депутатського імунітету у 42-х країнах, а також взаємозалежність рівня корупції та виду імунітету [11]. Зроблене порівняння ілюструє повну або часткову відсутність депутатського імунітету лише у деяких західних країнах усталеної демократії. Повна відсутність депутатського імунітету свідчить про наявність практик, де індемнітет виконує роль самодостатньої гарантії.

Продемонстроване розмаїття конституційних практик свідчить, що у конституціях більшості держав традиційно закріплено дві основні політико-правові категорії, які складають депутатську недоторканність: 1) індемнітет – принцип невідповідальності за сказане депутатом (свобода висловлювань); 2) імунітет – принцип недоторканності (свобода від арешту).

Це дає підстави стверджувати, що незалежно від теоретичної концепції, визнаної у певній країні, парламентська недоторканність як явище спрямована на захист представників народу від свавілля виконавчої та судової влади. Характерними рисами інституту парламентської недоторканності є те, що він гарантує одночасно колективні права парламенту в цілому як органу, а також захист прав та дій депутатів як членів парламенту. Таке специфічне (подвійне) функціональне призначення інституту депутатської недоторканності зумовлене природою парламенту як представницького органу, що має репрезентувати та враховувати інтереси різних електоральних і соціальних груп шляхом формування “спільної волі” та її втілення у відповідних консенсусних рішеннях, а також у рішеннях парламентської більшості (коаліції) чи парламентської меншості (опозиції).

Отже, законодавчо закріплена система гарантій діяльності членів парламентів (депутатів) спрямована на забезпечення ефективної діяльності загальнонаціональних представницьких органів державної влади (парламентів) [12].

При цьому не варто ототожнювати статусний (професійний) імунітет парламентарія, глави держави, суддів з іншими правовими імунітетами, що гарантовані

людині на конституційному рівні та передбачені, зокрема положеннями розділу II Конституції України. Відповідні відмінності цих правових явищ досліджено О. Ткалею [13]. Разом з тим, на мою думку, з точки зору загально-філософського методу наукового пізнання, зазначені правові явища співвідносяться як загальне (статтями 3 і 29 Конституції України гарантується особиста недоторканність людини) і спеціальне (гарантований Основним Законом України статусний (професійний) імунітет парламентарія, глави держави, суддів). Такий підхід дозволяє вести дискусію з позиції відсутності дискримінації між двома різними за юридичною природою статусами, тим більше, що конституційне закріплення саме статусних (професійних) імунітетів пов'язане з принципом поділу влади.

В аспекті ж цієї статті достатньо констатувати, що інститут парламентських привілеїв як явище не є суто українським винаходом.

Загальновідомо, що основні європейські моделі організації парламентських привілеїв – “британська” і “французька” стали результатом історичного розвитку демократичних інститутів у цих країнах і були згодом адаптовані іншими державами у певній формі, тією чи іншою мірою.

Характеризуючи сучасні тенденції, Водянніков О. стверджує про “наближення національних інститутів парламентських імунітетів до певного єдиного стандарту. Таке наближення йде або шляхом розширення парламентських привілеїв, як, зокрема, в англосаксонській традиції, або звуження таких імунітетів, як це відбувалося протягом останнього десятиріччя в континентальній Європі. Такий рух по суті є рухом назустріч. Континентальна система була історичною батьківщиною концепції абсолютного імунітету парламентаріїв, найбільш спотвореною формою якої була доктрина абсолютних імунітетів, прийнята в колишньому Радянському Союзі і залишки якої досить відчутні в пострадянських країнах. Англосаксонська система, навпаки, в силу історичних особливостей отримала функціональний характер. Тому перетворення, що відбулися протягом останнього часу, вказують на подальше зближення двох систем” [14].

Об'єктивно існуючі натеper відмінності у національних системах парламентських привілеїв, хоча і характеризують особливості правового статусу парламентарія, однак виносяться автором за межі цього дослідження. У контексті ж статті пропонується зосередити увагу на традиційних елементах парламентських привілеїв – індемнітеті та імунітеті з огляду на сучасну конституційно-правову статусну доктрину, за якою член парламенту розглядається як представник всієї нації, а не виборчого округу, де його обрано, і логічним наслідком чого є заборона імперативного мандату та права відкликання парламентарія виборцями.

Як відомо, у 1996 році в Україні конституйовано інститут парламентських привілеїв, як депутатська недоторканність (частина перша статті 80 Конституції України). Отже, саме це поняття увійшло у вітчизняний законодавчий та науковий обіг як таке, що охоплює обидва елементи – депутатський індемнітет та імунітет. У науковому сенсі ці поняття співвідносяться відповідно як ціле і одиночне. З метою розкриття їх сутнісних характеристик необхідно окреслити найсуттєвіші ознаки обох елементів інституту депутатської недоторканності з винесенням за межі цієї статті питання фінансово-матеріального забезпечення діяльності парламентарія.

В Основному Законі України (частина друга статті 80) закріплено депутатський індемнітет як право народного депутата України на вільне висловлювання у парламенті та його органах з відповідними обмеженнями. Реалізація цього права деталізована

законами України про статус народного депутата України, про комітети Верховної Ради України та про Регламент Верховної Ради України.

За логікою конституційних і законодавчих положень народний депутат України, беручи безпосередню участь в обігу публічної інформації як представник влади, користується достовірною інформацією, яку він отримує за своїми зверненнями та запитами. За надання неправдивої або неповної інформації може наставати адміністративна відповідальність (стаття 188<sup>19</sup> КУпАП), а за вчинення незаконного впливу у будь-якій формі на народного депутата України – кримінальна відповідальність за втручання у діяльність державного діяча (стаття 344 КК).

Отже, користуючись своїм правом на отримання інформації (відповідно до статей 7, 15–17, 19 і 24 Закону України “Про статус народного депутата України”), парламентарій на власний розсуд може її оприлюднити з парламентської трибуни чи через ЗМІ з додержанням вимог законодавства та передбачених ним обмежень.

Забезпечуючи ж реалізацію права громадянина чи ЗМІ на інформацію, парламентарій має доводити до їх відома отриману ним інформацію без перекручення її змісту.

Безпосередній зворотній зв’язок з виборцями забезпечується через приймальню народного депутата, що уможливорює, з одного боку, отримання повної та об’єктивної інформації від виборця, а з іншого боку – належне використання цієї інформації у межах парламентського контролю.

Оскільки парламентський контроль на індивідуальному та колегіальному рівнях реалізується шляхом свідомо-вольової діяльності парламентарія, то зміст його висловлювань на сесії парламенту чи в його органах обмежується рамками нормативно визначеного індемнітету. Будь-яке відхилення від цих правил є підставою для настання індивідуальної відповідальності, зокрема у разі порушення честі чи гідності опонента або іншої особи, про яку згадувалося у виступі парламентарія.

Основним призначенням парламентського індемнітету є забезпечення права на критику дій більшості та уряду. Вільне висловлення депутатами власної позиції та запобігання надмірного тиску більшості на меншість є однією із засад існування парламенту як демократичного органу. Демократичний характер природи індемнітету впливає з того, що даний привілей покликаний захищати голос, позицію депутата та його дії, але не політику, яка за цим слідує. Саме тому будь-які висловлювання депутата у парламенті та його органах мають ґрунтуватися на достовірній інформації, що є основною передумовою цивілізованого парламентського контролю.

У контексті свободи слова та поширення правдивої інформації індемнітет не лише робить парламентаріїв від більшості та меншості рівними, а й сприяє, як свідчить практика функціонування парламентсько-урядових коаліцій у розвинутих демократіях, конструктивній співпраці уряду і парламенту, в тому числі завдяки незалежному парламентському контролю з боку меншості (опозиції).

У розроблених Парламентською Асамблеєю Ради Європи керівних принципах щодо прав та обов’язків опозиції в демократичному парламенті, що містяться у тексті Резолюції 160 (2008), варто виокремити ті положення, які стосуються індемнітету:

*“І. Парламентарії мають здійснювати свої повноваження незалежно. Вони не мають бути зв’язаними жодною інструкцією або отримувати зв’язуючи повноваження (обов’язковий примусовий мандат). Ніхто не може засуджувати парламентарія захищати ідеї, які йдуть проти офіційної політики уряду або які не схвалюються більшістю населення.*

*1. Національні парламенти держав-членів Ради Європи мають визнавати наступні права відносно опозиції або парламентської меншості:*

*2.1. свободу висловлення та свободу думки; члени опозиції повинні мати право користуватися свободою слова; вони повинні мати можливість вільно висловлювати свої ідеї;*

*2.2. опозиція повинна мати право на участь в нагляді, перевірці і контролі за діями та політикою уряду:*

*2.2.1. члени опозиції мають право на інформацію; члени опозиції і члени більшості повинні отримувати від уряду одну й ту ж інформацію” [15].*

Наведений перелік рекомендацій можна вважати тими об’єктивними та універсальними критеріями, за допомогою яких має формуватися правильне уявлення про соціально-політичне призначення сучасного інституту депутатської недоторканності.

Традиційно цей вид депутатської недоторканності (індемнітет) має, як правило, довічний характер, що виключає переслідування члена парламенту в майбутньому після припинення його депутатських повноважень.

Порівняно з індемнітетом, що безумовно є первинним елементом інституту депутатської недоторканності, депутатський імунітет як вторинний елемент цього інституту законодавчо закріплено на основі широкої концепції депутатської недоторканності (частина третя статті 80 Конституції України, стаття 27 Закону України “Про статус народного депутата України”), що ґрунтується на доктрині абсолютного імунітету. При цьому Закон не використовує юридичну категорію “імунітет”, а ототожнює її з недоторканністю народного депутата України.

Основна відмінність національної концепції від концепцій європейських країн полягає в тому, що народного депутата України не може бути затримано чи заарештовано без згоди Верховної Ради України на місці вчинення ним злочину чи одразу після його вчинення. Відповідні конституційні приписи знайшли своє відображення у положеннях Кримінального процесуального кодексу України (статті 207, 208, 481 та 482) та, без сумніву, є процесуальною перешкодою для ефективного кримінального переслідування народного депутата України, повноваження якого не припинено. Особливості порядку притягнення народного депутата до кримінальної відповідальності наразі несистемно унормовано Кримінальним процесуальним кодексом України та Законом про Регламент Верховної Ради України. Це питання потребує окремого дослідження.

Парламентська процедура зняття депутатського імунітету, з одного боку, відіграє відповідну роль у механізмі стримувань і противаг (наприклад у разі встановлення політичних мотивів кримінального переслідування), а з іншого боку, дозволяє депутатському корпусу зберегти авторитет парламенту шляхом самоочищення – надання згоди на притягнення члена парламенту до кримінальної відповідальності.

Сутність же парламентського імунітету полягає в тому, що він спрацьовує як запобіжник під час оцінки у парламенті за встановленою процедурою (глава 35 Регламенту Верховної Ради України) обставин і характеру кримінального переслідування та зняття імунітету з парламентарія у разі відсутності політичних мотивів такого переслідування, що може бути пов’язане саме з певними висловлюваннями у парламенті чи його органах. Підтвердженням цьому є парламентська практика реалізації приписів статті 80 Конституції України в незмінній редакції, яка не має жодної документально зафіксованої відмови парламентом у наданні згоди на притягнення народного депутата до кримінальної відповідальності у

зв'язку з політичними мотивами кримінального переслідування. Водночас факт відсутності подібної статистики не може виключати існування спроб використання системи кримінальної юстиції за часів президенства В. Януковича для прихованого політичного переслідування опозиційних парламентаріїв.

Незалежно від різноманітності складу парламенту конституційно-правові гарантії депутатської недоторканності спрямовані на те, щоб його робота відбувалася з належною повагою до плюралізму думок.

Так, у пункті 3 Резолюції ПАРС 1601 (2008), що присвячена процедурним керівним принципам щодо прав та обов'язків опозиції в демократичному парламенті, зазначено, що: *“Політична опозиція як у, так і поза межами парламенту – є надзвичайно важливим компонентом ефективного здійснення демократії. Одна з головних функцій опозиції – це можливість запропонувати надійну політичну альтернативу до більшості, що є при владі, в наданні на суспільний розгляд інших політичних варіантів. Шляхом контролю та критики роботи уряду при владі, постійної оцінки дій уряду та притягнення уряду до звітності, опозиція працює для забезпечення прозорості державних рішень і ефективності в управлінні державними справами, забезпечуючи, таким чином, захист державного інтересу і запобігаючи зловживанню та неправильному управлінню”* [15].

Загально визнано, що серед інших традиційних форм парламентського контролю, парламентські слухання та дебати є найдієвішими інструментами публічного інформаційно-корекційного контролю за діяльністю уряду.

Таким чином, завдяки органічному поєднанню індемнітету та імунітету, що мають відповідне функціонально-цільове призначення, забезпечується повноцінний статус парламентарія як народного представника.

Разом з тим, самої лише наявності зазначених конституційно-правових гарантій забезпечення парламентського контролю недостатньо, аби він здійснювався незалежно та ефективно. Обов'язковою умовою такого парламентського контролю є усвідомлення кожним парламентарієм своєї ролі як первинної та водночас ключової ланки у системі парламентського контролю, що утворює індивідуальну основу для незалежного парламентського контролю. Інакше кажучи, лише за умови комплексного поєднання згаданих юридичних гарантій та добросовісної реалізації парламентарієм своїх інтелектуальних і професійних здібностей суспільство може розраховувати на дійсно незалежний парламентський контроль.

Наявні наразі у тексті присяги народного депутата України слова “виконувати свої обов'язки в інтересах усіх співвітчизників” мають відповідне навантаження саме у контексті здійснення парламентського контролю незалежно від існуючої моделі парламентських виборів.

На формування вітчизняної (широкої) концепції депутатської недоторканності вплинув не лише законодавець, а й Конституційний Суд України. Відповідні правові позиції містяться у його рішеннях та висновках.

Зокрема, Конституційний Суд України неодноразово наголошував, що недоторканність народних депутатів України не є особистим привілеєм, індивідуальним правом народного депутата України, а має публічно-правовий характер; вона спрямована на убезпечення народного депутата України від незаконного втручання в його діяльність, на забезпечення безперешкодного та ефективного здійснення ним своїх функцій та належного (нормального) функціонування парламенту (висновок від 11 липня 2000 року № 2-в/2000, рішення від 27 жовтня 1999 року № 9-рп/99, від 26 червня 2003 року № 12-рп/2003).

Тому зміни до статті 80 Конституції України не суперечать вимогам частини першої статті 157 Конституції України, оскільки стосуються лише спеціального статусу народного депутата і не впливають на зміст конституційних прав і свобод людини і громадянина (їх скасування чи обмеження) (висновки від 27 червня 2000 року № 1-в/2000, від 11 липня 2000 року № 2-в/2000, від 5 грудня 2000 року № 3-в/2000, від 10 вересня 2008 року № 2-в/2008, від 1 квітня 2010 року № 1-в/2010, від 10 липня 2012 року № 1-в/2012, від 27 серпня 2012 року № 2-в/2012, від 16 червня 2015 року № 1-в/2015).

Будучи послідовним у своїх правових позиціях і розглянувши законопроект за №7203, Конституційний Суд України зробив у висновку від 19 червня 2018 року № 2-в/2018 такі застереження: *“Водночас Конституційний Суд України вважає за доцільне звернути увагу на те, що, ухвалюючи рішення щодо скасування депутатської недоторканності, необхідно враховувати стан політичної та правової системи України – її здатність у разі повної відсутності інституту депутатської недоторканності забезпечити безперешкодне та ефективне здійснення народними депутатами України своїх повноважень, функціонування парламенту, а також реалізацію конституційного принципу поділу державної влади.*

*Крім того, на наслідки повного скасування депутатської недоторканності звертала увагу і Європейська Комісія “За демократію через право” (Венеціанська Комісія), яка зазначала, що у політичній системі з вразливою демократією, такою, як в Україні, повне скасування недоторканності може бути небезпечним для функціонування та автономії парламенту (пункт 18 Висновку щодо проекту закону про внесення змін до Конституції України щодо недоторканності народних депутатів України та суддів, ухваленого Венеціанською Комісією на її 103-му пленарному засіданні 19-20 червня 2015 року)” [16].*

Про можливі ризики та наслідки скасування депутатського імунітету йдеться також і в окремій думці судді Конституційного Суду України Мельника М.І., де зазначено: *“Скасування імунітету парламентаріїв може зробити їх беззахисними перед виконавчою владою, залежними від неї, стати своєрідним “щепленням” від опозиційності, ускладнити розвиток демократії в Україні. Повне скасування депутатського імунітету може дозволити собі лише держава з надзвичайно високим рівнем демократії, пануванням верховенства права, в якій фактично неможливим є безпідставне звинувачення особи та притягнення її до кримінальної відповідальності.*

*Ризики та наслідки скасування депутатського імунітету можна передбачити за чітко вираженою тенденцією останнього етапу конституційної реформи, яку виявили попередні законодавчі ініціативи щодо внесення змін до Конституції, що були предметом розгляду Конституційний Суд у 2015 – 2016 роках. Ця тенденція полягає, з одного боку, у зниженні рівня незалежності судової та законодавчої влади, зменшенні обсягу повноважень парламенту, з другого – у розширенні повноважень Президента України та посиленні його політичного впливу в системі державної влади” [17].*

Відповідна позиція щодо депутатської недоторканності міститься і в рекомендаціях, підготовлених Місією Європейського Парламенту (Місія Кокса) у *“Доповіді та дорожній карті щодо внутрішньої реформи та підвищення інституційної спроможності Верховної Ради України” (вересень 2015 – лютий 2016 рр.). Так, на думку Місії Кокса, “повне скасування системи депутатської недоторканності суперечитиме нормам найефективнішої міжнародної парламентарної практики... Таке скасування також наражатиме народних депутатів на ризики стати об’єктом*

політично вмотивованого судового переслідування за виконання законних обов'язків. Водночас обмеження недоторканності, беззаперечно, необхідне у разі вчинення кримінальних правопорушень, а також для надання Верховній Раді повноважень на позбавлення недоторканності за певних обставин" [18].

Наявність подібних аргументів на користь обмеження депутатського імунітету, а не повного його скасування, ускладнює свідоме і відповідальне голосування кожного народного депутата під час реалізації спеціальної процедури, що визначена статтею 155 Конституції України. Проте саме депутатами поточного (восьмого) скликання в ході судової реформи переглянуто та закріплено функціональний імунітет щодо суддів і суддів Конституційного Суду України.

За такої ситуації наразі у тексті Конституції України в редакції Закону України № 742-VII від 21.02.2014 (ВВР, 2014, № 11, ст. 143) зі змінами, внесеними Законом України № 1401-VIII від 2 червня 2016 року (Відомості Верховної Ради (ВВР), 2016, № 28, ст. 532) [19], передбачено статусний імунітет для Президента України (стаття 105), народних депутатів України (стаття 80), суддів (стаття 126) і суддів Конституційного Суду України (стаття 149).

Проте в нинішніх українських реаліях питання удосконалення імунітету як депутатського, так і президентського вирішуються несистемно, в тому числі й завдяки різним правовим позиціям органу конституційної юрисдикції щодо скасування недоторканності Президента України, народних депутатів України, суддів і суддів Конституційного Суду України.

Так, у 2010 та 2012 роках Конституційний Суд України мав протилежну правову позицію та визнав скасування гарантій недоторканності стосовно Президента України і суддів такими, що не відповідають вимогам частини першої статті 157 Конституції України [20; 21]. Рішення ж та висновки, ухвалені Конституційним Судом України, є обов'язковими, остаточними і не можуть бути оскаржені (стаття 151-2 Конституції України).

Наявність протилежних правових позицій Конституційного Суду України щодо одного і того ж конституційно-правового явища (статусного імунітету) є свідченням подвійних стандартів, що не мають наукового підґрунтя.

### **Висновки.**

З огляду на викладене можна підсумувати таке.

1. Вітчизняними науковцями констатовано наявність об'єктивної необхідності щодо удосконалення існуючого нині обсягу та змісту імунітету парламентарія. У зв'язку з цим запропонований суспільству "рецепт подолання політичної корупції" шляхом повного скасування парламентського імунітету є не лише помилковим, а й шкідливим для розвитку парламентаризму та становлення незалежного парламентського контролю в Україні.

Наведені у цій статті думки науковців, демократичні стандарти Ради Європи, аналітичні матеріали, судження та аргументи є цілком достатніми для усвідомлення суспільно-політичного призначення депутатського імунітету як конституційної гарантії добросовісного і незалежного виконання парламентарієм своїх обов'язків, і насамперед у процесі реалізації парламентського контролю. Наявність цієї конституційної гарантії є правостимулюючим засобом, що формує позитивну правову мотивацію до суспільно-корисної, представницької діяльності.

За нинішніх соціально-політичних умов в Україні, відсутності ефективної і незалежної правоохоронної системи, реально незалежного суду є передчасною постановка питання про скасування депутатського імунітету. Поточні інтеграційні



процеси та парламентська реформа зумовлюють розробку сучасної концепції депутатської недоторканності на основі такого обсягу індемнітету та імунітету, що притаманний статусу парламентаріїв розвинутих демократій та враховує демократичні стандарти Ради Європи [15; 22]. В іншому випадку скасування депутатського імунітету знівелює суспільно-політичне призначення проголошеного в Основному Законі України індемнітету, надавши йому декларативний характер, що перетворить парламентський контроль у звичайну бюрократичну формальність.

Поспішне та безвідповідальне скасування законодавцем депутатського імунітету замість його удосконалення на доктринально іншій основі (відмова від абсолютного імунітету) збільшить в умовах перехідного періоду ризику для політичних переслідувань та свавільних арештів опозиційних політиків.

2. Закріплений у частині третій статті 80 Конституції України принцип депутатського імунітету не є особистим привілеєм парламентарія, а конституційно-правовою гарантією незалежності його діяльності та роботи парламенту. Функціонування депутатського імунітету в “молодих демократіях” є виправданим саме у його гармонійному поєднанні з депутатським індемнітетом.

3. У разі остаточного прийняття Верховною Радою України законопроекту, яким скасовується депутатський імунітет, Україна як держава-член Ради Європи зробить крок, що вважатиметься відхиленням від демократичних стандартів Ради Європи.

4. Існуючий на сьогодні в Україні зміст та обсяг депутатського імунітету потребує удосконалення з урахуванням демократичних стандартів Ради Європи, сучасних тенденцій в національному праві розвинутих демократій стосовно парламентських імунітетів та на основі науково-обґрунтованої концепції депутатської недоторканності.

Будучи переконаним у необхідності ухвалення законодавцем у ході конституційної реформи виваженого політичного рішення щодо удосконалення змісту та обсягу депутатського імунітету, вважаємо, що в умовах перехідного періоду в основі сучасної концепції депутатської недоторканності може бути використано функціональний суддівський імунітет, однак з урахуванням особливостей статусу парламентарія, змісту та обсягу індемнітету. Відповідні напрацювання мали б здійснюватися фахівцями у галузі конституційного права.

Удосконалення ж вітчизняних конституційних і законодавчих положень щодо статусу парламентарія як складової парламентської реформи має відбуватися з урахуванням традиційних для європейського парламентаризму інститутів захисту депутата від неправомірних впливів з боку держави та за умови забезпечення балансу між недоторканністю та відповідальністю парламентарія. Саме такий концептуальний підхід сприятиме розвитку парламентаризму та слугуватиме відновленню довіри суспільства до Верховної Ради та її легіслатури.

### Використана література

1. Всеукраїнське опитування громадської думки Київського міжнародного інституту соціології. URL: <https://www.kiis.com.ua/?lang=ukr&cat=reports&id=851&page=1>
2. Костицький М.В. Філософсько-правовий аналіз депутатського імунітету та індемнітету в Україні. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького*. 2011. № 4. С. 8-12. URL: [http://nbuv.gov.ua/UJRN/Nivif\\_2011\\_4\\_3](http://nbuv.gov.ua/UJRN/Nivif_2011_4_3)
3. Угода про коаліцію депутатських фракцій “Європейська Україна”. URL: <https://zakon.rada.gov.ua/rada/file/text/33/f439014n8.pdf>

4. Повідомлення Центральної виборчої комісії від 25 квітня 2000 року “Про підсумки всеукраїнського референдуму від 16 квітня 2000 року”. URL: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=n0002359-00>
5. Рекомендація Парламентської Асамблеї Ради Європи від 4 квітня 2000 року. *Юридичний вісник України*. № 15. 13-19 квітня 2000 р.
6. Висновок Європейської Комісії “За демократію через право”. URL: [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-INF\(2000\)014-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-INF(2000)014-e)
7. Про внесення змін до статті 80 Конституції України (щодо недоторканності народних депутатів України): проект Закону України, реєстр. № 7203 від 17.10.2017 р. URL: [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=62727](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62727)
8. Фрицький Ю.О. Державна влада в Україні: становлення, організація, функціонування: монографія. Дніпропетровськ: Ліра ЛТД, 2006. 360 с.
9. Борденюк В.І. Депутатська недоторканність як гарантія діяльності представницького органу державної влади: конституційно-правові аспекти. *Юридична Україна*. 2011. № 3. С. 22-27.
10. Недоторканність по-європейськи. Між диктатурою та зловживаннями. – (Інститут міжнародних відносин Київського національного університету імені Тараса Шевченка; Democracy Reporting International, 17 лютого 2015 р.). URL: <http://www.eurointegration.com.ua/experts/2015/02/7/7030533>
11. Дослідження Міжнародного інституту демократії та сприяння виборам. URL: [https://drive.google.com/file/d/11YARQD8ih81vDL7BDEJRB\\_9Fn8Bar4sx/view](https://drive.google.com/file/d/11YARQD8ih81vDL7BDEJRB_9Fn8Bar4sx/view)
12. Конституційне право України. Академічний курс: підручник: у 2 т. / за заг. ред. Шемшученка Ю.С. Київ.: Юрид. думка, 2008. Т. 2. С. 376.
13. Ткаля О.В. Класифікація правових імунітетів. *Науковий вісник Ужгородського національного університету. Серія “Право”*. Ужгород, 2012. Вип. 20. Ч. 2. Т. 1. С.81-85. URL: <http://dspace.onua.edu.ua/handle/11300/3251>
14. Водянніков О.Ю. Статус парламентарів. Парламентські імунітети в сучасних демократичних державах. URL: [https://minjust.gov.ua/m/str\\_2408](https://minjust.gov.ua/m/str_2408)
15. Процедурні керівні принципи щодо прав та обов’язків опозиції в демократичному парламенті: Резолюція ПАРЕ 1601 (2008). URL: [http://w1.c1.rada.gov.ua/pls/mpz/docs/753\\_1601\\_Opozytsija\\_rezoljutsija.htm](http://w1.c1.rada.gov.ua/pls/mpz/docs/753_1601_Opozytsija_rezoljutsija.htm)
16. Висновок Конституційного Суду України у справі за конституційним зверненням Верховної Ради України про надання висновку щодо відповідності законопроекту про внесення змін до статті 80 Конституції України (щодо недоторканності народних депутатів України) (реєстр. № 7203) вимогам статей 157 і 158 Конституції України від 19 червня 2018 року № 2-в/2018. *Вісник Конституційного Суду України*. 2018. № 4. С. 86.
17. Мельник М.І. Депутатська недоторканність: скасувати не можна обмежити. Окрема думка судді Конституційного Суду України Мельника М.І. стосовно Висновку Конституційного Суду України у справі за конституційним зверненням Верховної Ради України про надання висновку щодо відповідності законопроекту про внесення змін до Конституції України (в частині скасування депутатської недоторканності) (реєстр. № 6773) вимогам статей 157 і 158 Конституції України. *Юридичний вісник України*. 29 червня – 5 липня 2018 року. № 26 (1199). С. 6-7.
18. Доповідь та дорожня карта щодо внутрішньої реформи та підвищення інституційної спроможності Верховної Ради України (вересень 2015 р. – лютий 2016 р.). – (Підготовлена місією Європейського Парламенту з оцінки потреб під головуванням Пета Кокса). URL: <http://www.europarl.europa.eu/resources/library/media/20160301RES16508/20160301RES16508.pdf>
19. Конституція України: Закон України. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141, з наступними змінами.
20. Висновок Конституційного Суду України у справі за зверненням Верховної Ради України про надання висновку щодо відповідності законопроекту про внесення змін до Конституції України (щодо гарантії недоторканності для окремих посадових осіб) вимогам

статей 157 і 158 Конституції України (справа про внесення змін до статей 80, 105, 108 Конституції України) від 1 квітня 2010 року № 1-в/2010. *Вісник Конституційного Суду України*. 2010. № 3. Стор. 67.

21. Висновок Конституційного Суду України у справі за зверненням Верховної Ради України про надання висновку щодо відповідності законопроекту про внесення змін до Конституції України щодо недоторканності вимогам статей 157 і 158 Конституції України (справа про внесення змін до статей 80, 105, 126, 149 Конституції України) від 10 липня 2012 року № 1-в/2012. *Вісник Конституційного Суду України*. 2012. № 4. Стор. 34.

22. Про двадцять принципів боротьби з корупцією: Резолюція № R(97)24 Комітету Міністрів Ради Європи від 6 листопада 1997 року. URL: [https://zakon.rada.gov.ua/rada/show/994\\_845](https://zakon.rada.gov.ua/rada/show/994_845).

~~~~~ \* \* \* ~~~~~

УДК 340:374.3

УХАНОВА Н.С., старший науковий співробітник НДІП НАПрН України

## ПРАВОВА КУЛЬТУРА МОЛОДІ В УКРАЇНІ

**Анотація.** Про сучасний стан правової культури української молоді, особливо у контексті усталених уявлень про критичний стан правосвідомості молодого покоління.

**Ключові слова:** правова культура, правосвідомість, правове виховання, правовий нігілізм, правова освіта.

**Summary.** About current state of the legal culture of Ukrainian youth, especially in the context of the established ideas about the critical state of legal awareness of the younger generation.

**Keywords:** legal culture, legal awareness, legal education, legal nihilism, legal education

**Аннотация.** О современном состоянии правовой культуры украинской молодежи, особенно в контексте устойчивых представлений о критическом состоянии правосознания молодого поколения.

**Ключевые слова:** правовая культура, правосознание, правовое воспитание, правовой нигилизм, правовое образование.

**Постановка проблеми.** Курс на побудову європейської, демократичної, соціальної, правової держави в Україні передбачає не тільки відхід від домінування влади над правом, а й високий рівень сформованості правосвідомості і правової культури населення країни. Розглядаючи правову культуру як сферу свободи, що сприяє реалізації людиною власних інтересів і потреб, не можна забувати, що вона передбачає високий рівень відповідальності і дисципліни, без яких свобода неможлива. Теоретичне, правове і практичне вирішення проблем, пов'язаних з організацією правового виховання молоді, дозволить підняти престиж права, виховати повагу до закону та створить умови для розвитку правової демократичної держави. В умовах активного розвитку технологій та спровокованих ними трансформаційних процесів у суспільстві питання формування правової культури молоді в Україні є надзвичайно актуальним.

**Метою статті** є визначення напрямків підвищення правової культури молоді України з урахуванням особливостей українського законодавства в частині регламентації прав і обов'язків основних інститутів соціалізації.

**Виклад основних положень.** В сучасній Україні простежується зниження рівня правосвідомості українського соціуму, послаблення моральних цінностей, а правопорушення стали ледь не нормою поведінки. Особливу небезпеку становлять такі види правопорушень, наслідком яких є свідоме вчинення людиною умисних, переважно тяжких кримінальних злочинів, мотивами яких найчастіше стають жорстокість, корисливість, організована злочинність і корупція, що завдають значної шкоди процесу реалізації принципу верховенства права, недоторканності основних прав і свобод людини, становленню демократичної, правової держави, підвищенню рівня правової культури особистості і суспільства в цілому.

З огляду на обрання українським суспільством європейського шляху розвитку особливого значення набувають формування нового юридичного мислення, виховання загальної правової культури, вироблення почуття відповідальності, справедливості, поваги до закону.

Під правовою культурою розуміють різновид загальної культури, який становить систему цінностей, що досягнуті людством у галузі права і стосується правової реальності певного суспільства. Правова культура, виникає не сама по собі, а як результат процесу правової соціалізації особи, послідовне набуття правових знань, залучення до правових цінностей і культурних надбань суспільства, що в результаті впливає на правомірну поведінку суб'єкта, його правову активність.

У “Національній програмі правової освіти населення”, затвердженій Указом Президента України 18 жовтня 2001 року, наголошується: “Потребують вирішення на державному рівні питання дальшого розвитку правосвідомості населення, подолання правового нігілізму, задоволення потреб громадян у одержанні знань про право.... Крім того реалізація Програми сприятиме підвищенню рівня правової культури як окремих громадян, так і суспільства в цілому; формуванню у громадян поваги до права, гуманістичних правових ідей, загальнолюдських та національних правових цінностей, а також подоланню правового нігілізму; поліпшенню якості підготовки викладачів правових дисциплін та підвищенню ефективності викладання цих дисциплін у загальноосвітніх, професійно-технічних, вищих навчальних закладах і закладах післядипломної освіти; підвищенню рівня правової поінформованості населення” [1, с. 37].

Реалізація проголошеної в Конституції України мети формування демократичної, соціальної, правової держави залежить від багатьох передумов, серед яких — наявність високого рівня правової свідомості і правової культури. Саме на підвищення якісного стану цих чинників правової держави спрямовано процес правового виховання, особлива актуальність вивчення якого в сучасних умовах визначає появу публікацій, автори яких намагаються розкрити його сутність та зміст Проблеми формування правової культури досліджували М. Алексєєв, І. Арістова, В. Бабкін, В. Головченко, О. Довгань, В. Костюк, В. Оксамитний, М. Орзих, В. Пилипчук, М. Подберезький, Л. Рабинович, О. Скакун, А. Скуратівський, С. Сливка, Н. Ткачова, В. Фурашев, І. Цвік, М. Щербань та багато інших [2].

Поняття правової культури має багато інтерпретацій, але всі вони, так чи інакше, акцентують увагу на тому, що правова культура є відбиттям права в культурі. За визначенням А. Скуратівського, у широкому розумінні правова культура – це “суспільно-правовий феномен, який включає в себе найсуттєвіші результати сукупного правового досвіду суспільства, насамперед право і правосвідомість, правову діяльність, законність і правопорядок та відображає якісний рівень розвитку правового буття. У вузькому розумінні правова культура є системою духовно-правових цінностей: правових знань, переконань, уявлень, світоглядно-правових орієнтацій, що відображаються в правовій свідомості людей і органічно поєднані з їх соціально-правовою активністю щодо освоєння та творення суспільно-правового буття” [3, с. 6].

Правова культура є засобом правового регулювання суспільних відносин, заснованих на законах, формах взаємодії їх учасників; органічно пов'язана та взаємодіє із законодавством; використовується як інструмент покращення стану правового життя суспільства в цілому; сприяє спілкуванню суб'єктів політичного й правового життя суспільства, що виражається в різних формах правомірної поведінки та мислення, побудованого на вільному виборі гарантованих законами правових засобів досягнення поставлених цілей.

Правова культура формується під впливом об'єктивних та суб'єктивних факторів суспільного розвитку. На неї впливають не тільки історичні та соціальні процеси, а й геополітична ситуація в державі і духовна сфера суспільства. Якщо правова система функціонує в умовах законності, свободи, соціальної справедливості, поваги до права,

то й рівень правосвідомості громадян у такій державі має бути високим, що виявляється у повазі до права та правових знань, традицій, виробленні потреби діяти у відповідності до закону, сприяє правовій активності громадян, посадових осіб і законодавців, урядовців та ін. відповідно до правових установок та переконань.

Отже, показниками правової культури є відповідність права вимогам справедливості та свободи, якість системи законодавства, участь громадян в управлінні державою, рівень якості роботи правоохоронних і правозастосовних органів та посадових осіб, рівень правотворчої та правозастосовної культури, рівень правосвідомості громадян і посадових осіб, наявність знань про державний устрій, призначення держави, політичну систему суспільства, норм права, стан законності та правопорядку, поваги до юридичної професії, належний ступінь розвитку юридичної науки тощо.

Правова культура особи передбачає наявність знань законодавства, переконаність у необхідності і соціальній корисності законів і підзаконних актів та вміння користуватися ними у практичній діяльності. Змістом правової культури особи є: правосвідомість і правове мислення, правомірна поведінка, а також результати правомірної поведінки і правового мислення [4].

Найважливішим фактором формування високого рівня правової культури молоді є правове виховання.

Рябко І. під правовим вихованням розуміє визначений і систематичний вплив на свідомість, психологію (індивідів і суспільних груп), усього способу суспільного життя та ідеологічних чинників з метою формування у них, на основі правової ідеології глибоких і стійких уявлень, переконань і почуттів, прищеплення їм високої правової культури, навичок юридичного спілкування відповідно до рівня і вимог сучасного правового розвитку суспільства [5, с. 35].

Іншими словами, метою правового виховання є формування системи знань, переконань, мотивів, настанов та звичок соціально активної поведінки. Одержані знання допомагають суб'єкту сформулювати ціннісні орієнтації та правові настанови, які він зможе застосувати у повсякденному житті. Крім того, вони відіграють важливу роль в упорядкуванні діяльності людей, виступають стрижневою основою правової культури та правосвідомості і в остаточному підсумку впливають на формування ставлення громадянина до різних суспільних і правових явищ, визначають його поведінку.

Від рівня правового виховання залежать і рівень правової культури суспільства, швидкість перетворення соціальних і правових норм у реальність, трансформація нормативних вимог у звичку та соціально-активну поведінку.

Ряд дослідників звертають увагу на те, що в Україні рівень правової культури молоді є невисоким, зокрема С. Третяк відзначає зниження рівня правової свідомості молоді в Україні: “Зарозуміле ставлення деякої частини молоді до себе і оточуючих знаходить прояви у відкритій неповазі до людей, незалежно від їх віку або соціального статусу, що призводить не лише до порушення дисципліни, а й прав та свобод людини і громадянина... З великим побоюванням треба нам усім ставитися до зростаючої бездуховності, особливо серед молоді. Без цілеспрямованого виховання (у тому числі й правового) держава аж ніяк не може обійтися...” [6, с. 27].

В Україні відбувається процес девальвації права, його регулятивних чинників, спостерігається масова неповага до права, зневажливе ставлення до законодавства, правових норм, широких масштабів набули явища правового нігілізму, який заперечує цінність права – зазначає О. Ганзенко [7, с. 283].

У своїй доповіді “Права людини: основні загрози їх забезпечення в Україні” В. Фурашев звертає увагу на відсутність в Україні на практиці принципів “закон – один

для всіх” та “невідворотність покарання”, що є загрозами у сфері дотримання та забезпечення прав людини [8, с. 20].

Нерозвиненість у населення юридичних традицій, що переходять у відкритий правовий нігілізм, заперечення необхідності і цінності права мають глибокі історичні корені. З покоління в покоління в Україні проявляється зневага до закону та суду, терпимість до свавілля – зазначає І. Дмитрієнко [9, с. 234].

За нашими спостереженнями, навіть ряд законодавців, політичних лідерів, керівників суспільних організацій і т.д. не відзначаються високим рівнем правової культури. І справа не у тому, що вони не знають законів, а у тому, що вони не рахуються з ними, тобто зневажають право.

Рівень правової культури залежить від чинників, які характеризують рівень правосвідомості, досконалості законодавства, організації роботи з його дотримання, стан законності й правопорядку, структура якої є не лише багатоаспектною, а й багатогранною, яка складається з багатьох елементів. Одним із них є досягнення якісного стану юридичної охорони та захисту основних прав і свобод людини та громадянина. Показником такого стану необхідно вважати: наявність демократичного, гуманістичного, справедливого законодавства, його відповідність міжнародним правовим стандартам у сфері прав людини; існування ефективних національних правових засобів та процедур для захисту конституційних прав і свобод; реальна можливість звернутися до міжнародних правових інституцій – Європейської Комісії з прав людини, Європейського Суду з прав людини. Не менш важливим елементом правової культури суспільства є ступінь впровадження у практику суспільного і державного життя принципів верховенства права і закону [10].

Криза права, сучасної правової свідомості, як важелі правової культури, зумовлена загальною кризою суспільних відносин в Україні, з якої має вийти українське суспільство. Вимога знати, поважати і виконувати закони має бути однією з першочергових завдань у вихованні молодого покоління. Правове виховання має стати важливим регулятором поведінки, важливим каналом засвоєння колективного досвіду суспільства.

Однією із сучасних форм впливу (негативного та деструктивного) на правову свідомість молоді є соціальні мережі. Сьогодні за допомогою соціальних мереж можна розповсюдити будь-яку інформацію на будь-яку аудиторію, при цьому не витрачаючи багато ресурсів та часу. В. Пилипчук у доповіді “Актуальні питання захисту прав, свобод і безпеки людини в сучасному інформаційному суспільстві” відзначає: “...система захисту прав, свобод і безпеки людини в умовах інтенсивного розвитку інформаційних технологій, ресурсів, продукції і послуг залишається далеко від ідеальної та потребує суттєвих трансформацій”. В низці зазначених ним проблем він звертає увагу на “проблеми правової культури та моральності в інформаційній сфері:

- спостерігається тенденція до різкого падіння моральності й поваги до загальнолюдських цінностей при так званому “віртуальному” спілкуванні;
- відсутні ефективні правові механізми протидії порушенням прав і свобод людини в мережах Інтернет та ЗМІ;
- обмежені можливості судового захисту честі, гідності чи приватності громадян” [11, с. 6, 8].

Негативні явища серед молодіжного середовища, такі як підліткова наркоманія, алкоголізм, проституція, відсутність зайнятості, злочинність, безпритульність, викликані, у тому числі й низьким рівнем правової культури населення та недостатністю використання засобів правовиховного впливу на формування правової культури молоді.

В сучасному світі значний вплив на свідомість людей мають засоби масової інформації. Але й серед журналістів часто зустрічається правовий інфантилізм (юридична безпечність), правовий нігілізм (зневага до права), правовий негативізм (відкидання права), що створює загрозу формування в соціумі негативного ставлення до права. Проблема правового нігілізму є надзвичайно актуальною для формування правової культури і правосвідомості сучасної молоді України, відповідальної за подальшу долю держави, її соціально-економічний, політико-правовий, духовний і моральний розвиток.

Правовий нігілізм відкидає соціальну цінність права і культивує негативне ставлення до нього, належить до стійких і поширених виявів деформації правосвідомості населення. Правовий нігілізм може виникнути через історичні передумови, пов'язані з безправністю людини, самодержавством, авторитаризмом, беззаконням, репресіями тощо. Низька загальна і правова культура населення, незадовільна якість законодавства, його декларативність, стан всездозволеності у суспільстві та у державі сприяють формуванню правового нігілізму.

Анексія Криму та збройний конфлікт на окупованих Російською Федерацією територіях Донецької та Луганської областей, що спричинили глибокі суспільно-політичні перетворення в Україні, внесли суттєві корективи в життєві орієнтації молоді, її поведінку, соціально-економічне становище та спричинили ряд проблем, серед яких зневіра, розчарування у владі, у справедливості правових інститутів та безнадійності на майбутнє.

Виявом такого стану є небажання громадян, і в першу чергу, молоді, брати участь в політичному та соціальному житті. Як показують результати досліджень, більшість опитаних молодих людей або взагалі не цікавляться політичним життям (31,8 %), або проявляють інтерес до нього дуже рідко (32,4 %). Найменшу зацікавленість політичним життям країни проявляють підлітки віком від 14 до 19 років, а найбільшу – молодь від 25 до 29 років. Постійно слідкує за актуальними політичними подіями в країні молодь у віці від 30 до 34 років. В розрізі регіонів молодь, яка проживає у Центральному (21,9 %) регіоні країни, на відміну від молоді, яка мешкає у інших регіонах, постійно стежить за політичним життям в Україні. Частіше про те, що взагалі не цікавляться політикою, під час опитування вказала молодь, яка мешкає у Північному (22,4 %) та Південному (22,2 %) регіонах України. Найбільшу електоральну активність (70,5 %) на виборах за останні 3 роки демонструє молодь, яка проживає у Західному регіоні. Найвищі відсотки відвідування виборчих дільниць молоддю у Івано-Франківській (88,4 %), Львівській (74,7%) та Закарпатській (71,8 %) областях. Більшість опитаних (78,9 %) не бере участі у діяльності громадських організацій. Однак 6 % молоді бере участь у роботі спортивних організацій або організацій, діяльність яких пов'язана із проведенням дозвілля, та 5,7 % молоді є активістами шкільного або студентського самоврядування.

За сучасних умов молодь достатньо високо оцінює свої можливості щодо дотримання звичаїв та традицій свого народу (35,4 %), власних дій відповідно до сумління та переконань (33,9 %), досягнення для себе та своєї сім'ї матеріального благополуччя та добробуту (32,4 %), можливість отримання інформації, важливої для молоді (31,5 %). Водночас молодь незадовільно оцінює свої можливості впливати на прийняття рішень, що стосуються життя свого населеного пункту (41,3 %), можливість отримання судового захисту (40,6 %), свої можливості щодо започаткування власної справи (38,5 %), отримання кваліфікованої медичної допомоги (35,1 %) та хорошої роботи за своєю спеціальністю (33,1 %). Найголовнішими соціальними проблемами, які сьогодні турбують вітчизняну молодь, є стан економіки в країні (63,3 %), загальне падіння рівня життя населення (60 %),



питання працевлаштування (52 %), наявна корупція та некомпетентність влади (50,5 %) та військові дії на Сході України (49,2 %) [12, с. 73, 74, 77, 83].

Із зазначеного можна зробити висновок, що більшу частину молоді, особливо у Західних регіонах країни, турбують проблеми зниження рівня життя в Україні, стан економіки та проблеми корупції і некомпетентності влади, і водночас молодь не вірить у власні можливості покращити ситуацію в країні.

З огляду на зазначене, пріоритетом розвитку держави і суспільства мають бути правове виховання і правова освіта для формування сучасного активного молодого громадянського суспільства, потреба в якому неухильно зростає, адже від позиції молоді в суспільно-політичному житті, її впевненості у завтрашньому дні і активності буде залежати майбутнє України.

Проблема відсутності інтересу у молодих людей до права і закону може бути пов'язана з недостатньою увагою органів правопорядку та інших державних структур до роботи з молоддю [13, с. 49].

В Україні при Міністерстві юстиції, відповідно до положення, затвердженого Постановою Кабінету Міністрів України від 29.05.95 р. № 366, було створено Всеукраїнську міжвідомчу координаційно-методичну раду з правової освіти населення. Основними завданнями Ради визначено:

- розроблення пропозицій щодо координації діяльності органів виконавчої влади, органів місцевого самоврядування, об'єднань громадян, навчальних закладів та закладів культури, наукових установ, видавництв та видавничих організацій, засобів масової інформації у сфері правової освіти населення;

- підготовка пропозицій щодо визначення шляхів, механізмів та способів вирішення проблемних питань правової освіти населення;

- сприяння підвищенню ефективності діяльності органів виконавчої влади, органів місцевого самоврядування, об'єднань громадян, навчальних закладів та закладів культури, наукових установ, видавництв та видавничих організацій, засобів масової інформації та удосконалення нормативно-правових актів з питань правової освіти населення;

- надання методичної допомоги органам виконавчої влади, органам місцевого самоврядування, об'єднанням громадян, навчальним закладам та закладам культури, науковим установам, видавництвам та видавничим організаціям, засобам масової інформації щодо організації заходів, спрямованих на підвищення правосвідомості та правової культури населення;

- розроблення пропозицій (рекомендацій) щодо удосконалення правової навчально-виховної роботи;

- поширення позитивного досвіду з питань правової освіти населення.

Але, складається враження, що рада з 2014 року взагалі не працює. На сайті Міністерства юстиції України останній план зазначеної ради датується 2013 роком [14], хоча склад згаданої ради оновлювався у 2015 році, відповідно до наказу Міністерства юстиції України від 06.07.15 р. № 199/7 [14]. Наразі невідомо, чи працює рада нині.

Оскільки саме молодь є стратегічним ресурсом соціально-економічного розвитку будь-якої держави, правова освіта молоді, виховання поваги до правопорядку і законності є необхідною умовою побудови суверенної і незалежної, демократичної, соціальної, правової держави, якою, відповідно до Конституції, має бути Україна.

Враховуючи викладене, можемо говорити про те, що правова культура молоді в Україні залишається на стадії формування й потребує цілеспрямованої діяльності з її становлення та активного розвитку. Тільки через сукупність всієї системи заходів,

спрямованих на підвищення правової культури, можна сформувати у молодих людей чіткі ціннісні установки, високу ступінь правосвідомості, а отже і почуття відповідальності за кожне прийняте рішення, що в цілому стане гарантом успішного розвитку українського суспільства.

Досвід останніх десятиліть переконливо доводить, що політичних та економічних успіхів досягають саме ті держави, які приділяють посилену увагу розвитку молодого покоління, і країни, що інвестують в молодь як у власне майбутнє.

Відмінною рисою молоді є мобільність, інтелектуальна активність, сприйнятливості до всього цікавого та нового. У наш час активність молоді може бути спрямована як в негативне так і в позитивне русло суспільного життя. У зв'язку з цим, актуальною умовою для формування правових переконань є створення можливості за допомогою первинних і вторинних агентів соціалізації свідомо брати участь в суспільно-політичній діяльності (сім'я, школа, вищі навчальні заклади, держава).

Цілеспрямована політика держави з правового виховання молоді має визначатися в залежності від вікових особливостей, обстановки і оточення, рівня освіти і культурного розвитку. Правове виховання повинно починатися з раннього віку. Школа та інші види навчальних закладів мають стати агітаторами участі молоді в суспільному житті, формувати в учнів почуття гідності та громадянської відповідальності, потреби відстоювати свою точку зору, а також вчити піклуватися не тільки про власне благополуччя, а й про успіх своєї держави.

Суспільні інститути держави, громадськість мають змінити своє ставлення до молодіжної та освітньої політики. Виділяти більше бюджетних коштів на належне виховання молоді, а менше – на політичні обіцянки, що роками не виконуються.

Прикладом позитивного досвіду з правового виховання й профілактики правопорушень серед дітей є запровадження експериментальної моделі співпраці навчальних закладів і поліції відповідно до листа МОН України від 27.05.16 р. № 2/2-14-966-16 “Про апробацію експериментальної моделі співпраці навчальних закладів і поліції “Шкільний офіцер поліції”. Починаючи з 2016 – 2017 н.р. у школах міст України: Івано-Франківську, Львові, Одесі та Києві працюють шкільні офіцери поліції, завданням яких є проведення просвітницько-профілактичних занять, індивідуальних зустрічей з учнями та/або їхніми батьками (особами, які їх замінюють); забезпеченні вчасного та ефективного реагування на виклики керівників навчальних закладів; участі у батьківських зборах і педагогічних радах з метою проведення інформаційно-роз'яснювальної роботи серед батьків та педагогічних працівників щодо попередження негативних явищ в дитячому середовищі. Загалом проект орієнтований на профілактику правопорушень в шкільному середовищі. У задачі поліцейських також входить пояснення учням правил безпечного поведіння в мережі Інтернет, що в сучасних умовах розвитку інформаційних технологій має суттєве значення.

На нашу думку, аналогічну модель “Шкільний офіцер поліції” слід запровадити в усіх школах України.

У зв'язку із суттєвим зростанням кількості звернень українців за правовою допомогою в структурі Міністерства юстиції України відповідно до Указу Президента України від 01.06.12 р. “Про внесення змін та визнання такими, що втратили чинність, деяких указів Президента України” [15] створено Координаційний центр з надання правової допомоги населенню. Серед основних завдань Центру:

- поширення правової, наукової та іншої інформації з питань надання правової допомоги;

- організація і проведення семінарів, конференцій, тренінгів, виставок, інших заходів із забезпечення підвищення професійного рівня працівників регіональних центрів з надання безоплатної вторинної правової допомоги;
- сприяння удосконаленню чинних та впровадженню нових стандартів і процедур у сфері надання безоплатної правової допомоги з урахуванням світової практики;
- забезпечення впровадження сучасних інформаційних технологій у сфері надання безоплатної правової допомоги;
- забезпечення проведення наукових досліджень і прикладних розробок, зокрема підготовки оглядів законодавства України та іноземних держав з питань надання правової допомоги та практики його застосування, словників, довідників, збірок, науково-практичних коментарів, методичних рекомендацій та посібників;
- забезпечення заснування друкованих засобів масової інформації, видання та розповсюдження книг, іншої друкованої продукції, у тому числі на платній основі, виготовлення та розміщення соціальної реклами, виготовлення, тиражування і розповсюдження відео- та аудіопроодукції;
- взаємодія з громадськими організаціями з метою збирання, проведення аналізу, узагальнення, обговорення та використання кращих напрацювань з питань надання безоплатної правової допомоги;
- забезпечення проведення моніторингу діяльності органів виконавчої влади з виконання взятих на себе Україною зобов'язань щодо надання безоплатної правової допомоги.

В Україні створені також регіональні Центри з надання безоплатної вторинної правової допомоги.

За висновками Уряду, потреби громадськості у забезпеченні безоплатної правової допомоги в Україні все ще не задоволені повною мірою [16]. Крім того, значна частина населення, а особливо – його вразливі верстви, має низький рівень правової грамотності, що стимулює виникнення корупційних явищ, стримує активну участь цієї частини громадян в економічному житті, провокує та підтримує бідність.

Окрім того, у результаті тимчасової окупації частини території України Російською Федерацією утворилися нові вразливі групи населення, зокрема внутрішньо переміщені особи, особи, які претендують на отримання статусу учасника антитерористичної операції, що потребують безоплатної вторинної правової допомоги.

На сайті Міністерства освіти і науки України у розділі “Виховна робота та захист прав дитини” на сторінці “Безпека дітей в Інтернеті” розміщена інформація, що стосується захисту дітей від впливу шкідливої інформації. На сторінці розміщено інформацію, призначену педагогам та батькам для навчання дітей безпечному користуванню Інтернетом, пам’ятку для батьків: “Діти. Інтернет. Мобільний зв’язок”, “Як забезпечити безпеку дітей в мережі Інтернет”. На сайті також є посилання на онлайн-ресурси, рекомендовані дітям, спеціалізовані Інтернет-сайти дитячої літератури, освітньо-інформаційні ресурси, сайти бібліотек та електронних бібліотек, музеїв та картинних галерей України тощо [17].

Отже певні кроки влади до покращення ситуації з правової освіти молоді в Україні зроблено.

На наш погляд не менш важливою складовою формування правової культури є самоосвіта. Розвиток інформаційних технологій спрощує процес підвищення рівня правової культури особистості за допомогою пошуку необхідної інформації в Інтернет. Необхідно лише навчитися користуватись інформаційними ресурсами, структурувати великі потоки даних, дотримуючись основних правил безпеки в мережі.

Слід зазначити, що важливою проблемою пошуку необхідної інформації в Інтернет є розпорошеність інформаційних ресурсів, зокрема й тих, що стосуються правової інформації. Пересічному користувачу досить складно віднайти необхідну інформацію й виділити з неї достовірну й актуальну. На проблеми, що пов'язані з обігом та розповсюдженням різноманітної інформації у всесвітній мережі Інтернет та пов'язаної з цим інформаційно-правової культури користувачів звертають увагу вітчизняні й іноземні дослідники, що потребує подальших наукових досліджень.

### **Висновки.**

1. До негативних чинників формування правової культури молоді в Україні слід віднести:

- недосконалість законодавства, його декларативність;
- низький рівень якості роботи правоохоронних органів та посадових осіб, а також рівень правотворчої та правозастосовної діяльності;
- недотримання на практиці принципів “закон – один для всіх” та “невідворотність покарання”;
- стан економіки та проблеми корупції і некомпетентності влади;
- відсутність ефективних правових механізмів протидії порушенням прав і свобод людини у мережах Інтернет та ЗМІ;
- обмеження можливостей судового захисту честі, гідності та приватності громадян;
- недостатність засобів правового виховання молоді з боку державних органів тощо.

2. Широких масштабів в Україні набули явища правового нігілізму, масова неповага до права, зневажливе ставлення до законодавства та правових норм. Часто негативний та деструктивний вплив на правову свідомість молоді в Україні чинять соціальні мережі та засоби масової інформації.

3. В Україні існує проблема відсутності інтересу у молодих людей до права, зневага до закону та суду, розчарування у владі, у справедливості правових інститутів та безнадії щодо майбутнього, зневіри у власних силах змінити ситуацію в країні на краще, що вилилось зокрема у небажання молоді брати участь в політичному та соціальному житті країни. Тільки через сукупність всієї системи заходів, спрямованих на підвищення правової культури, можна сформувати у молодих людей чіткі ціннісні установки, високу ступінь правосвідомості, а отже і почуття відповідальності за кожне прийняте рішення, що в цілому стане гарантом успішного розвитку українського суспільства.

4. Ретельно продумана і ефективна інформаційно-правова політика щодо роботи з молоддю, впровадження у практику принципів верховенства права і закону, принципу “закон – один для всіх” та “невідворотність покарання”, цілеспрямоване правове виховання сприятиме підвищенню рівня правосвідомості молоді. З огляду на це пропонуємо:

- запровадити в Україні проведення соціологічних досліджень для моніторингу стану правової культури молоді;
- зважаючи на розвиток інформаційних технологій, які в подальшому набуватимуть все більш складних форм, що вплине на формування більш складних суспільних відносин, доцільно ввести до програми шкільної освіти в рамках вивчення права, дисципліни “Основи інформаційного права і безпеки”;
- запровадити у кожній школі України програму “Шкільний офіцер поліції” для профілактики правопорушень серед дітей та пропаганди правомірного способу життя.

- в рамках діяльності Всеукраїнської міжвідомчої координаційно-методичної ради з правової освіти населення вживати заходів щодо надання методичної допомоги органам виконавчої влади, органам місцевого самоврядування, об'єднанням громадян, навчальним закладам та закладам культури, науковим установам, видавництвам та видавничим організаціям, засобам масової інформації щодо організації заходів, спрямованих на підвищення правосвідомості та правової культури населення.

### Використана література

1. Національна програма правової освіти населення: Указ Президента України від 18.10.01 р. № 992/2001.
2. Дзьобань О.П. До питання про місце правового виховання в сучасному українському суспільстві. *Правова культура і громадянське суспільство в Україні: стан і перспективи розвитку* : матер. міжнар. наук. конф., м. Харків, 12 жовт. 2007 р. Харків: Право, 2007. С. 66-68; Коваленко Н.Ю. Форми правового виховання студентів. *Держава і право. Юрид. і політ. науки*. Київ: Ін-т держави і права НАН України, 2005. Вип. 28. С. 56-63; Ковальський В. Мета правового виховання. *Юрид. вісн. України*. 2005. № 14. С. 3; Кутиркін А. Шляхи розвитку теорії та практики правового виховання населення України. *Право України*. 2008. № 3. С. 122-125; Ладиченко В. Правове виховання суспільства. *Юрид. вісн. України*. 2007. № 22. С. 12; Орлова О.О. Механізм правового виховання. *Вісн. Луганськ. держ. ун-ту внутр. справ*. Луганськ: ЛДУВС, 2005. Вип. 4. С. 57-65; Штангрет М.Й. Філософські проблеми правового виховання молоді (на прикладі закладів освіти МВС України): автореф. дис. ...канд. юрид. наук: 12.00.12. Львів: ЛДУВС, 2007. 20 с.
3. Скуратівський В.А., Палій О.М. Основи соціальної політики. Київ: МАУП, 2002. 200 с.
4. Субботін В.М., Філонов О.В., Тодоров І.Я. Теорія держави і права: підручник. Київ: Знання, 2005. 327 с.
5. Рябко И.Ф. Основы правовой педагогики. Ростов н/Д: Изд-во Ростов. ун-та, 1973. С. 35.
6. Третяк С. Правове забезпечення правової культури населення як умова створення основ громадянського суспільства. *Право України*. 2005. № 4. С. 26-28.
7. Ганзенко О.О. Правова культура особи в умовах розбудови правової держави Україна. *Вісник Запорізького юридичного інституту*. 1999. № 2. С. 279-284.
8. Фурашев В.М. Права людини: основні загрози їх забезпечення в Україні: матеріали наук.-практ. конф. *Проблеми захисту прав людини в інформаційному суспільстві*. м. Київ, 1 квітня 2016 р. / упорядн.: В.М. Фурашев, С.Ю. Петряєв. Київ: НДІП НАПрН України, Національний інститут стратегічних досліджень, Секретаріат Уповноваженого Верховної Ради України з прав людини, НТУУ "КПІ". Київ: Вид-во "Політехніка", 2016. 150 с. С. 18-21.
9. Дмитрієнко І. Проблеми та перспективи історичного осмислення української правової культури. *Держава і право. Юридичні і політичні науки*: зб. наукових праць. Вип. 38. Київ: Ін-т держави і права ім. В. Корецького НАН України, 2007. 776 с.
10. Попадинець Г. Правова культура як важливий елемент правової системи України. URL: <http://science.lpnu.ua/sites/default/files/journal-paper/2017/may/2077/vnulpurn201478225.pdf>
11. Пилипчук В.Г. Актуальні питання захисту прав, свобод і безпеки людини в сучасному інформаційному суспільстві: матеріали наук.-практ. конф. *Проблеми захисту прав людини в інформаційному суспільстві*. Київ, 1 квітня 2016 р. / упорядн.: В.М. Фурашев, С.Ю. Петряєв. Київ: НДІП НАПрН України, Національний інститут стратегічних досліджень, Секретаріат Уповноваженого Верховної Ради України з прав людини, НТУУ "КПІ". Київ: Вид-во "Політехніка", 2016. 150 с. С. 6-8.
12. Цінності Української молоді: результати репрезентативного соціологічного дослідження становища молоді. – (Дослідження Центру незалежних соціологічних досліджень "ОМЕГА" на замовлення Міністерства молоді та спорту України; автори: Наталія Дмитрук, Ганна Падалка, Сергій Кіреєв, Ірина Мостова, Олена Бікла, Владислав Шелепа). Київ, 2016. С. 73-74, 77, 83.

13. Педько Ю.С. Становлення адміністративної юстиції в Україні. Київ, 2003. С. 5
14. План роботи Всеукраїнської міжвідомчої координаційно-методичної ради з правової освіти населення на 2013 рік. – (Сайт Міністерства юстиції України). URL: [https://minjust.gov.ua/m/str\\_43463](https://minjust.gov.ua/m/str_43463)
15. Про Координаційний центр. URL: <https://www.legalaid.gov.ua/ua/pro-tsentr>
16. Про Стратегію реформування судоустрою, судочинства та суміжних правових інститутів на 2015 – 2020 роки: Указ Президента України. URL: <https://zakon.rada.gov.ua/laws/show/276/2015>; Про безоплатну правову допомогу: Закон України URL: <https://zakon.rada.gov.ua/laws/show/3460-17>; Забезпечення рівного доступу до правосуддя та правової допомоги. URL: <https://www.kmu.gov.ua/ua/diyalnist/reformi/verhovenstvo-prava-ta-borotba-z-korupciyeyu/zabezpechennya-rivnogo-dostupu-do-pravosuddya-ta-pravovoyi-dopomogi>; Середньостроковий план пріоритетних дій Уряду до 2020 року: Розпорядження Кабінету Міністрів України від 03.04.17 р. № 275-р.; Про сприяння розвитку громадянського суспільства в Україні: Указ Президента України. URL: <https://zakon.rada.gov.ua/laws/show/68/2016>
17. Безпека дітей в Інтернеті. – (Офіційний сайт Міністерства освіти і науки України). URL: <https://mon.gov.ua/ua/osvita/pozashkilna-osvita/vihovna-robota-ta-zahist-prav-ditini/bezpeka-dit-ej-v-interneti>

~~~~~ \* \* \* ~~~~~

УДК 342.1

**БЕЛЄВЦЕВА В.В.**, доктор юридичних наук, старший науковий співробітник,  
завідувач наукової лабораторії права міжнародної безпеки  
та протидії злочинам проти миру і безпеки людства  
НДІ інформатики і права НАПрН України

## **МІГРАЦІЙНИЙ РЕЖИМ ПЕРЕБУВАННЯ ІНОЗЕМНИХ ГРОМАДЯН І ОСІБ БЕЗ ГРОМАДЯНСТВА НА ТЕРИТОРІЇ УКРАЇНИ: СТАН І ПЕРСПЕКТИВИ**

**Анотація.** У статті на основі аналізу поняття, змісту і сутності міграційного режиму перебування іноземних громадян і осіб без громадянства на території України і його основних елементів доводиться необхідність розробки і ухвалення закону “Про міграційну політику України”.

**Ключові слова:** міграційне право, міграційний режим, іноземний громадянин, міграційний процес, державне регулювання, міграційна політика.

**Summary.** The article proves the necessity of development and passing an act the migratory policy of Ukraine based on analysis of concept, content and essence of the migratory mode of stay of foreign citizens and persons without citizenship on territory of Ukraine and its basic elements.

**Keywords:** migratory right, migratory regime, foreign citizen, migratory process, government control, migratory policy.

**Аннотация.** В статье на основе анализа понятия, содержания и природы миграционного режима пребывания иностранных граждан и лиц без гражданства на территории Украины и его основных элементов обосновывается необходимость разработки и принятия закона “О миграционной политике Украины”.

**Ключевые слова:** миграционное право, миграционный режим, иностранный гражданин, миграционный процесс, государственное регулирование, миграционная политика.

**Постановка проблеми.** Проголошені Президентом України у Стратегії міграційної політики України на період до 2025 року цілі щодо сприяння легальній міграції в Україну, узгодженій із соціальною політикою та економічним розвитком держави та забезпечення успішної інтеграції іноземців та осіб без громадянства, які перебувають в Україні на законних підставах, в українське суспільство; забезпечення іноземцям та особам без громадянства, які звернулися до відповідного органу міграційної служби із заявою про визнання біженцем або особою, яка потребує додаткового захисту, можливість розгляду їх заяв про визнання біженцем або особою, яка потребує додаткового захисту, за допомогою ефективної і справедливої процедури [1], спонукало до необхідності дослідження такої важливої форми державного регулювання міграційних відносин, як міграційний режим перебування іноземних громадян і осіб без громадянства на території України. Його вивчення проводилося і проводиться традиційно в рамках адміністративного права.

**Мета статті** є визначення сутності, виокремлення правових основ функціонування міграційного режиму перебування іноземних громадян і осіб без громадянства на території України, його складових та окремих питань оновлення законодавства з питань міграції та протидії загрозам у даній сфері.

**Виклад основного матеріалу.** Сутність міграційного режиму перебування іноземних громадян і осіб без громадянства на території України полягає в державному

регулюванні міграційних процесів в Україні сукупністю правових засобів, що використовуються для закріплення соціально-правового стану об'єктів впливу і спрямовані на забезпечення їх стійкого функціонування.

У числі перспективних складових міграційного режиму перебування іноземних громадян і осіб без громадянства в Україні пропонуємо розглядати наступні:

- правовий режим “транснаціональних коридорів” і транзитного проїзду іноземних громадян через територію України;
- правовий режим співвітчизників, що добровільно переселяються з-за кордону, та інших іноземних громадян, які тимчасово проживають на території України;
- правовий режим прикордонних територій.

Розглядаючи правовий режим “транснаціональних коридорів” і транзитного проїзду іноземних громадян через територію України, можна відзначити, що на даний час в Україні правовий акцент зроблено на систему обмежень і відповідальності за недотримання транзитного проїзду. У той же час режим – це й забезпечення з боку держави прав і свобод іноземних громадян, які вони мають відповідно до міжнародних стандартів і Конституції України, законно знаходячись (при транзитному проїзді) на її території.

До таких прав можна віднести, перш за все, право на користування рідною мовою, на вільний вибір мови спілкування, право мати майно у власності, володіти, користуватися і розпоряджатися ним як одоноособово, так і спільно з іншими особами, право на охорону здоров'я і медичну допомогу та низку інших особистих і соціально-економічних прав і свобод людини.

Правове регулювання так званих “транснаціональних коридорів” повинне здійснюватися на багатобічній основі у межах міждержавних договорів і угод, а також шляхом подальшого законодавчого встановлення правового режиму транзитного проїзду іноземних громадян і осіб без громадянства через територію України.

Ще одним перспективним напрямом міграційного режиму є правовий режим співвітчизників, які добровільно переселяються (повертаються) з-за кордону, та інших іноземних громадян, які тимчасово проживають в Україні.

На сучасному етапі розвитку української держави необхідно розробити та закріпити на законодавчому рівні принципи та цілі державної політики України стосовно співвітчизників за кордоном. На цей час має місце низка наступних проблем у цій сфері, а саме:

- недосконалість нормативно-правової бази та інституційного забезпечення співпраці із українцями за кордоном;
- недостатнє задоволення мовно-культурних та освітніх потреб світового українства, з метою збереження національної ідентичності;
- трудова міграція, та проблеми, пов'язані із поверненням та облаштуванням трудових мігрантів в Україні;
- комплекс питань, пов'язаних зі збереженням національної ідентичності українців за кордоном.

За результатами “круглого столу” “Українська держава та світове українство: актуальні питання, потенціал та перспективи взаємодії”, який відбувся в Національному інституті стратегічних досліджень 21 лютого 2013 року, стисло подані рекомендації учасників “круглого столу” щодо вирішення основних завдань державної політики у сфері забезпечення національної ідентичності закордонних українців. Зокрема, зміцнити інституційні основи та вдосконалити стратегічне планування роботи з діаспорою; здійснити комплекс заходів, що були б спрямовані на підтримку та розвиток освіти в українському зарубіжжі; здійснити заходи, спрямовані на збереження історико-культурної спадщини



України за кордоном; активізувати роботу із забезпечення соціальної захищеності українських працівників за кордоном, сприяння зворотності міграцій, стимулювання інвестування зароблених мігрантами коштів в економіку України [2].

Державна програма повинна сприяти соціально-економічному розвитку української держави, що неможливе без кардинальної зміни демографічній ситуації, яка характеризується на цей час відтоком населення із стратегічно важливих територій, скороченням загальної чисельності населення, у тому числі працездатного віку.

Сприяння добровільному переселенню в Україну співвітчизників, що проживають за кордоном, є одним з напрямів вирішення демографічної проблеми.

Особливої уваги потребує розгляд правового режиму прикордонних територій. На цей час Україна на суходолі межує з сімома країнами. Південний кордон України проходить зовнішньою межею українських територіальних вод. По морю Україна межує з Румунією і Росією.

Отже, Закон України “Про державний кордон України” вводить три принципово важливих поняття: режим державного кордону, прикордонна смуга та прикордонний режим.

Згідно п. 18 ст. 92 Конституції України виключно Законами України визначається режим державного кордону [3]. Так, відповідно до ст. 8 Закону України “Про державний кордон України” режим державного кордону України – порядок перетинання державного кордону України, плавання і перебування українських та іноземних невійськових суден і військових кораблів у територіальному морі та внутрішніх водах України, заходження іноземних невійськових суден і військових кораблів у внутрішні води і порти України та перебування в них, утримання державного кордону України, провадження різних робіт, промислової та іншої діяльності на державному кордоні України – визначається цим Законом, іншими актами законодавства України і міжнародними договорами України [4].

Натомість, розділ III наведеного Закону регулює прикордонний режим. Так, ст. 22 вказує, що з метою забезпечення на державному кордоні України належного порядку Кабінетом Міністрів України встановлюється прикордонна смуга, а також можуть установлюватися контрольовані прикордонні райони. Прикордонна смуга встановлюється безпосередньо вздовж державного кордону України на його сухопутних ділянках або вздовж берегів прикордонних річок, озер та інших водойм з урахуванням особливостей місцевості та умов, що визначаються Кабінетом Міністрів України. До прикордонної смуги не включаються населені пункти і місця масового відпочинку населення. Контрольовані прикордонні райони встановлюються, як правило, в межах території району, міста, селища, сільради, прилеглої до державного кордону України або до узбережжя моря, що охороняється органами Державної прикордонної служби України. До контрольованого прикордонного району включаються також територіальне море України, внутрішні води України і частина вод прикордонних річок, озер та інших водойм України і розташовані в цих водах острови [4].

Стаття 23 наведеного Закону регулює прикордонний режим. Так, у прикордонній смузі та контрольованому прикордонному районі в порядку, що визначається Кабінетом Міністрів України, встановлюється прикордонний режим, який регламентує відповідно до цього Закону та інших актів законодавства України правила в'їзду, перебування, проживання, пересування громадян України та інших осіб, провадження робіт, обліку та тримання на пристанях, причалах і в пунктах базування самохідних та несамохідних суден, їх плавання та пересування у внутрішніх водах України. Передбачений частиною першою цієї статті порядок обліку і тримання самохідних та несамохідних суден на пристанях, причалах і в пунктах базування, їх плавання і пересування в територіальному

морі і внутрішніх водах України поширюється і на територію району, міста, селища, сільради, що прилягає до державного кордону України або до узбережжя моря, яке охороняється органами Державної прикордонної служби України, де прикордонну смугу та контрольований прикордонний район не встановлено. Забороняється тримати самохідні та несамохідні судна поза встановленими пристанями, причалами і пунктами базування або на них, але з порушенням правил тримання, а також відходити від берега або причалювати до берега поза пристанями, причалами і пунктами базування [4].

Відповідно до ст. 24 вказаного Закону дозвіл на в'їзд, перебування, проживання, провадження робіт і пропуск у прикордонну смугу дає і здійснює Державна прикордонна служба України. У необхідних випадках Державна прикордонна служба України може запроваджувати додаткові тимчасові режимні обмеження на в'їзд і провадження робіт у прикордонній смузі [4].

Стаття 25 регулює особливості прикордонного режиму в частині внутрішніх вод України. Так, частина внутрішніх вод України і розташовані в ній острови перебувають під контролем органів Державної прикордонної служби України. Пересування по берегу і льоду прикордонних річок, озер та інших водойм поза встановленими для цього шляхами, стежками або з порушенням правил пересування забороняється [4].

У ст. 26. зазначається, що режим у пунктах пропуску через державний кордон України – порядок перебування і пересування всіх осіб і транспортних засобів у межах території прикордонних залізничних і автомобільних станцій, морських і річкових портів, аеропортів і аеродромів, відкритих для міжнародного сполучення, а також здійснення іншої діяльності, пов'язаної з пропуском через державний кордон України осіб, транспортних засобів, вантажів, – визначається згідно з законодавством України Державною прикордонною службою України разом з компетентними органами. У приміщеннях і місцях, де здійснюється прикордонний контроль, Державна прикордонна служба України встановлює додаткові режимні правила, що регламентують порядок допуску в них осіб, які беруть участь у контролі та обслуговуванні пасажирів і транспортних засобів закордонного прямування, відправленні з пунктів пропуску транспортних засобів, що вибувають за кордон і прибувають в Україну, а також інші обмеження для запобігання незаконному перетинанню державного кордону України [4].

Правове регулювання міграції населення на прикордонних територіях України на цей період набуває особливо важливого і актуального значення. Воно повною мірою обумовлене загрозами національній безпеці українській державі, які несуть в собі переміщення населення із зарубіжних країн, у тому числі нелегальне, на територію України.

Аналізуючи вказаний правовий режим, необхідно відзначити, що регулювання міграції досить часто виходить за межі окремих держав, набуває міжнародного значення, вимагаючи формування регулюючих механізмів не лише на національному, але і на міжнародному рівні. Включаючись у цей процес, держави повинні вирішувати такі основні завдання, як запобігання можливим конфліктам, що зароджуються на основі посилення міграційних процесів; захист національних інтересів за допомогою обмежувальних заходів у рамках чинного законодавства; створення механізмів інтеграції і адаптації мігрантів у приймаюче соціальне середовище тощо.

### **Висновки.**

Проведене дослідження вказує на зростання в останній час значення правової складової міграційного режиму. Об'єднуючим чинником міграційного режиму перебування (мешкання) іноземних громадян і осіб без громадянства на території України є його конституційно-правова складова. У зв'язку з цим необхідні розробка та

ухвалення Закону України “Про державну міграційну політику в Україні”. Такий Закон повинен визначати основні поняття у сфері міграції, цілі, принципи, основні напрями і коло суб’єктів державної міграційної політики, механізм її розробки і реалізації з метою створення правових, соціально-економічних і організаційних умов.

Серед основних причин необхідності ухвалення Закону України “Про державну міграційну політику в Україні” можна відзначити наступні: депопуляція в Україні; необхідність забезпечення державної безпеки і громадського порядку, захисту національних інтересів Української держави.

У цій ситуації необхідно встановити розмежування повноважень у сфері міграції. Зокрема, перспективним напрямом у зв’язку з цим є правове регулювання статусу прикордонної зони і критеріїв обмеження прав в цих зонах як громадян України, так й іноземних громадян та осіб без громадянства.

### **Використана література**

1. Стратегія міграційної політики України на період до 2025 року: Закон України від 12.07.17 р. URL: <https://zakon.rada.gov.ua/laws/show/482-2017-%D1%80>
2. URL: <http://www.niss.gov.ua/articles/1116>
3. Конституція України: Закон України від 28.06.96 р.; із змінами URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>
4. Про державний кордон України: Закон України від 4.11.91 р. № 1777-XII; із змінами. URL: <https://zakon.rada.gov.ua/laws/show/1777-12>

~~~~~ \* \* \* ~~~~~

УДК 342.951:351.82

**ДЕНИСОВ А.І.**, кандидат юридичних наук, доцент кафедри правового забезпечення господарської діяльності факультету № 6 Харківського національного університету внутрішніх справ

## ПЕРСПЕКТИВИ СТВОРЕННЯ СПЕЦІАЛЬНИХ ПРАВОВИХ РЕЖИМІВ ДЛЯ ТРУДОВИХ МІГРАНТІВ

**Анотація.** У статті досліджуються перспективи створення спеціальних правових режимів для окремих категорій трудових мігрантів з метою підвищення рівня міграційної безпеки України. Запропоновані окремі новації до вітчизняного законодавства, враховуючи світовий досвід у сфері створення окремих міграційних режимів для певних категорій осіб.

**Ключові слова:** міграційна безпека, засоби забезпечення, спеціальні правові режими.

**Summary.** The article examines perspectives of creating special legal regimes for certain categories of migrant workers with the aim of increasing the level of migration security in Ukraine. Some innovations to domestic legislation are proposed, according to world experience in the sphere of creating separate migration regimes for certain groups of people.

**Keywords:** migration security, means of security, special legal regimes.

**Аннотация.** В статье исследуются перспективы создания специальных правовых режимов для отдельных категорий трудовых мигрантов с целью повышения уровня миграционной безопасности Украины. Предложены отдельные новации в отечественное законодательство, с учетом мирового опыта в сфере создания отдельных миграционных режимов для определенных групп лиц.

**Ключевые слова:** миграционная безопасность, средства обеспечения, специальные правовые режимы.

**Постановка проблеми.** Сьогодні трудова міграція є можливо найбільш поширеним видом міграційних процесів у світі. Більшість держав йдуть шляхом створення розгалуженої складної системи спеціальних правових режимів для окремих категорій трудових мігрантів з метою забезпечення міграційної безпеки та запровадження ефективно діючої міграційної політики. Слід констатувати, що у разі вступу до ЄС та підвищення економічного добробуту в державі, проблема трудової міграції до нашої країни буде тільки зростати. Також важливим для аналізу є той факт, що трудова міграція може ставати засобом для інтервенції з інших країн (наприклад, використовуватись як зброя під час ведення гібридної війни). Тому необхідним вбачається розробка нашою державою ефективно діючої системи спеціальних правових режимів для окремих категорій трудових мігрантів.

**Результати аналізу наукових публікацій,** зокрема, свідчать, що наразі більшість країн світу активно створюють нові спеціальні правові режими для окремих категорій трудових мігрантів з метою підвищення ефективності власної міграційної політики, залучення висококваліфікованих спеціалістів тощо. Водночас в Україні можна констатувати майже повну відсутність нормативного закріплення положень щодо таких спеціальних режимів. Більшість публікацій українських науковців у сфері трудової міграції стосується еміграції, водночас вивчення проблематики іміграції в Україну наразі вбачається недостатнім.

**Мета статті** є визначення умов створення нових спеціальних нормативних режимів для окремих категорій трудових мігрантів та реформувати систему міграційної безпеки в цілому.

**Виклад основного матеріалу.** Слід констатувати існування на цей час світової тенденції створення складних систем спеціальних правових режимів для мігрантів. Так, більшість розвинених країн світу прийняли розгалуженні критерії для прийому, проживання та інтеграції різних категорій мігрантів. Водночас в нашій країні фактично відсутня аналогічна система, оскільки законодавчо майже не існує виокремлення окремих правових режимів для різних категорій мігрантів.

Трудова міграція наразі виступає найпоширенішим видом міграції у світі. Так, у 2013 році, з приблизно 244 мільйонів осіб, що офіційно мігрували в інші країни, частка легальних трудових мігрантів та їх сімей складала близько 150 мільйонів осіб [8, с. 113].

Важливим для виокремлення спеціальних правових режимів є безперечно чіткість критеріїв. Так, Anna Bouchery та Justin Gestz зазначають, що значна кількість класифікацій міграційних режимів не надають точних “індикаторів” таких режимів [10, с. 8-9]. І дійсно, створення нечітких критеріїв для визначення спеціальних правових міграційних режимів призведе до необхідності застосовувати оціночні критерії, створить складності у процесі віднесення до певної категорії окремих трудових мігрантів, призведе до потенційного підвищення корумпованості у Державній міграційній службі України. Тому слід наголосити на необхідності використовувати під час визначення окремих спеціальних правових режимів для трудових мігрантів виключно точних критеріїв (вік, кваліфікація працівника, країна походження тощо).

У країнах Перської затоки Riyasiri Wickramasekara виокремлює окремі спеціальні міграційні режими для тимчасових працівників-мігрантів. Так, лише висококваліфіковані працівники-мігранти мають право на проживання разом із родинами (хоча й існують спеціальні квоти), а водночас для робітників середньої та низької кваліфікації встановлено окремий правовий режим і вони не мають відповідного права [13, с. 4].

Тобто можна вести мову про створення спеціальних правових режимів для трудових мігрантів та їх сімей в залежності від їх кваліфікації. Цікавим є питання щодо можливості запровадження аналогічних правових режимів в нашій країні. З одного боку, таке розшарування може бути трактовано як певна дискримінація, оскільки некваліфіковані працівники втрачають право на сімейне возз'єднання. Однак з іншого боку встановлення спеціального правового режиму для висококваліфікованих працівників може бути окремим правовим засобом стимулювання міграції висококваліфікованої робочої сили. Крім того, можливим є використання не цієї моделі, а, наприклад, австралійської, де стимулюється міграція не просто висококваліфікованих працівників, а фахівців за окремими спеціальностями, яких потребує економіка країни.

Крім того, слід зазначити, що застосування такого підходу створить ще один спеціальний правовий режим для родин працівників мігрантів, що матимуть особливий правовий статус. Це потребуватиме створення окремої процедури отримання дозволу на в'їзд в країну для таких сімей.

Окрім спрощеної процедури отримання дозволу на міграцію членами родин можливим є застосування інших стимулюючих заходів. Наприклад, спрощена процедура отримання дозволу на трудову міграцію, спрощена процедура подальшого отримання громадянства тощо.

Безперечно важливим є швидке створення стимулюючого правового режиму для висококваліфікованих мігрантів. Так, досліджуючи міграційні процеси у Німеччині,

Frank Wolff дійшов висновку, що так звані “Зелені карти” для висококваліфікованих працівників мігрантів робили спроби запровадити ще на початку 2000-х років, однак через політичні суперечки опозиція не дозволила цього. При цьому нестача висококваліфікованої робочої сили продовжувала лише зростати. У 2012 році вже колишня опозиційна Консервативна партія сформувала уряд і прийняла рішення щодо запровадження так званих “Блакитних карток”, що фактично також були покликані збільшити трудову міграцію висококваліфікованих спеціалістів до країни. Однак ситуація вже змінилася і було подано заявки лише на декілька сотень “Блакитних карток”. При цьому більшість заявок була подана від вже працюючих у Німеччині мігрантів, що бажали поновити свій статус [14, с. 2]. Тому можна дійти висновку, що зволікання у запровадженні ефективного спеціального правового режиму для висококваліфікованих мігрантів може бути фатальним для економіки держави.

Особливо важливим це є враховуючи загальну тенденцію до скорочення притоку мігрантів в Україну й збільшення еміграції з нашої держави, що значно підвищився з часів початку Російської агресії у 2015 році і хоча наразі зменшується, однак зберігається міграційне скорочення населення [1, с. 80]. Тому вкрай важливим вбачається стимулювання трудової міграції у зв’язку із негативною міграційною тенденцією наразі та вивільненням робочих місць.

Можливим є також використання іншого австралійського досвіду – застосування вікових обмежень у сфері міграції для окремих правових режимів. Так, в Австралії максимальний вік заявника на професійну візу становить 49 років, а у разі перевищення відповідного віку, заявнику автоматично відмовляють [3, с. 263]. Повністю копіювати подібний досвід вбачається недоцільним, оскільки існують спеціальності, де вік працівника не має критичного значення (науковці, економісти тощо). Однак можливим є встановлення спеціальних вікових обмежень щодо окремих категорій трудових мігрантів (в основному – низькокваліфікованих працівників та працівників, що працюють у сферах, які вимагають значних фізичних навантажень).

У такому разі необхідно розробити методику визначення граничного міграційного віку для окремих спеціальностей, щоб уникнути дискримінації за віковою ознакою.

Щодо загального граничного міграційного віку для всіх категорій працівників, то можливим є порівняння його до загального пенсійного віку в Україні.

Крім того, з метою покращення демографічної ситуації та залучення молоді у нашу країну, можливим є створення також окремого стимулюючого правового режиму для мігрантів певного віку (наприклад, до 30 років).

Також можливим є створення окремих правових режимів для мігрантів з різних країн. Так, у Іспанії, фактично існує два правових режими – один для мігрантів-працівників з країн-членів ЄС, а інший для всіх інших країн. При цьому, трудову міграцію з країн-нечленів ЄС з початком фінансової кризи було майже припинено [11, с. 11].

Враховуючи перспективи євроінтеграції України та проголошений з ЄС безвізовий режим, наша держава також може, залучаючи європейський досвід, розробити два окремі спеціальні правові режими для трудових мігрантів з країн-членів ЄС та інших країн. Більше того, враховуючи наше прагнення до входу до Єврозони, у разі входження України у склад ЄС ми будемо змушені привести вітчизняне законодавство у відповідність до норм Європейського права, зокрема гарантуючи вільне працевлаштування мешканців інших країн ЄС в нашій державі. Тому створення спеціального правового режиму для трудових мігрантів з Європейського Союзу є нагальною проблемою.

При цьому важливим є той факт, що для процесу визначення статусу трудових мігрантів з країн-членів ЄС необхідно не тільки розробити та прийняти відповідні

нормативно-правові документи, а й вести діалог з керівництвом ЄС та окремих країн щодо спільного вирішення проблемних питань трудової міграції. Це підтверджується й положеннями, що містяться у ст. 16 Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, де зазначено, що Україна та країни, що підписали цю Угоду, підтверджують важливість спільного управління міграційними потоками між їхніми територіями та надалі розвиватимуть всеохоплюючий діалог щодо всіх питань у сфері міграції [9].

Також можливим є створення окремого рестриктивного правового режиму для трудових мігрантів з недружніх країн з метою обмеження такої міграції з метою зменшення економічної інтервенції або підсилення заходів безпеки щодо цієї категорії мігрантів. Особливо актуальним це є, враховуючи конфлікт на Донбасі та агресивні дії з боку Російської Федерації. Слід зазначити, що досвід створення подібних рестриктивних режимів вже мають Балтійські країни. Так, у Латвії ще в 2014 році було введено цілий ряд обмежень для мігрантів з Російської Федерації (зокрема, було припинено видачу дозволів на тимчасове проживання та введено цілий ряд обмежень щодо придбання нерухомості для росіян) [12, с. 195].

Враховуючи специфіку трудової міграції, особливості такого рестриктивного режиму можуть полягати у наступному:

1. Введення квот щодо кількості трудових мігрантів.
2. Ускладнення процедури отримання дозволу на роботу. Зокрема, можливим є введення додаткової перевірки благонадійності потенційних трудових мігрантів.
3. Створення спеціального режиму перебування для трудових мігрантів. Це може полягати у забороні покидати певні зони роботи та проживання, нагляд за мігрантами Державної міграційної служби, заборона працювати на окремих видах робіт, чи на окремих територіях (наприклад, на територіях, що межують з державним кордоном) тощо.
4. Повна заборона трудової міграції.

Слід зазначити, що величезною прогалиною є відсутність спеціального нормативно-правового акту, що регулював би відносини з трудової міграції іноземних працівників з-за кордону (дані відносини регулюються лише нормами Закону України “Про зайнятість населення”, водночас спеціальний закон відсутній). Саме у такому акті мають визначатися спеціальні правові режими для окремих категорій трудових мігрантів. Окремі норми щодо трудової міграції містяться у Законі України “Про зовнішню трудову міграцію”. Однак цей Закон регулює відносини, пов’язані лише з трудовою міграцією та соціальним захистом громадян України за кордоном (трудовах мігрантів) і членів їхніх сімей [6]. Завдяки цьому нормативно-правовому акту можливо виокремити ще один спеціальний правовий режим для трудових мігрантів – режим для зовнішніх трудових емігрантів. Він суттєво відрізняється від інших спеціальних правових режимів у сфері трудової міграції, оскільки суб’єктами є виключно громадяни України.

Так, для цього правового режиму, звісно, не може встановлюватись порядок отримання дозволу на в’їзд у країну, отримання подальшого дозволу на роботу чи інших обмежень. Тому виокремлення спеціальних правових режимів для зовнішніх мігрантів вбачається недоцільним.

Окремо можна вести мову про створення окремих спеціальних правових міграційних режимів в залежності від часу перебування працівника на території України. Так, можливо створити окремі режими для сезонних робітників,

короткострокових працівників (до 1 року), довгострокових працівників (більше 1 року) тощо. Звісно, що більший строк перебування працівника в державі, то більші гарантії мають йому надаватися. Також важливою є програма інтеграції довгострокових працівників у суспільство. Наразі світового досвіду щодо програм інтеграції саме тимчасових мігрантів-працівників майже не існує. Водночас можливим є запровадження таких програм у нашій державі для висококваліфікованих працівників та працівників зі спеціальностей, яких потребує вітчизняна економіка, з метою стимулювання їх до залишення у межах країни та подальшого отримання громадянства.

Виходячи з вищезазначеного, пропонується утворити та законодавчо забезпечити спеціальний правовий режим у сфері трудової міграції – стимулюючий режим для окремих категорій висококваліфікованих працівників.

Мінусом вітчизняної системи забезпечення трудової міграції є також майже повна відсутність у Державної міграційної служби України повноважень у сфері контролю трудової міграції, хоча це є найбільш масовим видом переміщень населення. Натомість значна частина повноважень з регулювання відносин, пов'язаних з трудовою міграцією, покладена на Державну службу зайнятості [2, с. 9].

Водночас, на наш погляд, саме на Державну міграційну службу має бути покладено переважну частину повноважень у сфері регулювання відносин пов'язаних з трудовою міграцією в Україні. Це буде повністю кореспондуватися з нормами Положення “Про Державну міграційну службу України”, відповідно до п. 1 якого Державна міграційна служба реалізує державну політику у сферах міграції (імміграції та еміграції), у тому числі протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших визначених законодавством категорій мігрантів [5].

Саме Державна міграційна служба має подавати до Верховної ради України проекти нормативних документів, де будуть встановлюватись спеціальні правові режими для окремих категорій трудових мігрантів та в подальшому здійснювати діяльність з виконання таких актів.

На жаль, прийнята у 2017 році Стратегія державної міграційної політики України на період до 2025 року не містить положень щодо створення спеціальних правових режимів щодо окремих категорій мігрантів. Більше того, сама Стратегія спрямована на зменшення негативних наслідків від еміграції українського населення за кордон. Однак Стратегія майже не звертає уваги на проблему залучення трудових мігрантів з інших країн.

Однак у Стратегії міститься положення щодо необхідності поступової систематизації національного імміграційного законодавства в рамках формування Міграційного кодексу України, яким будуть врегульовуватися всі питання міграції [7].

Вбачається доцільним основні норми, що регулюватимуть відносини, пов'язані з існуванням спеціальних правових режимів у сфері трудової міграції, викласти саме у такому Міграційному кодексі України.

На жаль, наразі процес прийняття Міграційного кодексу України перебуває ще на своєму початку. Так, на сайті Державної міграційної служби України міститься проект Концепції міграційного кодексу України. Однак у зазначеному проекті Концепції на даному етапі відсутні прямі пропозиції щодо вдосконалення нормативного забезпечення у сфері трудової міграції. Самий же проект Концепції носить виключно декларативний характер і не містить жодної практичної пропозиції щодо прийняття будь-якої спеціальної норми [4]. Тому вкрай важливим є продовження активної роботи



з підготовки та прийняття Міграційного кодексу України, що має систематизувати норми, що регулювали б відносини у сфері міграції.

### **Висновки.**

Необхідним є створення системи спеціальних нормативн-правових режимів для трудових мігрантів в Україні.

Для цього необхідним є модернізація чинного законодавства у сфері міграції.

Пропонується розглянути можливість створення відповідних режимів для працівників-мігрантів в залежності від їх віку, кваліфікації, країни походження, строку перебування в Україні та місця міграції.

Також необхідним вбачається створення рестриктивного режиму для трудових мігрантів з країн, що становлять загрозу для національної безпеки та стимулюючого режиму для окремих категорій висококваліфікованих працівників.

### **Використана література**

1. Ковальська Л., Гук Р. Міграційні процеси в Україні в період агресії Російської Федерації. International Scientific and Practical Conference World science 1 (1), 78-82. URL: <http://archive.ws-conference.com/migracijni-procesi-v-ukra%D1%97ni-v-period-agresi%D1%97-rosijsko%D1%97-federa ci%D1%97>

2. Малиновська О. Міграційна політика в Україні: формування, зміст, відповідність сучасним вимогам. – (Інститут економічних досліджень та політичних консультацій. 2014). URL: [http://www.ier.com.ua/files/publications/Policy\\_Briefing\\_Series/PB\\_01\\_migration\\_2013\\_ukr.pdf](http://www.ier.com.ua/files/publications/Policy_Briefing_Series/PB_01_migration_2013_ukr.pdf).

3. Міграційне право України: підручник / С.М. Гусаров, А.Т. Комзюк. О.Ю. Салманова та ін. / за заг. ред. д-ра юрид. наук, чл.-кор. НАПрН України С.М Гусарова. Харків: ХНУВС. 2016. 296 с.

4. Проект концепції Міграційного кодексу України. – (Сайт Державної міграційної служби України). URL: <https://dmsu.gov.ua/diyalnist/konsultacij-z-gromadskisty/gromadske-obgovorennya/proekt-konczepczij-proektu-migraczijnogo-kodeksu-ukrajni.html>

5. Про затвердження Положення про Державну міграційну службу України: Постанова Кабінету Міністрів України від 20.08.14 р. № 360. *Офіційний вісник України*. 2011. № 29. С. 147. Ст. 1239.

6. Про зовнішню трудову міграцію: Закон України від 05.11.15 р. № 761-VIII. *Відомості Верховної Ради України*. 2015. № 49-50 Ст. 463.

7. Про схвалення Стратегії державної міграційної політики України на період до 2025 року: Розпорядження Кабінету Міністрів України від 12.07.17 р. № 482-р. URL: <http://zakon5.rada.gov.ua/laws/show/482-2017-%D1%80>

8. Січко С.М. Міжнародна трудова міграція як форма міжнародних економічних відносин. *Економіка і менеджмент*. 2016. № 10. С. 112-116.

9. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони URL: [http://zakon2.rada.gov.ua/laws/show/984\\_011](http://zakon2.rada.gov.ua/laws/show/984_011)

10. Anna Boucher, Justin Gest. Migration studies at a crossroads: A critique of immigration regime typologies. *Migration Studies*, Volume 3, Issue 2, 1 July 2015, Pages 182-198. – Electronic text data. – Access mode: <https://doi.org/10.1093/migration/mnu035>

11. Hobson, Barbara, Zenia Hellgren and Luwam Bede (2015): How Institutional Contexts Matter: Migration and Domestic Care Services and the Capabilities of Migrants in Spain and Sweden. Working paper and final project report, FamiliesAndSocieties project (familiesandsocieties.eu), funded by the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 320116. Marianna – Electronic text data. – Access mode: <http://www.familiesandsocieties.eu/wp-content/uploads/2015/11/WP46HobsonEtAl2015.pdf>

12. Marianna Gladysz. Security of the Baltic States: Effectiveness of the EU Common Security and Defence Policy and Influence of the Ukrainian Crisis. – Electronic text data. – Access mode: <https://pressto.amu.edu.pl/index.php/pp/article/download/7230/7249>

13. Piyasiri Wickramasekara. Circular and Temporary Migration Regimes and Their Implications for Family. QScience Proceedings, Family, Migration & Dignity Special Issue. 2013. – Electronic text data. – Access mode: <http://www.qscience.com/doi/pdf/10.5339/qproc.2013.fmd.1>

14. Wolff, Frank. 2013. Rethinking Migration Regimes: Lesson of Post-Communism. Lesson of Post-Communism Working Paper, Indiana University, Bloomington, IN. – Electronic text data. – Access mode: <http://www.indiana.edu/~reeiweb/newsEvents/2013/wolff.pdf>

~~~~~ \* \* \* ~~~~~

УДК: 340.12:342.5:343.352

**КОСИЦЯ О.**, кандидат юридичних наук, доцент кафедри правового забезпечення господарської діяльності  
Харківського національного університету внутрішніх справ

## ПУБЛІЧНИЙ КОНТРОЛЬ ЗА ЗАБЕЗПЕЧЕННЯМ ПРАВ ВИКРИВАЧІВ

**Анотація.** У статті розкрито роль та правові засади публічного контролю за забезпеченням прав викривачів. Проаналізовано сутність державного, громадського, муніципального та міжнародного контролю щодо забезпечення прав викривачів.

**Ключові слова:** викривач, запобігання корупції, захист прав викривачів, публічний контроль, державний контроль, громадський контроль, муніципальний контроль, міжнародні неурядові організації, форми громадського контролю.

**Summary.** In the article the author reveals the role and legal principles of public control over the provision of the rights of whistleblowers. The essence of state, public, municipal and international control over the provision of the rights of whistleblowers is analyzed.

**Keywords:** whistleblowers, counteraction to corruption, protection of the rights of whistleblowers, state control, public control, community control, municipal control, international non-governmental organizations, forms of public control.

**Аннотация.** В статье раскрыта роль и правовые основы публичного контроля за обеспечением прав обличителей. Проанализированы сущность государственного, общественного, муниципального и международного контроля по обеспечению прав обличителей.

**Ключевые слова:** обличитель, противодействие коррупции, защита прав обличителей, государственный контроль, общественный контроль, муниципальный контроль, международные неправительственные организации, формы общественного контроля.

**Постановка проблеми.** Визнаним є факт, що наявність і функціонування інституту контролю як державного, так і громадського сприяє забезпеченню в Україні верховенства права і дотримання прав і свобод людини і громадянина. З огляду на законодавче декларування захисту прав викривачів, важливим є дослідження суб'єктів публічного контролю за забезпеченням їх прав. У даному випадку контроль здійснюється за реалізацією, охороною та захистом прав викривачів.

**Результати аналізу наукових публікацій.** Теоретико-правові засади державного та громадського контролю розглядали в своїх дослідженнях велика кількість науковців, серед яких Андрійко О.Ф., Борець Л.В., Буханевич А.І., Вітвіцький С.С., Гаращук В.М., Джафарова О.В., Стеценко С.Г., Касьяненко Л.В., Коломоєць Т.О., Кравчук В.М., Савченко Л.А., Шестак В.С. та ін. Праці Бенедик В.І., Гвоздецького В.М., Костенко О.О., Мусієнко О.П., Нестеренко О.В., Плиски В.В., Тугарової О.К., Шостко О.Ю., Яцківа І.І. мають фундаментальне значення для правового регулювання та впровадження інституту викривачів в національне правове поле та юридичну науку.

В той же час питання контролю за забезпеченням прав викривачів розглядаються науковцями фрагментарно.

**Метою статті** є розкриття сутності та правових засад публічного контролю за забезпеченням прав викривачів.

**Виклад основного матеріалу.** Досліджуючи різні наукові погляди на поняття викривач, вбачається що означений суб'єкт асоціюється як правило з корупційними

правопорушеннями. Крім того, на законодавчому рівні захист прав гарантується саме викривачам корупційних правопорушень та порушень, пов'язаних з корупцією. Саме тому ми розглянемо роль та сутність публічного контролю за виконанням законодавства у сфері запобігання та протидії корупції в частині забезпечення прав викривачів. Дослідник В.В. Плиска справедливо наголошує, що контроль за виконанням законів у сфері запобігання та протидії корупції має бути системним та здійснюватися належними суб'єктами відповідного контролю на підставах та в межах встановлених чинним законодавством. Метою відповідного контролю має бути перевірка законності здійснення правоохоронними органами дій в процесі протидії та запобігання корупції, їх доцільності та відповідності наданим повноваженням, а також попередження неправомірного порушення прав людини у сфері запобігання та протидії корупції [1, с. 40].

Розпочнемо розгляд публічного контролю з етимології слів “контроль” та “публічний”. Порівняльно-узагальнюючий підхід до зазначених тлумачень показує, що “контроль” – це: 1) перевірка, облік діяльності кого-, чого-небудь, нагляд за кимось, чимось; 2) установа або організація, що здійснює нагляд за ким-, чим-небудь або перевіряє його; 3) люди, які здійснюють перевірку; контролери [2, с. 12-13].

Термін “публічний” походить від латинського *publica, publicus* та в різних словниках тлумачиться по-різному, а саме: як всенародний, оголошений, явний, відомий; організований для публіки, суспільства, народний, загальнонародний, всенародний, вселюдний; всіма спільний, такий, що всім належить [3, с. 535]; як “людовий, народний, громадський, державний” [4]; як “відкритий, гласний, суспільний” [5, с. 560]; як “громадський, публічний, державний” [6, с. 292]. Новий тлумачний словник української мови подає кілька значень слова “публічний”: 1. Який відбувається в присутності публіки, людей; прилюдний, привселюдний, гласний, відкритий. 2. Призначений для широкого відвідування, користування; громадський, загальний, загальнодоступний. 3. Стосується публіки [7, с. 843]. В юридичній енциклопедії термін “публічний” розкривається через словосполучення “публічна влада” (суспільно-політична влада, народовладдя) та “публічне право” (система правових норм, якими регулюються суспільні відносини у сфері публічної влади) [8, с. 196-198].

Як зазначає Кравчук В.М., **публічний контроль** – це система організаційно-правових форм забезпечення додержання законності в діяльності публічної адміністрації, прав і свобод людини, ефективного виконання повноважень і завдань органами державної влади, органами місцевого самоврядування, їх службовими та посадовими особами. Публічний контроль класифікують за суб'єктом його проведення на державний, громадський, муніципальний, міжнародний [9, с. 214].

*Державний контроль* – це самостійно чи зовнішньо ініційована діяльність уповноважених на те суб'єктів, яка спрямована на встановлення фактичних даних щодо об'єктів цього контролю задля визначення їх відповідності (невідповідності) тим правомірним оціночним критеріям, котрі припускають застосування адекватних одержаному результату заходів реагування в унормованому порядку [2, с. 26].

Державний контроль є функцією, стадією публічного управління та ефективним засобом забезпечення верховенства права та реалізації управлінських рішень. Основним суб'єктом державного контролю за забезпеченням прав викривачів є Національне агентство з питань запобігання корупції. Відповідно до повноважень, Національне агентство з питань запобігання корупції здійснює співпрацю із особами, які добросовісно повідомляють про можливі факти корупційних або пов'язаних з корупцією правопорушень, інших порушень Закону України “Про запобігання корупції” [10], вжиття заходів щодо їх правового та іншого захисту, притягнення до відповідальності осіб,

винних у порушенні їх прав, у зв'язку з таким інформуванням. Іншим суб'єктом державного контролю за забезпеченням прав викривачів є Уповноважений Верховної Ради України з прав людини, на якого покладається завдання здійснення парламентського контролю за додержанням конституційних прав і свобод людини і громадянина. Організація роботи омбудсмена у сфері захисту прав викривачів може здійснюватись у наступних напрямках: утворення представництва Уповноваженого з питань контролю за додержанням прав викривачів та забезпеченням їх захисту; утворення в структурі секретаріату Уповноваженого Верховної Ради України з прав людини самостійного структурного підрозділу з питань контролю за додержанням прав викривачів та забезпеченням їх захисту; наукове та організаційне забезпечення формування експертної ради з питань фінансування захисту викривачів тощо.

До речі, в одному із законопроектів щодо захисту прав викривачів [11] передбачено, що контроль за додержанням прав викривачів та забезпеченням їх захисту здійснюватиметься Уповноваженим Верховної Ради України з прав людини; у сфері захисту викривачів, які повідомляють про корупційні, пов'язані з корупцією правопорушення, інші порушення Закону України “Про запобігання корупції” – Національним агентством з питань запобігання корупції. Звичайно, державний контроль за забезпеченням прав викривачів здійснюють і органи прокуратури і органи національної поліції, у випадку загрози життю, житлу, здоров'ю та майну викривачів або їх близьких осіб.

*Громадський контроль* є різновидом соціального контролю і хоча він не є основним з точки зору інтенсивності та обсягів здійснюваних заходів, все одно набуває дедалі більшого значення в українському суспільстві. Це пояснюється його характерними особливостями, як-то: неупередженість, незаангажованість суб'єктів відповідної контрольної діяльності, а також зростанням свідомості та впливовості громадськості, зокрема, її духовними організаційними та іншими ресурсами [12, с. 419]. Серед перешкод, з якими стикається громадськість і які заважають ефективно запобігати корупційним злочинам в державі, називаються пасивність органів державної влади і відсутність взаєморозуміння з нею, недовіра до представників правоохоронних органів і недосконалість законодавства (зокрема, відсутність більш широких прав громадськості, недостатня захищеність викривачів корупційних злочинів) [13, с. 77].

Ми погоджуємось з А. В. Білецьким, що жодна демократична держава не може існувати без дієвого контролю за органами влади з боку суспільства. Контроль є універсальним засобом поліпшення взаєморозуміння між органами публічної влади та громадськістю. Громадськість здатна здійснювати контроль за дотриманням антикорупційних практик не тільки органами влади, але й бізнесом. Контроль тісно переплітається з моніторингом, адже саме за результатами останнього і здійснюється перевірка бізнесу у сфері антикорупції. До того ж, громадськості потрібно буде здійснювати громадську оцінку процесу запровадження антикорупційних програм на підприємствах. Отже, громадськість може стати потужним суб'єктом з подолання корупційних злочинів у приватному секторі [13, с. 165]. Громадський контроль – це системна діяльність уповноважених інститутів громадянського суспільства й окремих громадян щодо встановлення відповідності функціонування публічної адміністрації нормативно-правовим стандартам і корегування виявлених відхилень за допомогою звернень до уповноважених державних органів або до громадської думки [17, с. 355-356].

Дослідник С. А. Косінов узагальнює існуючі в юридичній літературі точки зору щодо визначення громадського контролю і вирізняє такі його істотні ознаки:

– громадський контроль є одним з видів соціального контролю, який здійснюється

об'єднаннями громадян та самими громадянами, і є важливою формою реалізації демократії і способом залучення населення до управління суспільством та державою;

– суб'єктами громадського контролю виступають профспілки, трудові колективи, партії, рухи та ін.;

– громадський контроль виступає засобом забезпечення законності у сфері державного управління;

– це своєрідна форма зворотного зв'язку, який дозволяє побачити, виявити, наскільки точно витримуються параметри системи [15, с. 247].

Як зазначається у п. 8 ст. 21 Закону України “Про запобігання корупції”, громадськість має право здійснювати громадський контроль за виконанням законів у сфері запобігання корупційним злочинам з використанням при цьому таких форм контролю, які не суперечать законодавству [10]. У науковій літературі існують різні погляди на форми громадського контролю. Так, С.Ф. Денисюк визначає, що формами громадського контролю за правоохоронною діяльністю є: звернення громадян, створення та діяльність громадських рад, громадська експертиза, моніторинг дотримання прав людини у правоохоронній діяльності, створення та діяльність громадських організацій, взаємодія із засобами масової інформації [18]. Своєю чергою А.С. Крупник вирізняє наступні форми громадського контролю: соціологічні та статистичні дослідження шляхом анкетування, опитування, стороннього нагляду, включеного нагляду, контент-аналізу, фокус-групових дискусій тощо; участь громадян у виборах, референдумах, зборах, місцевих ініціативах, громадських слуханнях; громадська експертиза актів органів публічної влади та їх проектів; участь громадськості у роботі колегіальних органів влади; включення представників громади до складу робочих груп, які утворюються органами влади; перевірка діяльності будь-якої організації або відповідальної особи, аналіз звітності, результатів діяльності; пропозиції (зауваження), заяви, скарги, клопотання у вигляді письмових та усних, індивідуальних та колективних звернень громадян [19]. За А.В. Білецьким формами участі громадськості є: 1) участь суб'єктів громадського контролю в роботі консультативно-дорадчих органів об'єктів громадського контролю; 2) громадський моніторинг; 3) громадські слухання, консультації з громадськістю, публічні громадські обговорення; 4) громадська антикорупційна експертиза; 5) контроль за прийнятими управлінськими рішеннями спеціальних суб'єктів запобігання корупційним злочинам [13].

Громадський контроль за забезпеченням прав викривачів здійснює консультативно-дорадчий орган – Громадська рада при Національному агентстві з питань запобігання корупції, основними повноваженнями якої є: заслуховування інформації про діяльність, виконання планів і завдань Національного агентства; затвердження щорічних звітів про діяльність Національного агентства; надання висновків за результатами експертизи проектів актів Національного агентства; делегування для участі в засіданнях Національного агентства свого представника з правом дорадчого голосу [10]. Громадська рада повинна і може стати дієвим засобом участі громадськості у реалізації законодавчо задекларованих положень щодо забезпечення прав викривачів.

У Кодексі кращих практик участі громадськості у процесі прийняття рішень 2009 р. зазначено про такі переваги громадського обговорення: 1. Захист – гарантування розгляду потреб та інтересів зацікавлених сторін, яких стосується цей проект правового акта, та на основі цього здійснення впливу на суб'єктів прийняття рішень до голосування. 2. Поліпшення поінформованості – інформування членів, споживачів і ключових груп громадян про процес створення проекту правового акта. 3. Експертиза та рекомендації – проведення аналізу та дослідження з питань, що розглядаються з метою

інформування та впливу на суб'єктів прийняття рішень. 4. Інновація – напрацювання рішення шляхом впровадження нових підходів, практичних заходів і конкретних моделей, які будуть корисними для конкретних груп громадян. 5. Контроль – моніторинг розробки проекту для забезпечення демократичності, прозорості та оптимальної ефективності процесу його прийняття [20].

*Муніципальний контроль* слід розглядати як контроль органів місцевого самоврядування за забезпеченням трудових прав викривачів. Адже згідно п. 3. ст. 53 Закону України “Про запобігання корупції” [10] особа або член її сім'ї не може бути звільнена чи примушена до звільнення, притягнута до дисциплінарної відповідальності чи піддана з боку керівника або роботодавця іншим негативним заходам впливу (переведення, атестація, зміна умов праці, відмова в призначенні на вищу посаду, скорочення заробітної плати тощо) або загрози таких заходів впливу у зв'язку з повідомленням нею про порушення вимог цього Закону іншою особою. В умовах децентралізації муніципальний контроль набуває окремого значення. Згідно ст. 38 Закону України “Про місцеве самоврядування” [14] до відання виконавчих органів сільських, селищних, міських рад належать повноваження щодо внесення подань до відповідних органів про притягнення до відповідальності посадових осіб, якщо вони ігнорують законні вимоги та рішення рад і їх виконавчих органів, прийняті в межах їх повноважень; забезпечення вимог законодавства щодо розгляду звернень громадян, здійснення контролю за станом цієї роботи на підприємствах, в установах та організаціях незалежно від форм власності. А згідно ч. 3 ст. 34 цього ж Закону [14] до відання виконавчих органів міських рад міст обласного значення та об'єднаних територіальних громад належать повноваження щодо: 1) здійснення на відповідних територіях контролю за дотриманням законодавства про працю та зайнятість населення у порядку, встановленому законодавством; 2) накладення штрафів за порушення законодавства про працю та зайнятість населення у порядку, встановленому законодавством.

*Міжнародний контроль* – це контроль держави за виконанням міжнародних зобов'язань її органами, установами, юридичними та фізичними особами, який реалізується через систему міжнародних органів, урядових і неурядових організацій. Зокрема, міжнародний контроль здійснюється шляхом поширення на території держави юрисдикції:

- органів міжнародних організацій, членом або учасником яких є держава, зокрема ОБСЄ, МВФ, Міжнародного банку реконструкції та розвитку, СОТ тощо;
- Міжнародних судових установ, зокрема Європейського суду з прав людини (м. Страсбург), Міжнародного кримінального суду (м. Гаага), Міжнародного арбітражного суду (м. Гаага) [9, с. 214].

Міжнародними організаціями, які підтримують визначальну роль викривання правопорушень у різних сферах суспільного життя та необхідність захисту осіб, які повідомили інформацію про шкоду суспільним інтересам підтримують Європейська Комісія, Рада Європи і Європейський Союз, ОБСЄ, ЮНЕСКО, ООН та ін.

Громадські антикорупційні організації є важливим партнером у запобіганні корупційним злочинам, оскільки, виконуючи представницьку функцію, враховують і виражають у подальшому інтереси громадян і володіють необхідною інформацією про особливості корупційних злочинів всередині країни. Поєднання зовнішнього і внутрішнього впливу не тільки прискорює процес реформування українського законодавства, а й надає необхідну ресурсну підтримку українським громадським організаціям, яку вони отримують від міжнародних неурядових організацій [13, с. 112].

На сьогодні в Україні і світі діє низка міжнародних неурядових організацій, метою діяльності яких є запобігання корупції та співпраця з викривачами. Серед таких організацій: Transparency International, Blue Print for Speech, International Anti-corruption Resource Center, Corruption Watch, Transparify, UNCAC Civil society Coalition, UNICORN, Global Witness, Integrity Action та ін.

Міжнародні судові установи є одним із суб'єктів здійснення публічного контролю за забезпеченням прав викривачів. Відомими справами Європейського суду з прав людини із захисту прав викривачів є справи “Гуджа проти Молдови” *Guja v. Moldova*, по. 14277/04, ECHR 2008, а також *Guja v. Moldova* 2[GC], по. 1085/10, ECHR 2018; “Гайніш проти Німеччини” (*Heinisch v. Germany*) по. 28274/08, ECHR 2011; “Марченко проти України” (*Marchenko v. Ukraine*), по. 4063/04, § 46, 19 лютого 2009), які можуть застосовуватись національними судами при вирішенні публічно-правових спорів з питань захисту прав осіб, незаконно звільнених у зв'язку з їх діяльністю як викривача.

### Висновки.

Публічний контроль за забезпеченням прав викривачів є системою організаційних та правових форм забезпечення додержання закону в діяльності як публічного так і приватного сектору щодо реалізації, охорони, захисту прав викривачів, який здійснюється на підставі та в межах законодавства різними суб'єктами на міжнародному, державному, громадському та муніципальному рівнях.

### Використана література

1. Плиска В.В. Адміністративно-правовий механізм забезпечення прав і свобод громадян у сфері запобігання та протидії корупції: дис. ...канд. юрид. наук: 12.00.07. Ужгород. ДВНЗ “Ужгородський національний університет”, 2015. 210 с.
2. Шестак В.С. Державний контроль в сучасній Україні (загальнотеоретичні питання): дис. ...канд. юрид. наук: 12.00.01. Харків. Національний університет внутрішніх справ, 2002. 195 с.
3. Даль В.И. Толковый словарь: в 4 т. Москва: Рус. яз., 1999. Т. 3: П. 1999. С. 535.
4. Кобилянський Юліан. Латинсько-український словар для середніх шкіл. Відень, 1912.
5. Словник іншомовних слів / за ред. чл.-кор. АН УРСР О.С. Мельничука. Київ, 1977.
6. Кілієвич О. Англо-український глосарій термінів і понять з аналізу державної політики та економіки. Київ: Вид-во Соломії Павличко “Основи”, 2003. 510 с
7. Новий тлумачний словник української мови: у 4 т. / уклад. В. Яременко, О. Сліпушко. Київ: Аконт, 2000. Т. 3 (О-Р). 927 с.
8. Юридична енциклопедія: в 6 т. / редкол.: Ю.С. Шемшученко (відп. ред.) та ін. Київ: “Укр. енцикл.”, 2003. Т. 5: П-С. 398 с.
9. Кравчук В. Публічний контроль у державі. *Юридичний вісник*. 2015. № 1. С. 210-215. URL : [http://nbuv.gov.ua/UJRN/urid\\_2015\\_1\\_39](http://nbuv.gov.ua/UJRN/urid_2015_1_39)
10. Про запобігання корупції: Закон України від 14.10.14 р. № 1700-VII. URL : <https://zakon.rada.gov.ua/laws/show/1700-18>
11. Про захист викривачів і розкриття інформації про шкоду або загрозу суспільним інтересам: проект Закону України від 20.07.16 р. № 4038а. URL: [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=59836](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=59836)
12. Попова О.О., Калініченко А.П. Громадський контроль у сфері надання адміністративних послуг органами внутрішніх справ: проблемні питання. *Форум права*. 2014. № 1. С. 418-421.
13. Білецький А.В. Участь громадськості у запобіганні корупційним злочинам в Україні: дис. ...канд. юрид. наук: 12.00.08. Харків: Національний юридичний університет імені Ярослава Мудрого, 2018. 228 с.
14. Про місцеве самоврядування в Україні: Закон України від 21.05.97 р. № 280/97-ВР. URL: <https://zakon.rada.gov.ua/laws/show/280/97-%D0%B2%D1%80>



15. Косінов С.А. Контроль у демократичній державі: монографія. Харків: Право, 2015. 360 с.
16. Денисюк С.Ф. Організація громадського контролю у сфері забезпечення правоохоронними органами громадського порядку. *Форум права*. 2009. № 2. С. 102-107. URL: [http://nbuv.gov.ua/UJRN/FP\\_index](http://nbuv.gov.ua/UJRN/FP_index)
17. Вітвіцький С.С. Контроль як гарантія законності діяльності публічної адміністрації: дис ...д-ра юрид. наук: 12.00.07. Київ, 2016. 480 с.
18. Денисюк С.Ф. Громадський контроль за правоохоронною діяльністю в Україні: адміністративно-правові засади: автореф. дис. ...д-ра юрид. наук: спец. 12.00.07. Дніпропетровськ, 2010. 36 с.
19. Крупник А.С. Громадський контроль: сутність та механізми здійснення. Теоретичні та прикладні питання державотворення. *On-line збірник наук. праць ОРІДУНАДУ при Президентіві України*. Вип. № 1. 2007. URL : <http://novyi-stryi.at.ua/gromkontrol/> KRUPNYK\_A\_pro\_grom\_kontrol.pdf
20. Code of Good Practice for Civil Participation in the Decision-Making Process (CONF/PLE (2009) CODE 1): Adopted by the Conference of INGOs at its meeting on 1st October 2009. Strasburg, 2009. P. 10-12.

~~~~~ \* \* \* ~~~~~

УДК 347.952

**ЛИМАРЬ І.В.**, аспірант кафедри цивільного процесу,  
Національний юридичний університет імені Ярослава Мудрого

## ДИСКУСІЙНІ ПИТАННЯ МІСЦЯ ВИКОНАВЧОГО ПРОВАДЖЕННЯ В СИСТЕМІ ПРАВА УКРАЇНИ

**Анотація.** Статтю присвячено дослідженню підходів визначення правової природи виконавчого провадження, його місця в системі права України, аналізу існуючих у науковій літературі точок зору на виконавче провадження як завершальну стадію судового процесу шляхом проведення порівняльної характеристики з іншими поглядами щодо місця виконавчого провадження в системі права. У зв'язку із суттєвим оновленням законодавства у галузі примусового виконання рішень залишається багато суперечливих невирішених питань у теорії та практиці застосування законодавства у виконавчому провадженні, оскільки неможливо провести реформування галузі примусового виконання не визначившись із суттю та місцем виконавчого провадження в системі права України, що обумовлює актуальність та значимість теми дослідження. Підвищення ефективності застосування нового законодавства у галузі виконання рішень неможливе без поєднання доктрини та практики, що сприятиме удосконаленню процесуального механізму примусового виконання рішень. Визначення галузевої та інституціональної належності виконавчого провадження має наукове та практичне значення з причини відсутності правової позиції щодо чіткого закріплення місця виконавчого провадження в системі права України. Крім іншого, законодавство, що регулює примусове виконання рішень, характеризується неоднорідністю правових норм.

**Ключові слова:** виконавче провадження; виконавчий процес; виконання рішень; правова природа; цивільно-процесуальна природа виконавчого провадження; виконавче право; стадія процесу.

**Summary.** The article is devoted to the study of the approaches to determining the legal nature of executive proceedings, its place in the system of law of Ukraine, the analysis of the points of view existing in the scientific literature on executive proceedings as the final stage of the judicial process by conducting a comparative characteristic with other views on the place of executive proceedings in the system of law. In connection with the significant updating of the law in the field of enforcement of decisions, there are many controversial unresolved issues in the theory and practice of applying the law in the enforcement proceedings, since it is impossible to reform the sphere of forced execution without defining the essence and place of enforcement proceedings in the system of law of Ukraine, which stipulates relevance and significance of the research topic. Increasing the effectiveness of the application of new legislation in the area of implementation of decisions is impossible without combining doctrine and practice, which will facilitate the improvement of the procedural mechanism of enforcement of decisions. The determination of sectoral and institutional membership of executive proceedings has a scientific and practical significance, due to the lack of a legal position regarding the clear attachment of the place of enforcement in the system of law of Ukraine. Among other things, the law governing the enforcement of decisions is characterized by heterogeneity of legal norms.

**Keywords:** executive proceedings; executive process; execution of decisions; legal nature; civil procedural nature of enforcement proceedings; executive power; stage of the process.

**Аннотация.** Статья посвящена исследованию подходов определения правовой природы исполнительного производства, его места в системе права Украины, анализа существующих в научной литературе точек зрения на исполнительное производство как завершающую стадию судебного процесса путем проведения сравнительной характеристики с другими взглядами относительно места исполнительного производства в системе права. В связи с существенным

обновлением законодательства в области принудительного выполнения решений остается много противоречивых нерешенных вопросов в теории и практике применения законодательства в исполнительном производстве, поскольку невозможно провести реформирование области принудительного выполнения, не определившись с сутью и местом исполнительного производства в системе права Украины, которая обуславливает актуальность и значимость темы исследования. Повышение эффективности применения нового законодательства в области выполнения решений невозможно без объединения доктрины и практики, которое будет содействовать усовершенствованию процессуального механизма принудительного выполнения решений. Определение отраслевой и институциональной принадлежности исполнительного производства имеет научное и практическое значения по причине отсутствия правовой позиции относительно четкого упрочения места исполнительного производства в системе права Украины. Кроме другого, законодательство, которое регулирует принудительное выполнение решений, характеризуется неоднородностью правовых норм.

**Ключевые слова:** исполнительное производство; исполнительный процесс; исполнение решений; правовая природа; гражданско-процессуальная природа исполнительного производства; исполнительное право; стадия процесса.

**Постановка проблеми.** Проблеми галузі примусового виконання рішень набули нового змісту з прийняттям оновленого законодавства про виконавче провадження, однак залишило деякі спірні питання в правовій науці залишилися не вирішеними. Виконавче провадження забезпечує досягнення матеріально-правової мети юрисдикційної діяльності, за показником фактичного виконання рішень можна робити про ефективність та дієвість механізму впорядкування суспільних відносин та правового захисту в державі в цілому. Саме фактичною реалізацією судового рішення повинен завершуватися будь-який цивільний процес у справі, оскільки на стадії виконання відбувається реальний захист прав, обов'язків, охоронюваних законом інтересів, підтверджених рішенням суду. Без визначення місця виконавчого провадження в правовій системі України неможливо здійснити якісне вдосконалення механізму примусового виконання рішень та забезпечення повноцінного захисту прав та законних інтересів учасників виконавчого провадження. Відсутність чіткої правової позиції в науці та законодавстві щодо правової природи та визначення місця виконавчого провадження в системі права України негативно впливає на правове регулювання правовідносин, які виникають під час примусового виконання рішень судів та інших юрисдикційних органів.

**Результати аналізу наукових публікацій.** Теоретичні і практичні проблеми виконавчого провадження в різних аспектах досліджувалися такими науковцями як: Ю.В. Білоусов (U.V. Bilousov), С.С. Бичкова (S.S. Bichkova), Д.Х. Валєєв (D. Kh. Valyev), Є.В. Васьковський (Є.V. Vaskovsky), П.П. Заворотько (P.P. Zavorotko), В.В. Комаров (V.V. Komarov), В.І. Тertiшніков (V.I. Tertichnikov), С.Я. Фурса (S. Ya. Fursa), М.Й. Штефан (M.J. Stefan), Є.О. Харитонов (Є.O. Kharitonov), С.В. Щербак (S.V. Shcherbak), С.О. Якимчук (S.O. Yakimchuk) та іншими. Але і нині існують полярні погляди щодо правової природи виконавчого провадження. Це, безперечно, впливає на формування новітнього законодавства та практику примусового виконання рішень. Зважаючи на вищезазначене, особливості виконавчих правовідносин потребують подальшого наукового дослідження з метою їх класифікації.

**Метою статті** є визначення моделей правової природи та місця виконавчого провадження в системі права України, а саме правовідносин, що виникають під час примусового виконання рішень, галузевої приналежності норм, якими врегульовані правовідносини у виконавчому провадженні, та визначення закономірностей і шляхів

удосконалення механізму цивільно-правового регулювання у сфері виконавчого провадження.

**Виклад основного матеріалу.** Фактичне виконання судових рішень та рішень інших органів (посадових осіб) (далі – рішень) є показником ефективності здійснення правосуддя в державі та невід’ємною частиною юрисдикційної діяльності під час захисту і фактичного поновлення порушених прав, свобод та інтересів людини і громадянина.

Виконанням судових рішень завершується процес захисту суб’єктивних прав юридичних та фізичних осіб шляхом їх фактичної реалізації у спосіб та порядок, визначений Конституцією України та законами України. Саме забезпечення прав і свобод людини є головним обов’язком держави відповідно до статті 3 Конституції України [1].

У цивільному процесуальному законодавстві та в науці відповідної галузі права відсутня єдність у характеристиці стадії виконання судових рішень. Можна зустріти різні назви цієї стадії, а саме: “виконавче провадження”, “виконавчий процес”, “виконання судових рішень”, “виконання судових постанов”. Останні взагалі не охоплюють рішень, у т.ч. інших органів, що підлягають виконанню в порядку цивільного судочинства, передбачених законодавством.

Думки науковців з цього питання різняться. Наприклад, Гукасян Р.Є. вважав, що найменування даної стадії саме як “виконавче провадження” передбачає єдині засоби виконання рішень державних органів та інших несудових органів [2, с. 135]. Натомість Щербак С.В. вважає некоректним об’єднання декількох проваджень під одним поняттям “виконавче провадження” та пропонує їх назвати “виконавчий процес” [3, с. 15].

Сібільов Д.М., у свою чергу, вважає, що виконавче провадження на сьогодні фактично перетворюється на “виконавчий процес”, оскільки виконавчому провадженню притаманна така ознака процесуальної форми як стадійність, а система норм виконавчого провадження за ступенем урегульованості є вищою, ніж звичайна система процедур, і тяжіє до системи процедур щодо розгляду справ, установлені відповідним процесуальним законодавством [4, с. 38].

На думку Заворотько П.П., термін “виконавче провадження” не є вдалим, оскільки його значення підкреслює відособленість цієї стадії від інших стадій цивільного процесу в цілому, та не вказує, що виконавче провадження є судовим, тобто здійснюється в порядку цивільного судочинства. Найбільш вдалим найменуванням, на думку автора, є термін “судове виконання”, який підкреслює приналежність виконання саме до цивільного процесу, відображає роль суду у виконанні та показує його відмінність від інших видів примусового виконання [5, с. 141].

Зважаючи на різність думок та трактувань науковцями та законодавцем найменування стадії “виконання судових рішень” необхідно виробити єдину назву даної стадії, яка б найбільш повно відображала зміст правовідносин, що виникають під час примусового виконання рішень між учасниками даних правовідносин та привести у відповідність до цього законодавство.

Відносно визначення місця виконавчого провадження також не існує єдності наукових підходів. Так, у 1924 р. Краснокутським В.А. у своїй праці “Очерки гражданского процессуального права” уперше висловлена думка про розмежування виконавчого провадження та цивільно-процесуального права, оскільки, на думку вченого, право на судові рішення є однією з форм захисту права, а примусове виконання – іншою.

Юков М.К. у 1975 р. вперше зробив спробу обґрунтувати думку, що виконавче провадження є комплексною галуззю права та має визначену юридичну цілісність, предмет, метод правового регулювання та специфіку [6]. Пізніше у своєму

дисертаційному дослідженні Юков М.К. сформулював і назву цієї галузі – виконавче право [7, с. 155-191].

Такі висновки підтримали та розвинули Шерстюк В.М. та Ярков В.В. При цьому вони відзначили непроцесуальний характер виконавчого провадження, зазначивши, що відносини, які виникають під час виконання рішень різних юрисдикційних органів та цивільні процесуальні відношення не є однорідними [8, с. 22; 9]. Прибічники цієї теорії висловили припущення щодо формування нової галузі та запропонували її назви: “цивільне виконавче право”, “виконавче право”. Однак жодна з них на сьогодні так і не закріпилась.

Ісаєнкова О.В. також розглядає виконавче провадження як предмет виконавчого права поза цивільним процесом, а галуззю права не саме виконавче провадження, а виконавче право як сукупність норм, які регулюють виконання юрисдикційних актів. Авторкою виокремлено у виконавчому праві специфічний предмет, метод, нормативну базу та принципи [9].

Прихильники виокремлення виконавчого права за галузевою ознакою обґрунтовують позицію про виникнення в системі права “адміністративно-виконавчого права”. Наводяться аргументи щодо розгляду виконавчого провадження як складової частини адміністративного процесу, серед яких: участь у правовідносинах виконавчого провадження обов’язкового суб’єкту – державного виконавця та його підпорядкованість органам Міністерства юстиції України; наділення державного виконавця владними повноваженнями та публічно-правовий характер правовідносин у виконавчому провадженні, які мають всі ознаки адміністративних процесуальних норм та ін.

Наприклад, досліджуючи місце інституту виконавчого провадження в системі права України, Щербак С.В. не погоджується з думками вчених щодо самостійності галузі виконавчого права та робить висновок про те, що виконавче провадження перебуває у сфері дії адміністративного процесу, а для з’ясування місця виконавчого провадження в системі права вагоме значення має його адміністративно-правове регулювання [10, с. 7]. Аналогічної думки дотримується також Ігонін Р.В. на підставі аналізу властивостей, притаманних виконавчому провадженню, зазначаючи, що виконавче провадження є складовою адміністративного процесу, оскільки поєднує в собі адміністративно-процедурну та адміністративно-юрисдикційну ознаки [11, с. 8; 12, с. 200].

Схожої думки дотримується і авторський колектив під керівництвом видатного вченого Фурси С.Я., визначаючи виконавче провадження як інститут адміністративного процесу, а правовідносини, що виникають у виконавчому провадженні – як адміністративно-процесуальні [13, с. 797]. Крім іншого, Фурса С.Я., розкриваючи сутність та систему виконавчих правовідносин зазначає, що примусове виконання рішень є однією з юрисдикційних функцій держави, яка, на відміну від цивільного процесу, має свої індивідуалізуючі ознаки, обумовлені предметом і методом правового регулювання цих відносин, тому виконавчі правовідносини є різновидом правових відносин, що виникають у сфері організації та діяльності органів та осіб примусового виконання [14, с. 12-13].

На нашу думку, такі твердження вбачаються досить спірними, оскільки система законодавства та нормативно-правові акти з питань примусового виконання рішень знаходяться на етапі реформування та становлення, тому виокремлення виконавчого провадження в самостійну галузь права є занадто передчасним, доцільніше приділити більше уваги уніфікації законодавства, із об’єднанням специфічних форм та методів, процедур примусового виконання рішень різних галузей права в один блок загальних засад виконавчого провадження з урахуванням специфічних особливостей окремих

галузей судочинства. Із точкою зору щодо визнання виконавчих правовідносин адміністративно-процесуальними теж важко погодитись, оскільки правова природа правовідносин у виконавчому провадженні не співпадає з предметом адміністративно-процесуального регулювання відносин у сфері державного управління.

Хоча єдина точка зору щодо природи та місця виконавчого провадження в системі права на сьогодні відсутня, все ж можна виокремити декілька основних напрямків, в яких виконавче провадження розглядається як: 1) стадія цивільного (господарського, адміністративного) процесу; 2) частина вказаних галузей права; 3) самостійна галузь права (назва якої є також дискусійною та неоднозначною).

В той же час слід відзначити те, що більшість авторів розглядає виконання судових рішень як завершальну стадію саме цивільного процесу.

Як зазначав з цього приводу Талан Л.Г., виконання рішень суду є заключною стадією цивільного процесу та завершує діяльність по здійсненню правосуддя та захисту права, що здійснюється судом, а отже, правосуддя варто розуміти в широкому вимірі – як діяльність суду з розгляду спору і виконання судового рішення [15, с. 100]. На думку Шерстюка В.М., виконавче провадження є складовою частиною механізму захисту цивільного права та заключним етапом (стадією) його реалізації [16]. Білоусов Ю.В. вважає виконання рішення кінцевим етапом юрисдикційної (правозахисної) діяльності. Без реалізації цієї стадії (етапу), на його переконання, втрачається сенс попередньої діяльності суду, оскільки саме виконанням рішення суду завершується процес захисту суб'єктивних майнових та особистих немайнових прав громадян та юридичних осіб шляхом їх фактичної реалізації у спосіб та порядок, визначений Конституцією та законами України [17, с. 5]. Дискусія ґрунтується на різних поглядах щодо моменту завершення процесу захисту права. Одні вчені, про що мова йшла вище, стверджують, що процес захисту порушених прав та законних інтересів завершується з моменту прийняття судового рішення. Інші дослідники вважають завершенням процесу захисту порушеного права реальне виконання рішення.

Найбільш вірною, на нашу думку, є остання точка зору, оскільки вона найповніше відображає сутність виконавчого провадження. Не можна вважати досягнутою основну мету цивільного процесу, обмежившись отриманням судового рішення та набранням ним законної сили.

Так, Боннер О.Т. вважає, що суспільні відносини, які виникають під час виконання рішень, мають похідно-допоміжний характер та в повною мірою відображають основну модель цивільних процесуальних відносин між компетентними державними органами та учасниками процесу, а тому не можуть бути самостійним об'єктом правового регулювання [18]. Тобто автором також розглядається виконавче провадження як заключна стадія цивільного процесу, в якій відбувається реалізація рішення суду, де суд виступає контролюючим органом, що діє в інтересах держави та суспільства.

Виконавче провадження як частина єдиного цивільного процесу здійснення правосуддя само по собі є заключною, логічно-монолітною процесуальною стадією. Розмежування виконавчої діяльності на стадії дозволяє акцентувати увагу практичних працівників (суддів, юрисконсультів, адвокатів, судових виконавців) на процесуальних особливостях здійснення дій на різних етапах провадження, що природно, підвищує ефективність виконання та законну реалізацію судового рішення в повному обсязі [20, с. 39].

Точка зору щодо виконавчого провадження як заключної стадії цивільного процесу підтримується Комаровим В.В. На його думку, виконання рішень є частиною цивільного процесу, його заключною стадією, зв'язок якої з попередніми обумовлений тим, що в

рамках цивільного процесу відбувається реалізація норм матеріального права та самого суб'єктивного матеріального права, що впливає з цієї норми. Як відзначає автор, захист порушених прав передбачає не тільки декларацію певного правового становища в судовому рішенні, а й обов'язкову реалізацію висновків суду, у тому числі в межах провадження щодо примусового виконання [21, с. 941]. Пелевін С.М. також зазначав, що стадія виконання рішень є останньою, заключною та обов'язковою стадією цивільного процесу, оскільки вона є наслідком розгляду і вирішення цивільної справи, у якій захист суб'єктивних цивільних прав і законних інтересів знаходить своє реальне втілення та не переходить в іншу стадію цивільного судочинства [22]. У контексті зазначеного вище Заворотько П.П. відзначав, що особливістю цивільного процесу є не лише швидкий і повний розгляд цивільних справ, а й створення умов на всіх стадіях процесу, необхідних для виконання судових рішень, досягнення повного відновлення порушеного права. На його думку, позов і виконавче провадження є засобом захисту права на різних етапах цивільного процесу, що мають спільну кінцеву мету, але досягають її різними процесуальними засобами. Позов є засобом захисту порушеного чи оспорюваного права, а виконавче провадження – засобом захисту права, яке перестало бути спірним і підлягає примусовій реалізації [23, с. 3-4].

Конституційний та Верховний суди України у своїх рішеннях неодноразово зазначали, що виконання рішення, ухваленого будь-яким судом, має розцінюватися як невід'ємна частина судового розгляду, завершальна стадія судового провадження, складова права кожного на судовий захист та справедливий суд, процесуальною гарантією доступу до суду [24 – 27], що передбачено статтями 6, 13 Конвенції Ради Європи “Про захист прав людини та основоположних свобод” від 04.11.1950 р. (далі – ЄКПЛ).

Статтею 8 Загальної декларації прав людини від 10 грудня 1948 року проголошено право кожного не тільки на ефективне правосуддя, але й на поновлення в правах у випадку їх порушення, покладаючи обов'язок поновлення прав на “компетентні національні суди” [28]. Під поновленням розуміється не тільки прийняття судом законного та обґрунтованого рішення, а й контроль за його виконанням, оскільки саме на цьому етапі здійснення правосуддя відбувається реальне поновлення порушених прав.

У справах “Торнсбі проти Греції” від 19.03.1997 р., “Бурдов проти Росії” від 07.05.2002 р., “Ромашов проти України” від 27.07.2004 р., “Шаренок проти України” від 22.02.2004 р., “Васильчук проти України” від 10.12.2009 р. [29 – 33] та низці інших, ЄСПЛ зазначає, що право на судовий захист було б ілюзорним, якби правова система держави дозволяла, щоб остаточне зобов'язальне рішення залишалося бездієвим на шкоду одній із сторін. Виконання рішення, ухваленого будь-яким судом, має вважатися невід'ємною частиною цивільного процесу та не може бути відокремлене від судового провадження. Отже, згідно з прецедентною практикою ЄСПЛ, провадження з виконання судових рішень є самостійною і невід'ємною частиною судового розгляду та складовою права на справедливий суд.

### **Висновки.**

Таким чином, виконавче провадження можна визначити як заключну стадію цивільного процесу при примусовому виконанні рішень судів цивільної юрисдикції. Його також можна визнати як сукупність пов'язаних між собою та визначених законодавством процесуальних дій уповноважених органів та осіб з примусового виконання рішень суду та інших юрисдикційних органів, врегульованих правовими нормами, які забезпечені державним примусом та спрямовані на фактичне поновлення порушених (оспорюваних) суб'єктивних цивільних (в широкому розумінні) матеріальних прав та охоронюваних законом інтересів.

На нашу думку, виконавче провадження в частині забезпечення виконання виконавчих документів цивільних судів можна вважати заключною стадією цивільного процесу, органічним продовженням судового розгляду та його логічним завершенням. Судове рішення має ознаки виконавчого документу та ініціює процедуру виконавчого провадження, а сторони у виконавчому та судовому процесі не можуть бути іншими. Судове рішення має встановлені гарантії виконуваності, головною з яких є процедура примусового виконання, що забезпечена механізмами державного примусу. Виконавче провадження є невід'ємною складовою дотримання та захисту права людини на справедливий судовий розгляд упродовж розумного строку, встановленого статтею 6 ЄКПЛ.

Виконавче провадження, попри неоднозначність поглядів, має нерозривний зв'язок із попередніми стадіями цивільного процесу та єдністю цілей для всіх видів судочинства (цивільного, господарського, адміністративного), які полягають у захисті та поновленні порушених, невизнаних та оспорюваних прав, свобод і інтересів юридичних осіб, а також інтересів держави. Отже, виконавче провадження можна визначити завершальною стадією судового провадження, яке є невід'ємним елементом права на судовий захист та в якій досягається основна мета цивільно-процесуальної діяльності та правосуддя в цілому, а саме реальне відновлення захищених судом або іншим органом порушених прав чи інтересів.

Як вірно зазначила Щербак С.В., однією з причин того, що виконавче провадження є слабкою ланкою механізму захисту прав громадян і юридичних осіб, є недостатня увага вчених і практиків до проблем виконання судових рішень у період бурхливого розвитку економічних відносин, що було зумовлене невизначеністю місця виконавчого провадження в системі правових наук [11, с. 1].

### Використана література

1. Конституція України: Закон України. URL: <http://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80> (дата звернення: 18.12.2018).
2. Гукасян Р.Є. Єдність засобів виконання рішень державних органів та суспільних організацій, що здійснюють захист прав громадян та соціалістичних організацій. – (“50 років Радянської влади та актуальні проблеми правової науки”). Саратов, 1967. С. 111.
3. Щербак С.В. Зміст виконавчого процесу. *Правовий вісник УАБС*. 2011. № 2(5). С. 15-18.
4. Сібільов Д.М. Генетичні ознаки виконавчого провадження в системі цивільної юрисдикції. *Юрист України*. 2011. Вип. 2. С. 34-38.
5. Заворотько П.П. Процессуальные гарантии исполнения судебного решения. Москва: Юридическая литература, 1974. 360 с.
6. Юков М.К. Самостоятельность норм, регулирующих исполнительное производство. *Проблемы совершенствования ГПК РСФСР*. Свердловск. 1975. Вып. 40. С. 91-97.
7. Юков М. К. Теоретические проблемы системы гражданского процессуального права: дис. ...д-ра юрид. наук. Свердловск, 1975.
8. Шерстюк В.М. Система советского гражданского процессуального права. Москва: Изд-во МГУ, 1989. С. 133.
9. Ярков В. В. Проблемы реализации судебных актов. Проблемы совершенствования правосудия по гражданским делам. Ярославль: Изд-во Ярославского ун-та, 1991. С. 80-81.
10. Исаенкова О.В. Проблемы исполнительного права в гражданской юрисдикции: автореф. дис. ...д-ра юрид. наук. Саратов, 2003. 17 с.
11. Щербак С.В. Адміністративно-правове регулювання виконавчого провадження в Україні: автореф. дис. ...канд. юрид. наук. Київ, 2002. 17 с.



12. Ігонін Р.В. Організаційно-правові засади діяльності суб'єктів виконавчого провадження: автореф. дис. ...канд. юрид. наук. Ірпінь, 2007. 22 с.
13. Лівар Ю.О. Про виконавчі провадження в адміністративному праві. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія "Право".* 2015. Вип. 19. С. 198-202.
14. Цивільний процес України: академічний курс/ за ред. С.Я. Фурси та ін. Київ : Видавець Фурса С.Я.: КНТ, 2009. 848 с.
15. Фурса С.Я. Формування теоретичних основ виконавчих процесуальних правовідносин: сутність, система, ознаки та класифікація. *Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки.* Київ, 2013. Вип. 95. С. 12-16.
16. Талан Л.Г. Виконавче провадження в структурі цивілістичного процесу. *Вісник Академії правових наук України.* Харків. 2009. Вип. 2. С. 96-102.
17. Юков М.К. Исполнительное производство. Москва, 2000.
18. Білоусов Ю.В. Виконавче провадження: навч. посібник. Київ: Прецидент, 2004. 192 с.
19. Боннер А.Т. Проблемы установления истины в гражданском процессе. СПб, 2009.
20. Зайцев И., Худенко В. Стадии исполнительного производства в гражданском процессе. *Российская юстиция.* 1994. Вып. 6. С. 39-41.
21. Комаров В.В., Бігун В.А., Баранкова В.В., Гусаров К.В. Курс цивільного процесу : підручник. Харків: Право, 2011. 1352 с.
22. Мусина М.А., Чечина Н.А., Чечота М.Д. Гражданский процесс. Москва. 1996. С. 370.
23. Загоротько П.П. Процессуальные гарантии исполнения судебного решения. Москва: Юрид. лит-ра, 1974. С. 360.
24. Рішення Конституційного суду України від 13 грудня 2012 р. № 18-рп/2012, судова справа № 1-26/2012. URL: <http://zakon3.rada.gov.ua/laws/show/v018p710-12> (дата звернення: 20.07.2018).
25. Рішення Конституційного суду України від 25 квітня 2012 р. № 11-рп/2012, судова справа № 1-12/2012. URL: <http://zakon5.rada.gov.ua/laws/show/v011p710-12/paran17#n17> (дата звернення: 20.07.2018).
26. Рішення Конституційного суду України від 26 червня 2013 р. № 5-рп/2013, судова справа № 1-7/2013. URL: <http://zakon3.rada.gov.ua/laws/show/v005p710-13> (дата звернення: 13.07.2018).
27. Рішення Верховного суду України від 16 січня 2018 р. № 520/5696/14-ц, судова справа № 520/17779/14-ц. URL: <http://reyestr.court.gov.ua/Review/71666815> (дата звернення: 16.07.2018).
28. Загальна декларація прав людини. URL: [https://zakon.rada.gov.ua/laws/show/995\\_015](https://zakon.rada.gov.ua/laws/show/995_015) (дата звернення 13.02.2019).
29. Рішення ЄСПЛ від 19.03.1997 р., судова справа Горнсбі проти Греції. URL: [https://zakon.rada.gov.ua/laws/show/980\\_079/print](https://zakon.rada.gov.ua/laws/show/980_079/print) (дата звернення 15.02.2019).
30. Рішення ЄСПЛ від 07.05.2002 р., судова справа Бурдов проти Росії. URL: [https://zakon.rada.gov.ua/laws/show/980\\_045](https://zakon.rada.gov.ua/laws/show/980_045) (дата звернення 15.02.2019).
31. Рішення ЄСПЛ від 27.07.2004 р., судова справа Ромашов проти України. URL: [https://zakon.rada.gov.ua/laws/show/980\\_227](https://zakon.rada.gov.ua/laws/show/980_227) (дата звернення 15.02.2019).
32. Рішення ЄСПЛ від 22.02.2004 р., судова справа Шаренок проти України. URL: [https://zakon.rada.gov.ua/laws/show/980\\_235](https://zakon.rada.gov.ua/laws/show/980_235) (дата звернення 15.02.2019).
33. Рішення ЄСПЛ від 10.12.2009 р., судова справа Васильчук проти України. URL: [https://zakon.rada.gov.ua/laws/show/974\\_532](https://zakon.rada.gov.ua/laws/show/974_532) (дата звернення 15.02.2019).

~~~~~ \* \* \* ~~~~~

## 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 напрямками 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.
- 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 вчитаними, 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 370 грн. на рахунок Інституту.**

**Реквізити для оплати робіт:**

*Науково-дослідний інститут інформатики і права Національної академії правових наук України. Р/р 31251259111870 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 НДІП 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 дотримання 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

**№ 2(29)/2019**

|                                               |                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Засновники журналу:                           | <ul style="list-style-type: none"> <li>- Науково-дослідний інститут інформатики і права Національної академії правових наук України (НДІП НАПрН України);</li> <li>- Національна бібліотека України ім. В.І. Вернадського Національної академії наук України;</li> <li>- Відкритий міжнародний університет розвитку людини “Україна”.</li> </ul>                 |
| Видавець:                                     | © НДІП НАПрН України.                                                                                                                                                                                                                                                                                                                                            |
| Адреса редакції:                              | 01032, м. Київ, вул. Саксаганського, 110-В.<br>Науково-дослідний інститут інформатики і права<br>Національної академії правових наук України.<br>Тел.: 234-94-56; e-mail: bvm777@ ukr.net                                                                                                                                                                        |
| Веб-сторінки журналу у мережі Інтернет:       | URL: //www.ippi.org.ua – НДІП НАПрН України;<br>URL: //www.nbuv.gov.ua – Нац. бібліотека України ім. В.І. Вернадського.                                                                                                                                                                                                                                          |
| Founders of journal:                          | <ul style="list-style-type: none"> <li>- Scientific Research Institute of Informatics and Law of the National Academy of Law Sciences of Ukraine (SRIIL of the NALS of Ukraine);</li> <li>- Vernadsky National Library of Ukraine of National Academy of Sciences of Ukraine;</li> <li>- Open International University of Human Development “Ukraine”</li> </ul> |
| Publisher:                                    | © SRIIL of the NALS of Ukraine.                                                                                                                                                                                                                                                                                                                                  |
| Address of release:                           | 01032, Kyiv, Saksaganskogo str., 110-V.<br>Scientific Rresearch Institute of Informatics and Law<br>of the National Academy of Law Sciences of Ukraine.<br>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;<br>URL: //www.nbuv.gov.ua – Vernadsky National Library of Ukraine of National Academy of Sciences of Ukraine.                                                                                                                  |