

ДЕРЖАВНА НАУКОВА УСТАНОВА «ІНСТИТУТ ІНФОРМАЦІЇ, БЕЗПЕКИ І ПРАВА
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ»
АПАРАТ ВЕРХОВНОЇ РАДИ УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ РЕЄСТРАЦІЇ ІНФОРМАЦІЇ
НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ

НОРМАТИВНО-ПРАВОВА ІНФОРМАЦІЯ І ПАРЛАМЕНТСЬКИЙ КОНТРОЛЬ

МАТЕРІАЛИ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

Київ, 21 вересня 2023 року

Київ
2023

УДК 342.53:004(477)
Н 83

*Рекомендовано до друку вченою радою
Державної наукової установи «Інститут інформації, безпеки і права
Національної академії правових наук України»
(протокол № 10 від 3 жовтня 2023 р.)*

Н 83 Нормативно-правова інформація і парламентський контроль : матеріали наук.-практ. конф. (Київ, 21 верес. 2023 р.) / наук. керівник конф.: Д. В. Ланде ; упор.: В. М. Фурашев, А. І. Нижник, С. О. Дорогих ; ДНУ «Ін-т інформ., безпеки і права Нац. академії правов. наук України». – Київ, 2023. – 118 с.
ISBN 978-617-8395-12-4

У збірнику висвітлено матеріали науково-практичної конференції щодо оцінки проблемних питань правового і програмно-технічного забезпечення здійснення ефективного парламентського контролю та його подальшого розвитку. Запропоновано напрями вдосконалення правотворчої діяльності, розвитку системи нормативно-правової інформації та використання сучасних інформаційних (цифрових) технологій в галузі держави і права як основи парламентського контролю.

Видання розраховано на фахівців, експертів і вчених, науково-педагогічних працівників і здобувачів вищої освіти.

УДК 342.53:004(477)

Матеріали подано в авторській редакції

- © Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», 2023
- © Апарат Верховної Ради України, 2023
- © Інститут проблем реєстрації інформації Національної академії наук України, 2023
- © Колектив авторів, 2023

ISBN 978-617-8395-12-4

ЗМІСТ

РЕКОМЕНДАЦІЇ	5
--------------------	---

ТЕЗИ ДОПОВІДЕЙ

Нижник А. І. ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ	8
Жиляєв І. Б. СУЧАСНА МОДЕЛЬ КОНТРОЛЬНОЇ ДІЯЛЬНОСТІ УКРАЇНСЬКОГО ПАРЛАМЕНТСЬКОГО КОМІТЕТУ	14
Фурашев В. М. ПАРЛАМЕНТСЬКИЙ КОНТРОЛЬ: РОЛЬ В СУЧАСНИХ УМОВАХ	17
Корж І. Ф. ПРОБЛЕМИ ДОСТУПУ ДО НОРМАТИВНО-ПРАВОВОЇ ІНФОРМАЦІЇ В СУЧАСНИХ УМОВАХ	24
Ланде Д. В. СЕМАНТИЧНЕ ІНДЕКСУВАННЯ ДОКУМЕНТІВ В ГАЛУЗІ ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ	28
Брайчевський С. М. ШТУЧНИЙ ІНТЕЛЕКТ ТА АНАЛІЗ МЕРЕЖЕВОГО КОНТЕНТУ У ПАРЛАМЕНТСЬКОМУ КОНТРОЛІ	33
Vitalii Andreichuk APPLICATION OF ARTIFICIAL INTELLIGENCE METHODS IN THE TASKS OF PARLIAMENTARY CONTROL IN MODERN CONDITIONS	37
Костенко О. В. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЗІ ШТУЧНИМ ІНТЕЛЕКТОМ ЯК СУЧАСНИЙ ІНСТРУМЕНТАРІЙ ЕФЕКТИВНОГО ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ	41
Майстренко І. А., Фурашев В. М. СУБ'ЄКТИ ТА ОБ'ЄКТИ ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ В УМОВАХ СОЦІАЛЬНИХ ТРАНСФОРМАЦІЙ	45
Лихоступ С. В. ОСНОВИ СИСТЕМИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ В ПРОЦЕСАХ РОЗВИТКУ СОЦІАЛЬНИХ СТРУКТУР УКРАЇНИ	52
Радзівська О. Г. ПАРЛАМЕНТСЬКИЙ КОНТРОЛЬ ЗА ДОДЕРЖАННЯМ ІНФОРМАЦІЙНИХ ПРАВ ЛЮДИНИ В УМОВАХ ВОЄННОГО СТАНУ	56
Білан І. А. ПАРЛАМЕНТСЬКИЙ КОНТРОЛЬ ЗА ДІЯЛЬНІСТЮ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ	60

<i>Дорогих С. О.</i> ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН УКРАЇНИ В УМОВАХ ВІЙНИ.	64
<i>Лазор О. Д., Лазор О. Я.</i> ОПРИЛЮДНЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ ФІЗИЧНОЇ ОСОБИ: ПРАВОВЕ РЕГУЛЮВАННЯ ПИТАНЬ.	68
<i>Заславська Л. В.</i> ПРОБЛЕМИ ПРИТЯГНЕННЯ ДО ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА РОЗПОВСЮДЖЕННЯ АНТИУКРАЇНСЬКОЇ ПРОПАГАНДИ В УМОВАХ ВОЄННОГО СТАНУ.	72
<i>Дурач О. А.</i> ПРОБЛЕМНІ ПИТАННЯ СУДОВОГО РОЗГЛЯДУ ВІЙСЬКОВИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ.	75
<i>Качинський А. Б., Шаповалов А. А.</i> СУЧАСНІ МЕТОДИ АНАЛІЗУ ПРОПАГАНДИСТСЬКИХ КАМПАНІЙ В УМОВАХ ВІЙНИ.	79
<i>Данильян О. Г., Дзьобань О. П.</i> МЕРЕЖЕВІ ВІЙНИ ЯК СОЦІОКУЛЬТУРНЕ ТЛО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.	84
<i>Кірієнко В.</i> ПРОТИДІЯ ІНФОРМАЦІЙНІЙ АГРЕСІЇ ТА ІНФОРМАЦІЙНІЙ ПРОПАГАНДИ.	88
<i>Васько В. А.</i> ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ: ОГЛЯД ПРАВОВИХ ПРОБЛЕМ.	90
<i>Сердечна А. Ю.</i> ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ОБ'ЄКТ ЗЛОЧИННОГО ВПЛИВУ З БОКУ СИЛ ДЕРЖАВИ-АГРЕСОРА ТА ПЕРСПЕКТИВИ ЇЇ ЗАХИСТУ.	95
<i>Горун О. Ю.</i> ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.	100
<i>Хроленко Я. О.</i> МЕТОДИ ПРОТИДІЇ ФІШИНГОВИМ АТАКАМ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ.	105
<i>Каліновський Я. О., Боярінова Ю. Є., Гнатенко В. Д.</i> КОДУВАННЯ ІНФОРМАЦІЇ ШТРИХОВИМИ КОДАМИ.	109
<i>Казьмірук С. Д., Леонов Б. Д.</i> ЗАСТОСУВАННЯ ПОЛІГРАФА ЯК ЗАХІД З ВІДНОВЛЕННЯ ДОВІРИ ДО ДЕРЖАВНИХ ІНСТИТУТІВ.	112
<i>Петряєв О. С.</i> ПОЛІТИЧНА ПОЗИЦІЯ РОСІЙСЬКОГО МУСУЛЬМАНСЬКОГО ДУХОВЕНСТВА В УКРАЇНСЬКО-РОСІЙСЬКІЙ ВІЙНІ.	115

РЕКОМЕНДАЦІЇ
учасників науково-практичної конференції
«НОРМАТИВНО-ПРАВОВА ІНФОРМАЦІЯ
І ПАРЛАМЕНТСЬКИЙ КОНТРОЛЬ»

21 вересня 2023 року Державною науковою установою «Інститут інформації, безпеки і права Національної академії правових наук України» спільно з Апаратом Верховної Ради України та Інститутом проблем реєстрації інформації Національної академії наук України проведено науково-практичну конференцію «*Нормативно-правова інформація і парламентський контроль*».

В ході конференції розглянуто наступні питання:

- *основи державної політики у сфері парламентського контролю;*
- *проблеми становлення і розвитку систем і баз даних нормативно-правової інформації;*
- *методи, моделі й технології правової інформатики;*
- *аналітичні правові системи на основі відкритих джерел інформації (OSINT);*
- *перспективи застосування штучного інтелекту для розвитку систем нормативно-правової інформації та забезпечення парламентського контролю;*
- *особливості забезпечення інформаційної безпеки та кібербезпеки систем нормативно-правової інформації в умовах воєнного стану.*

В ході активного експертного обговорення вказаних питань учасники науково-практичної конференції **констатували:**

- відсутність необхідного юридичного визначення понятійно-категоріального апарату у сфері парламентського контролю в національному законодавстві, а також недосконалість правового регулювання форм і методів парламентського контролю, що негативно позначається на ефективності його організації та здійснення;
- необхідність розробки, наукового і правового опрацювання концепції подальшого розвитку системи парламентського контролю та її складових в контексті європейської та євроатлантичної інтеграції України;
- потребу подальшого опрацювання робочої моделі парламентського контролю в умовах цифровізації, змісту електронних баз даних нормативно-правових актів, як основи створення національної інтегрованої системи нормативно-правових актів, а також правових проблем розвитку систем нормативно-правової інформації;

- актуальність проблеми ефективності правотворчої діяльності, якості підготовлених та поданих до реєстрації у Верховній Раді України законопроектів, організації їх науково-правової експертизи, а також проблеми визначення об'єктивної необхідності прийняття цих законопроектів для врегулювання відповідних суспільних відносин у різних сферах життєдіяльності людини, суспільства і держави;
- поширеність практики подальшого доопрацювання вже прийнятих законів шляхом внесення до них численних змін і доповнень. Зокрема, аналіз динаміки прийняття законів України у 2019-2023 рр. (станом на 06.09.2023) свідчить, що за цей час було прийнято 1155 законів, з яких 80% – щодо внесення змін і доповнень;
- актуальність питання організації належного наукового та інформаційно-аналітичного забезпечення правотворчої діяльності, а також покладання завдання щодо розробки концептуальних засад розвитку законодавства на профільні наукові установи НАН України і НАПрН України та Дослідницьку службу Верховної Ради України.

Розглянувши зазначені та інші актуальні проблемні питання учасники науково-практичної конференції **рекомендували:**

1. Запропонувати Комітету Верховної Ради України з питань регламенту, депутатської етики та організації роботи Верховної Ради України та Комітету Верховної Ради України з питань правової політики:

- забезпечити законодавче визначення понятійного апарату у сфері парламентського контролю, а також подальший розвиток системи парламентського контролю в Україні;
- розглянути питання про внесення змін до Конституції України щодо функціонування коаліційної моделі парламентсько-урядової взаємодії в межах чинної парламентсько-президентської форми правління;
- забезпечити адаптацію змісту нового Регламенту Верховної Ради України до Конституції України з урахуванням стандартів ЄС з питань коаліційної парламентсько-урядової взаємодії;

2. Запропонувати Апарату Верховної Ради України спільно з ДНУ ПБП НАПрН України:

- опрацювати питання щодо правового регулювання подальшого використання сучасних інформаційно-комунікаційних (цифрових) технологій та штучного інтелекту в інтересах розвитку системи парламентського контролю та захисту кібернетичної безпеки у цій сфері;

- забезпечити подальше формування і розвиток електронних баз даних нормативно-правових актів, як основи створення національної інтегрованої системи правової інформації.

3. Забезпечити у визначені терміни реалізацію вимог Закону України «Про правотворчу діяльність» та внести зміни до цього закону щодо покладання завдання розробки концепції розвитку законодавства на НАН України, НАПрН України та Дослідницьку службу Верховної Ради України.

4. В контексті європейської інтеграції України опрацювати питання щодо підготовки та прийняття законів України *«Про парламентську службу»*, *«Про лобіювання»*, *«Про гарантії парламентської опозиції»*, а також кодекс парламентської етики.

ТЕЗИ ДОПОВІДЕЙ

Нижник А. І.

Перший заступник керівника

Головного юридичного управління

Апарату Верховної Ради України

ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ

Серед вітчизняних наукових визначень державної політики найбільш прийнятними у контексті парламентського контролю – діяльності з реалізації контрольної функції парламенту, видаються такі.

О. Валевський пропонує під «державною політикою розуміти діяльність, націлену на вирішення проблем суспільного розвитку» [1, с. 21].

В. Тертичка трактує державну політику як відносно стабільну, організовану й цілеспрямовану діяльність/бездіяльність державних інституцій, здійснюваної ними безпосередньо чи опосередковано щодо певної проблеми або сукупності проблем, яка впливає на життя суспільства. [2, с. 82-83].

О. Кучеренко дійшов висновку, що в сучасній суспільно-політичній думці переважають три головні концепції державної політики, а саме:

1) плюралістична (акцентує увагу на процесі формування та здійснення державної політики в сучасному демократичному суспільстві як мультирівневої конкуренції між впливовими суспільно-політичними групами та об'єднаннями); 2) суспільного вибору і 3) детерміністська. [3, с.279].

Актуальність втілення в Україні плюралістичної концепції державної політики набула нового виміру у контексті європейської та євроатлантичної інтеграції. І це цілком природний процес, оскільки основою цієї концепції є спільні ідеологічні цінності європейської спільноти та демократичні (діалогові) механізми формування і реалізації публічної політики, що здатні забезпечити сталий суспільний розвиток на основі дійсного демократичного урядування.

Тому на сучасному етапі суспільного розвитку вітчизняна державна політика у мирний час має формуватися та реалізовуватися на демократичних засадах, що властиві плюралістичним, відкритим суспільствам, з урахуванням членства України в Раді Європи, членства українського парламенту в Міжпарламентському Союзі, набуття Україною статусу держави – кандидата до ЄС та її євроатлантичних прагнень.

Зокрема, щодо виконання критеріїв вступу країн до Європейського союзу (копенгагенські критерії), то варто виділити політичний критерій: стабільність інституцій, що гарантують демократію, верховенство права, права людини та повагу і захист меншин, а також правовий критерій: спроможність взяти зобов'язання щодо членства, включаючи відданість цілям політичного, економічного та валютного союзу. Інституцією від стабільності якої залежить законодавче забезпечення реалізації гарантій демократії є парламент.

Сама представницька природа парламенту, його місце та роль у державному механізмі покладають на нього провідну організаційну роль у владному трикутнику (глава держави, парламент, уряд) щодо втілення плюралістичної концепції державної політики шляхом: стратегічного планування розвитку законодавства, визначення засад внутрішньої та зовнішньої політики, остаточного санкціонування розроблених урядом законів, нагляду за своєчасним виданням урядом підзаконних актів і здійснення інших заходів, спрямованих на ефективну реалізацію та удосконалення державної політики.

Оскільки плюралістична концепція державної політики є похідною від плюралістичної моделі демократії ліберального типу, ознаки якої закріплені у тексті Основного Закону України, системний аналіз її положень та практика їх удосконалення дозволяє окреслити деякі особливості сучасного процесу формування та здійснення державної політики у сфері парламентського контролю.

Так, фактом схвалення у 2016 році українським парламентом параметрів «парламентської реформи» (йдеться про посилення інституційної спроможності парламенту), цю реформу визнано однією з ключових [4]. Однак, реалізація відповідних рекомендацій потребує також і внесення змін до Конституції України, спрямованих на розвиток парламентаризму і парламентського контролю. Це, зокрема, стосується положень статті 81, якою закріплено імперативний мандат.

Хоча відповідні рекомендації не містять натяку на скасування депутатського імунітету, а у пункті 44 йдеться про необхідність врегулювання статусу парламентської опозиції, що й досі є актуальним, розпочата хвиля політичного популізму завершилася прийняттям 3 вересня 2019 року закону № 27-ІХ і ліквідацією депутатського імунітету як парламентського явища.

Внаслідок руйнування інституту депутатської недоторканності парламентарія (як цілісне явище передбачає обов'язкове поєднання індемнітету та імунітету) недоліки імперативного мандату за пропорційної виборчої системи ще більше посилюються. Подібна практика не вписується

ся у європейські стандарти парламентаризму як така, що не забезпечує гарантії діяльності парламентської опозиції у контексті парламентського контролю [5].

Описуючи функціональні характеристики парламенту Л. Герасіна та М. Панов зазначають: «Увесь парламент і кожен депутат окремо може виступати в ролі «гласу народу», його «опікуна», «слуги», «дзеркала» народної волі. Крім того, кожен депутат має так званий загальний мандат, за яким він отримує право представляти всю націю в цілому» [6].

Відтак, гарантований нині статтею 80 Конституції України депутатський індемнітет, що походить від фундаментального принципу ідеологічного та політичного плюралізму, закріпленого статтею 15 Конституції України (елемент конституційного ладу), має реалізовуватися як в мирний час, так і в умовах воєнного стану, однак з урахуванням обмежень, що зумовлені особливим режимом організації роботи органів державної влади у воєнний час.

Проведення ж у демократичний спосіб необхідних реформ та втілення відповідних стандартів в українські реалії має здійснюватися за участі громадянського суспільства, на основі принципів і механізмів плюралістичної концепції державної політики, що забезпечують раціональне поєднання належного громадянського контролю і дієвого та конструктивного парламентського контролю.

На відміну від загального поняття державної політики, державно-правова політика (нормативна складова) у сфері парламентського контролю є невід'ємною складовою парламентського права, що згідно загальної теорії парламентаризму і парламентського права віднесено до галузі конституційного права (відповідно матеріального і процесуального). Такий теоретичний поділ парламентського права на матеріальну та процесуальну складові дозволяє виокремити парламентський регламент як внутрішній процесуально-процедурний акт серед інших законодавчих актів у сфері парламентського контролю.

Попри наявність формальних розбіжностей між положеннями Конституції України (статей 19, 92 і 83, 88) щодо правової форми парламентського регламенту як внутрішнього процесуального акту, нині діючий регламент має форму закону.

Загальновідомо, що в багатьох парламентах світу, які працюють за Вестмінстерською моделлю Великої Британії, поширеною є практика коли парламентський регламент не є законом і тому парламентські правила та процедури можуть тлумачитися лише спікером, а не судами.

Така, на перший погляд, лише формальна відмінність регламенту як законодавчого акту, зумовлена принципом поділу влади, автономією

парламенту та особливою природою внутрішньо-парламентських відносин, що безпосередньо не стосуються реалізації прав громадян. Відтак діяльність з унормування та перегляду законодавцем процесуальних парламентських правил у власному регламенті виведена із стандартного для законів циклу державної політики. Адже внутрішньо-парламентські відносини за своєю політико-юридичною природою не підпадають під суспільну проблему у сенсі державної політики, що потребує законодавчого втручання на основі стандартних процедур демократії участі із залученням громадськості.

На основі цих тез і міркувань робимо умовивід, що притаманна коаліційній моделі парламентсько-урядової взаємодії урядово-центристська технологія законотворення, не повинна поширюватися на процес удосконалення парламентських правил і процедур.

Відповідно до засадничих положень розділу I Конституції України парламентський контроль у правовій, демократичній державі має здійснюватися на професійній основі парламентом і іншими уповноваженими законом суб'єктами (*парламентськими комітетами і тимчасовими слідчими комісіями, уповноваженим з прав людини, Рахунковою палатою, а також парламентаріями*). Коло цих суб'єктів визначене безпосередньо у Конституції України і вони зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України (частина друга статті 19). Тобто, формально-юридично ця імперативна конституційна вимога не допускає нормативне регулювання організації та здійснення парламентського контролю на підзаконному рівні.

За такої конституційної логіки виключно законодавець зобов'язаний прийняти відповідну сукупність первинних законодавчих актів, які системно та комплексно унормують обидва правові механізми організації та здійснення внутрішнього і зовнішнього парламентського контролю.

Отже, державно-правова політика у сфері парламентського права і контролю має певні кількісні та якісні характеристики, за якими її можна виокремити у окремий блок державно-правової політики.

Згідно з інформацією, що розміщена на веб-сайті українського парламенту у базі даних «законодавство», з 24.06.1991 року чинними станом на 10.07.2023 року є 7533 закони, у тому числі: первинних – 819 і вторинних (якими внесено зміни) – 6714. Ці показники ілюструють нестабільність державно-правової політики.

У загальному масиві первинних законодавчих актів України діє біля десяти законодавчих актів, що можна віднести до сфери парламентського права. Спеціального закону про парламентський контроль не існує, так само як і закону про парламентську опозицію, однак статусні закони

містять положення, що передбачають періодичність і строки звітування у парламенті відповідних державних органів і силових структур.

До сталих законодавчих актів відносяться: Конституція України, закони про статус народного депутата, про комітети Верховної Ради України, про тимчасові комісії Верховної Ради України, про уповноваженого Верховної Ради України, про Рахункову палату, про Кабінет Міністрів України тощо (статусні законодавчі акти).

До змінних законодавчих актів відноситься: Регламент Верховної Ради України (процесуально-процедурний акт). Про це свідчить його життєвий цикл, упродовж якого (починаючи з 10 лютого 2010 року) до нього вносилися зміни більше 64 разів. При цьому особливою якісною характеристикою чинного Регламенту є те, що у ньому містяться також і матеріальні норми.

Загальними якісними характеристиками законодавчих актів у сфері парламентського права і контролю є такі: вища юридична сила, зміст відповідає положенням Конституції України, що забезпечує узгодженість положень, чіткість, зрозумілість, однозначність норм права, завершеність правового механізму тощо.

Завдяки плюралізму в науці маємо дещо різні доктринальні позиції вітчизняних вчених щодо широкого [7] та вузького [8] розуміння джерел парламентського права. Зважаючи на відповідні підходи стосовно наукової класифікації і систематизації джерел парламентського права, можемо з урахуванням відмінностей їх природи та юридичної сили зробити наступні висновки:

1) суспільні відносини з питань внутрішнього парламентського контролю регулюються Конституцією України, парламентським Регламентом, Угодою про коаліцію депутатських фракцій, парламентськими прецедентами, традиціями та звичаями;

2) суспільні відносини з питань зовнішнього парламентського контролю регулюються Конституцією України, статусними законами, парламентським Регламентом.

Така дещо спрощена класифікація сукупності джерел парламентського права, якими регулюються організація та здійснення внутрішнього і зовнішнього парламентського контролю, ілюструє принципову відмінність за обсягом, юридичною силою та природою джерел парламентського права. Головною відмінністю унормування процесу зовнішнього парламентського контролю є виключно законодавчий рівень регулювання відповідних суспільних відносин взаємодії суб'єктів парламентського контролю з іншими підзвітними органами державної влади, діяльність яких врегульовано статусними законами (про кабінет міністрів, про центральні органи виконавчої влади тощо).

Державотворчі українські реалії в умовах існуючої моделі коаліційної парламентсько-урядової взаємодії свідчать про тенденцію розширення сфери парламентського контролю на діяльність новоутворених антикорупційних, правоохоронних і військових структур, що закономірно має збільшити навантаження на суб'єктів, уповноважених на здійснення парламентського контролю. Проте, розвиток конституційно закріпленої системи суб'єктів парламентського контролю є неможливим через її консерватизм, що зумовлений вищою юридичною силою Конституції України.

Таким чином, гіпотеза про системоутворювальні недоліки відповідних конституційних положень, консервативний характер їх змісту, що не сприяють розвитку парламентського права у сфері парламентського контролю, підтвердилася. Отже питання необхідності узгодження та системного удосконалення положень Конституції України в частині парламентської реформи має вирішуватися комплексно як складова конституційної реформи.

Список використаних джерел:

1. Валевський О. Л. Державна політика в Україні: методологія аналізу, стратегія, механізми впровадження : [монографія] / О. Л. Валевський. – К. : НІСД, 2001. – 242 с.

2. Тертичка В. В. Державна політика: аналіз та здійснення в Україні / В. В. Тертичка. – К. : Вид-во Соломії Павличко«Основи», 2002. – 750 с.

3. Кучеренко О. Державна політика: аналіз сучасних політологічних концепцій / О. Кучеренко// Актуальні проблеми реформування державного управління в Україні : Мат. наук.-практ. конф. – К. : Вид-во УАДУ, 1997. – С. 279-281.

4. Постанова Верховної Ради України від 17 березня 2016 року № 1035-VIII – Режим доступу: <https://zakon.rada.gov.ua/rada/show/1035-19#Text>

5. Нижник А. Недоторканність народного депутата України – конституційно-правова гарантія незалежного парламентського контролю: інформаційно-правовий аспект (ст. 141-155). Журнал «Інформація і право» 2(29)/2019.

6. Політико-правові інститути сучасності: Структура, функції, ефективність/ За заг. ред. М. І. Панова, Л. М. Герасіної. – К., 2005. – С. 157.

7. Олуйко В. Парламентське право України: проблеми теорії та практики. Юрінком Інтер. 2004. 216 с.

8. Древаль Ю., Тодика Ю. Формування парламентського права у процесі державотворення. Віче. 2006. №7.

Жиляєв І. Б.

*доктор економічних наук, старший
дослідник, головний науковий
співробітник Інституту вищої освіти
НАПедН України*

СУЧАСНА МОДЕЛЬ КОНТРОЛЬНОЇ ДІЯЛЬНОСТІ УКРАЇНСЬКОГО ПАРЛАМЕНТСЬКОГО КОМІТЕТУ

Парламентський контроль (Parliamentary control) – складний і кропіткий процес, який вимагає участі значної кількості учасників, зокрема – експертів, вивчення матеріалів нормативно правового, інформаційно-довідкового і науково-аналітичного характеру, статистичних та інших даних. Правового визначення терміну «парламентський контроль» в українському законодавстві немає, що негативно впливає на детермінацію парламентського контролю (ПК) [1]. Використовується термін «контрольні функції парламенту», конкретного визначення змісту якого українським законодавством також не надано (див. глава 38 та 38-1 парламентського Регламенту [2]). Наукові дослідження використовують ці терміни у достатньо широкому змісті. Підсумкові рішення з ПК формуються і реалізуються парламентом на публічних засіданнях, але їх підготовка забезпечується кропіткою роботою значної кількості суб'єктів ПК, саме тому існують різні організаційні форми його діяльності, однією з основних є комітети і комісії.

Інструменти парламентського контролю. Серед інструментів ПК (Tools of Parliamentary Oversight) R. Pelizzo і R. Stapenhurst виділяють: комісію з розслідування (Commission of enquiry) 95,9%, запитання до урядовців (Questions) – 96,3%, комітетські слухання (Committee Hearing) – 95,6%, парламентські слухання (Hearing in plenary sitting) – 90,8%, проведення часу запитань (Question time) – 84,0%, розслідування (Interpellations) – 75,4% та діяльність омбудсмена (Ombudsman) 72,4%. Примітка: розміщено у порядку частоти практики використання на основі опитування парламентів 83 країн у 2001 році [3].

Парламентські слухання. Особливе місце в питаннях здійснення ПК займають парламентські слухання у Верховній Раді, які проводяться з метою вивчення питань, що становлять суспільний інтерес та потребують законодавчого врегулювання (частина 1 статті 233 Регламенту [2]). На наш погляд, ключовим на наш погляд є визначення мети «вивчення питань, що становлять суспільний інтерес та потребують законодавчого врегулювання», що передбачає розуміння у законодавця відповідного «поля проблем» та виділення найбільш актуальної з цих проблем для

суспільства, що виноситься на розгляд. Не менш важливим є й друга частина мети, тобто наявності **потреби і потенціалу законодавчого врегулювання проблем, їх пріоритизації** (вибору найбільш законодавчо актуальної). Фактично, обидві частини мети проведення парламентських слухань надалі розшифровуються у частині 9 статті 236 Регламенту: «Постанова, якою схвалюються рекомендації за результатами проведення парламентських слухань, повинна містити строки надання інформації про стан реалізації рекомендацій, а також, у разі необхідності, план проведення обговорень («круглих столів», громадських обговорень, слухань у комітетах тощо) щодо стану їх реалізації, список законопроектів, необхідних для реалізації рекомендацій, орієнтовний строк їх розробки і внесення та перелік комітетів, яким Верховна Рада доручає розробити відповідні законопроекти, перелік інших заходів, спрямованих на реалізацію рекомендацій та контроль за їх виконанням» [2]. Знов таки, вищезазначена норма передбачає, на наш погляд, певну конкретизацію інструментів парламентського нагляду (Tools of Parliamentary Oversight), перш за все у формуванні цілей суспільно-політичного розвитку.

Особливості здійснення ПК у сфері науки та освіти. За Комітетом ВР України з питань освіти, науки та інновацій було закріплено наступні предмети: освіта; наука, науково-технічна діяльність та наукові парки; правовий статус та соціальний захист наукових, педагогічних і науково-педагогічних працівників; інноваційна діяльність, розвиток високих технологій (крім питань, які віднесені до предметів відання інших комітетів); засади здійснення наукових і науково-технічних експертиз [4]. Особливості діяльності Комітету ВР України, за яким закріплено повноваження у сферах освіти і науки (у ВР України VIII скликання (2014 – 2019 рр.) – Комітет з питань науки і освіти; у ВР України IX скликання (2019 р. по цей час) – Комітет з питань освіти, науки та інновацій). Перелік інструментів ПК комітету включає: 1) парламентські слухання, в яких комітет є головним; 2) слухання в комітеті; 3) розгляд контрольних питань; 4) проведення інших масових заходів у вигляді круглих столів та виїзних засідань; 5) аналіз законодавчої бази та формування ініціатив щодо її розвитку; 6) затвердження звернень (запитів) народних депутатів з актуальних питань тощо. При цьому, статистичні дані демонструють достатньо напружену діяльність Комітету. Так, Комітет ВР України VIII скликання з питань науки і освіти провів 111 засідань, на яких розглянув 649 питань, з яких 111 розгляд законопроектів, 55 контрольних питань. Було проведено 5 парламентських слухань та 3 комітетських слухань. Комітет ВР України IX скликання з питань освіти, науки та інновацій за II-VIII сесії провів 113 засідань, на яких розглянув 731 питання, з яких

417 присвячених розгляду законопроектів, 57 контрольних питань. Було проведено 12 комітетських слухань [5].

Резюме. 1. В Україні створена діюча система ПК, яка модернізувалася протягом останніх років у зв'язку з пандемією та широкомасштабною війною в бік більш широкого застосування цифровізація комунікативних функцій як спілкування з інституціями громадського суспільства, так з виконанням функцій ПК. Зазначене призвело до зміни об'єктів та форм ПК, «заморожуванням» використання традиційних форм, таких як парламентські слухання, запровадженням мережевих технологій у здійсненні ПК, інтенсифікацією застосування експертних умоглядних матеріалів замість результатів статистичних та наукових досліджень. 2. Фактично функції ПК в частині проведення консультацій з громадськістю в значному ступені змістилися з рівня парламенту на рівень парламентських комітетів. 3. Здійсненню ПК заважає, на наш погляд, гіперактивність парламентарів (порівняно із іншими суб'єктами права законодавчої ініціативи) у здійсненні законотворчих функцій. Зазначене призводить к некоректній гіпертрофії вноормування в законах сукупності проблем, сформованих на основі як експертних уявлень, так й впливу політичних вподобань. Це призводить до подальшого поширення практики доопрацювання норм законів, некритичного до них ставлення, що у певних випадках знижує саму ефективність ПК. 4. Верховна Рада України має проаналізувати практики здійснення парламентськими комітетами ПК в сучасних умовах, а на основі цього аналізу – розглянути доцільність розробки уніфікованих технологій політики комітетського ПК. 5. Розглянути доцільність створення окремого законодавства, яке б сприяло підвищенню рівня безпосередньої участі громадян у законодавчому процесі, практик ПК.

Список використаної літератури

1. Жилиєв І. Б. Інструментарій контрольних функцій парламентського комітету (на прикладі науки та вищої освіти). *Інформація і право*. 2022. № 4. с. 139-148. http://ippi.org.ua/sites/default/files/15_24.pdf

2. Про Регламент Верховної Ради України: Закон України від 10.02.10 р. № 1861-VI, редакція від 31.03.23 р. URL: <https://zakon.rada.gov.ua/laws/show/1861-17#Text>

3. Pelizzo, R. & Stapenhurst, R. (2004). Tools for Legislative Oversight: An Empirical Investigation. Washington, DC: *World Bank Policy Research Working Paper*. URL: <https://openknowledge.worldbank.org/entities/publication/d491f73e-6d3c-50c7-8205-fb1bc280d9da>

4. Про комітети Верховної Ради України: Закон України від 04.04.95 р. № 116/95-ВР, редакція від 31.03.23 р. URL: <https://zakon.rada.gov.ua/laws/show/116/95-%D0%B2%D1%80#Text>

5. Офіційний веб-сайт Комітету ВР України з питань освіти, науки та інновацій. URL: <https://kno.rada.gov.ua/>

Фурашев В. М.

кандидат технічних наук, старший науковий співробітник, перший заст. директора Державної наукової установи «Інститут інформації, безпеки і права НАПрН України»

ПАРЛАМЕНТСЬКИЙ КОНТРОЛЬ: РОЛЬ В СУЧАСНИХ УМОВАХ

Стаття 5 Конституції України чітко вказує: «Носієм суверенітету і **єдиним джерелом влади** в Україні **є народ**. Народ здійснює владу безпосередньо і через органи державної влади та органи місцевого самоврядування. Право визначати і змінювати конституційний лад в Україні належить виключно народові і не може бути узурповане державою, її органами або посадовими особами. **Ніхто не може узурпувати державну владу**».

Стаття 6 також чітко структурує систему державної влади – «державна влада в Україні здійснюється на засадах її поділу на законодавчу, виконавчу та судову.»

Таким чином, законодавчу владу, з урахуванням більш деталізованих положень Розділу IV «Верховна Рада України», можна визнати як основного представника народовладдя.

Стаття 85 Конституції України встановлює **37** головних напрямів повноважень Верховної Ради України в системі державного управління, а саме:

- 1) внесення змін до Конституції України в межах і порядку, передбачених розділом XIII цієї Конституції;
- 2) призначення всеукраїнського референдуму з питань, визначених статтею 73 цієї Конституції;
- 3) прийняття законів;
- 4) затвердження Державного бюджету України та внесення змін до нього, контроль за виконанням Державного бюджету України, прийняття рішення щодо звіту про його виконання;

5) визначення засад внутрішньої і зовнішньої політики, реалізації стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору;

6) затвердження загальнодержавних програм економічного, науково-технічного, соціального, національно-культурного розвитку, охорони довкілля;

7) призначення виборів Президента України у строки, передбачені цією Конституцією;

8) заслуховування щорічних та позачергових послань Президента України про внутрішнє і зовнішнє становище України;

9) оголошення за поданням Президента України стану війни і укладення миру, схвалення рішення Президента України про використання Збройних Сил України та інших військових формувань у разі збройної агресії проти України;

10) усунення Президента України з поста в порядку особливої процедури (імпичменту), встановленому статтею 111 цієї Конституції;

11) розгляд і прийняття рішення щодо схвалення Програми діяльності Кабінету Міністрів України;

12) призначення за поданням Президента України Прем'єр-міністра України, Міністра оборони України, Міністра закордонних справ України, призначення за поданням Прем'єр-міністра України інших членів Кабінету Міністрів України, Голови Антимонопольного комітету України, Голови Державного комітету телебачення і радіомовлення України, Голови Фонду державного майна України, звільнення зазначених осіб з посад, вирішення питання про відставку Прем'єр-міністра України, членів Кабінету Міністрів України;

12-1) призначення на посаду та звільнення з посади за поданням Президента України Голови Служби безпеки України;

13) здійснення контролю за діяльністю Кабінету Міністрів України відповідно до цієї Конституції та закону;

14) затвердження рішень про надання Україною позик і економічної допомоги іноземним державам та міжнародним організаціям, а також про одержання Україною від іноземних держав, банків і міжнародних фінансових організацій позик, не передбачених Державним бюджетом України, здійснення контролю за їх використанням;

15) прийняття Регламенту Верховної Ради України;

16) призначення на посади та звільнення з посад Голови та інших членів Рахункової палати;

17) призначення на посаду та звільнення з посади Уповноваженого Верховної Ради України з прав людини; заслуховування його щоріч-

них доповідей про стан дотримання та захисту прав і свобод людини в Україні;

18) призначення на посаду та звільнення з посади Голови Національного банку України за поданням Президента України;

19) призначення на посади та звільнення з посад половини складу Ради Національного банку України;

20) призначення на посади та звільнення з посад половини складу Національної ради України з питань телебачення і радіомовлення;

21) призначення на посади та звільнення з посад членів Центральної виборчої комісії за поданням Президента України;

22) затвердження загальної структури, чисельності, визначення функцій Служби безпеки України, Збройних Сил України, інших утворених відповідно до законів України військових формувань, а також Міністерства внутрішніх справ України;

23) схвалення рішення про надання військової допомоги іншим державам, про направлення підрозділів Збройних Сил України до іншої держави чи про допуск підрозділів збройних сил інших держав на територію України;

24) встановлення державних символів України;

25) надання згоди на призначення на посаду та звільнення з посади Президентом України Генерального прокурора; висловлення недовіри Генеральному прокуророві, що має наслідком його відставку з посади;

26) призначення на посади третини складу Конституційного Суду України;

28) дострокове припинення повноважень Верховної Ради Автономної Республіки Крим за наявності висновку Конституційного Суду України про порушення нею Конституції України або законів України; призначення позачергових виборів до Верховної Ради Автономної Республіки Крим;

29) утворення і ліквідація районів, встановлення і зміна меж районів і міст, віднесення населених пунктів до категорії міст, найменування і перейменування населених пунктів і районів;

30) призначення чергових та позачергових виборів до органів місцевого самоврядування;

31) затвердження протягом двох днів з моменту звернення Президента України указів про введення воєнного чи надзвичайного стану в Україні або в окремих її місцевостях, про загальну або часткову мобілізацію, про оголошення окремих місцевостей зонами надзвичайної екологічної ситуації;

32) надання законом згоди на обов'язковість міжнародних договорів України та денонсація міжнародних договорів України;

33) здійснення парламентського контролю у межах, визначених цією Конституцією та законом;

34) прийняття рішення про направлення запиту до Президента України на вимогу народного депутата України, групи народних депутатів України чи комітету Верховної Ради України, попередньо підтриману не менш як однією третиною від конституційного складу Верховної Ради України;

35) призначення на посаду та звільнення з посади керівника апарату Верховної Ради України; затвердження кошторису Верховної Ради України та структури її апарату;

36) затвердження переліку об'єктів права державної власності, що не підлягають приватизації, визначення правових засад вилучення об'єктів права приватної власності;

37) затвердження законом Конституції Автономної Республіки Крим, змін до неї.

Наприкінці наведеного переліку вказується, що «Верховна Рада України здійснює також інші повноваження, які відповідно до Конституції України віднесені до її відання».

Враховуючи значення Конституції України, як Основного закону держави, розподіл напрямів повноважень, у даному випадку Верховної Ради України, за логікою розробників Конституції України, здійснювалася за ступенем важливості у відповідності до поділу державної влади згідно положень статті 6 Конституції України. Також необхідно звернути увагу на те, що під позицією 3 головних напрямів повноважень Верховної Ради України в системі державного управління визначено **«прийняття законів»**, а не **«законотворча діяльність»**. Це – з одного боку, а з іншого, народні депутати є суб'єктами законотвірчої діяльності.

Законодавчу основу організації та здійснення парламентського контролю складають Конституція України та закони України «Про Регламент Верховної Ради України», «Про комітети Верховної Ради України» та «Про статус народного депутата України», але у цих законах України відсутнє законодавче визначення поняття «парламентський контроль».

Розгляд питань, пов'язаних із здійсненням контрольних функцій Верховною радою України присвячені положення розділу VI закону України «Про Регламент Верховної Ради України» з використанням наступних механізмів:

- внесення депутатського запиту (глава 37 «Розгляд Верховною Радою України питань, пов'язаних із депутатськими запитами»);
- конституційно визначеною функцією здійснення контролю за діяльністю Кабінету Міністрів України відповідно до цієї Консти-

туції та закону (п. 13 ст. 85) (глава 38 «Розгляд питань, пов'язаних з парламентським контролем за діяльністю Кабінету Міністрів України»);

- розгляд Верховною Радою звітів і доповідей державних органів та посадових осіб (глава 38-1 «Розгляд Верховною Радою звітів і доповідей державних органів та посадових осіб (крім Кабінету Міністрів України»);
- проведення парламентських слухань (глава 39 проведення у верховній Раді України парламентських слухань);
- розгляд Верховною Радою України питання про дострокове припинення повноважень Верховної Ради Автономної Республіки Крим (глава 40 «Розгляд Верховною Радою України питання про дострокове припинення повноважень Верховної Ради Автономної Республіки Крим»)

Закон України «Про комітети Верховної Ради України» визначає, що Комітет Верховної Ради України – орган Верховної Ради України, який утворюється з числа народних депутатів України для здійснення за окремими напрямками законопроектної роботи, підготовки і попереднього розгляду питань, віднесених до повноважень Верховної Ради України, **виконання контрольних функцій** (ст. 1). Під поняттям «виконання контрольних функцій» даний Закон України розуміє: аналіз практики застосування законодавчих актів у діяльності державних органів, їх посадових осіб з питань, віднесених до предметів відання комітетів, підготовці та поданні відповідних висновків та рекомендацій на розгляд Верховної Ради України; участь за дорученням Верховної Ради України у проведенні «години запитань до Уряду»; контроль за виконанням Державного бюджету України в частині, що віднесена до предметів їх відання, для забезпечення доцільності, економності та ефективності використання державних коштів у порядку, встановленому законом; участь в організації та підготовці за дорученням Верховної Ради України парламентських слухань; організації та підготовці слухань у комітетах; взаємодії з Рахунковою палатою; взаємодії з Уповноваженим Верховної Ради України з прав людини; направленні матеріалів для відповідного реагування в межах, установлених законом, органам Верховної Ради України, державним органам, їх посадовим особам; розгляді на своїх засіданнях або під час слухань у комітеті звітів, доповідей та інформації державних органів та посадових осіб, які у передбачених законом випадках подаються до Верховної Ради України, здійсненні попередньої підготовки питань щодо розгляду на пленарному засіданні Верховної Ради України таких звітів, доповідей та інформації; здійсненні комітетом Верховної

Ради України, до предмета відання якого віднесено питання забезпечення контрольних функцій Верховної Ради України за діяльністю органів спеціального призначення з правоохоронними функціями, правоохоронних органів спеціального призначення та розвідувальних органів, передбачених цим Законом заходів з метою гарантування неухильного і безумовного дотримання цими органами вимог Конституції України щодо забезпечення національної безпеки, недопущення їх використання для узурпації влади, порушення прав і свобод людини і громадянина (ст. 14).

Саме реальна сучасність розставила акценти багатогранної діяльності Верховної Ради України. Саме дана сучасність вказала на справжню роль та місце парламентського контролю. У багатьом, завдяки оперативності та якості парламентського контролю залежить ефективність правозастосовної діяльності та правоохоронної діяльності, а також підвищення якості законотворчої діяльності.

На жаль, проглядається тенденція оцінки ефективності діяльності народного депутата України, а відповідно, і Верховної Ради України в цілому, не по конкретним справам, а по кількості внесених законопроектів, незалежно від їх суспільної корисності. Такий підхід не може не відобразитися негативно на довірі до діяльності Верховної Ради України, в тому числі і процесах підготовки та здійснення парламентського контролю.

Підтвердженням цьому може бути «Оцінка громадянами ситуації в країні, довіра до соціальних інститутів, політиків, посадовців та громадських діячів (травень 2023р.)»: Серед державних та суспільних інститутів найчастіше довіра висловлюється до Збройних Сил України (ім довіряють 93% опитаних), добровольчих загонів (86%), Президента України (83%), Національній гвардії України (83%), волонтерських організацій (82%), Державної служби з надзвичайних ситуацій (80%), Державної прикордонної служби (79%), Міністерства оборони України (75%), Служби безпеки України (66%), громадських організацій (61%), Церкви (61%), Національної поліції (59%), Голови міста (селища, села), в якому живе респондент (58%), ради міста (селища, села), в якому живе респондент (55%).

Також частіше висловлюється довіра, ніж недовіра до ЗМІ України (відповідно 49% і 37,5%), до Уповноваженого Верховної Ради з прав людини (Омбудсмена) (відповідно 46% і 28%), до Національного банку України (відповідно 46% і 37%).

Більшість респондентів висловлюють недовіру судам (судовій системі загалом) (не довіряють 70%), політичним партіям (69%), державному апарату (чиновникам) (66%), прокуратурі (58%), комерційним банкам (56%), **Верховній Раді України (55%)**.

На основі викладеного вище вважаємо за доцільне **запропонувати**:

1. Розглянути питання впровадження законодавчо визначеного поняття терміну «парламентський контроль», а також більш чіткого законодавчо визначеної ролі та місця парламентського контролю в національній системі публічного контролю, його взаємозв'язку із іншими видами публічного контролю з урахуванням законодавчого врегулювання імплементації міжнародних правових стандартів щодо здійснення парламентського контролю відповідно до участі України в міжнародних організаціях, прийнятих міжнародних зобов'язань.

2. У законах України «Про Регламент Верховної Ради України» та «Про комітети Верховної Ради України» доцільно розглянути питання посилення наголосу на значимості місця та значимому відсотковому зростанню в загальній системі депутатської діяльності здійснення складного процесу парламентського контролю, як одного з головних показників народовладдя та оцінки ефективності діяльності, як конкретного народного депутата, так і Верховної Ради України в цілому. В статті 85 Конституції України серед **37** головних напрямів повноважень Верховної Ради України в системі державного управління здійснення парламентського контролю знаходиться на **33** місці. Конституція України є Основним законом держави тому ставити питання внесення змін подібного роду недоцільно, а згадані закони України є «робочими».

Список використаної літератури

1. Конституція України, *Відомості Верховної Ради України (ВВР)*, 1996, № 30, ст. 141, URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

2. Про Регламент Верховної Ради України: Закон України від 10.02.10 р. № 1861-VI, редакція від 31.03.23 р. URL: <https://zakon.rada.gov.ua/laws/show/1861-17#Text>

3. Про комітети Верховної Ради України: Закон України від 04.04.95 р. № 116/95-ВР, редакція від 31.03.23 р. URL: <https://zakon.rada.gov.ua/laws/show/116/95-%D0%B2%D1%80#Text>

4. Оцінка громадянами ситуації в країні, довіра до соціальних інститутів, політиків, посадовців та громадських діячів (травень 2023р.) URL: <https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/otsinka-gromadianamy-sytuatsii-v-kraini-dovira-do-sotsialnykh-institutiv-politykiv-posadovtsiv-ta-gromadskykh-diiachiv-traven-2023r>

Корж І. Ф.

доктор юридичних наук, старший науковий співробітник, заступник керівника наукового центру електронного парламенту та правової інформації Державної наукової установи «Інститут інформації, безпеки і права НАПрН України»

ПРОБЛЕМИ ДОСТУПУ ДО НОРМАТИВНО-ПРАВОВОЇ ІНФОРМАЦІЇ В СУЧАСНИХ УМОВАХ

Якщо звернутися до терміну «демократія», який в сучасних умовах є орієнтиром розвитку суспільств, то наукові довідники в ньому вбачають такий державницький лад, що ґрунтується на принципі народовладдя (грец. Δημοζ – народ, і κρατοζ – влада), і який забезпечує формування державного управління шляхом виборів та відповідальності влади перед народом. Таке врядування має забезпечуватися законом через забезпечення прав громадян – передусім виборчого права та свободи слова [1]. При цьому управління державою здійснюється народом, безпосередньо (пряма демократія), або через обраних представників (представницька демократія) [2, с.227].

Тим самим демократична держава покликана забезпечити весь комплекс прав людини і громадянина, передбачених чинним законодавством в усій багатоманітності їх прояву: закріплених як у Конституції України (особистих, політичних, соціально-економічних, соціально-культурних тощо), так і в галузевих актах. Реалізація і гарантування усього комплексу цих прав є головною формою здійснення демократії.

Особливо важливе значення в сучасних умовах набуває принцип знання громадянами своїх прав, а також обов'язків державної влади щодо їх забезпечення. І права громадян, і обов'язки державної влади щодо їх забезпечення набувають свого зовнішнього виразу через висвітлення відповідних нормативно-правових актів. Тобто, саме в нормативно-правових актах знаходять свій вираз і права, і обов'язки та їх впровадження та забезпечення, при цьому обов'язливі. З огляду на зазначене громадяни просто зобов'язані знати нормативно-правові акти, в яких визначаються як права, так і обов'язки сторін.

Відповідно до статті 57 Конституції України [3] закони та інші нормативно-правові акти, що визначають права і обов'язки громадян, мають бути доведені до відома населення у порядку, встановленому законом. Закони та інші нормативно-правові акти, що визначають права і обов'язки

громадян, не доведені до відома населення у порядку, встановленому законом, є нечинними. Тобто, перед державою поставлено завдання виконати важливий обов'язок – забезпечити доведення до відома громадян зміст законів та інших нормативно-правових актів, що визначають їхні права і обов'язки. Це свідчить про те, що держава має бути готова забезпечити виконання та дотримання законних прав громадян. А показником реалізації зазначеного є наявність розвинутого громадянського суспільства, яке є невід'ємною складовою всіх демократичних правових держав світу.

Тим паче, положення Конституції України, а саме її частина друга статті 68 [3] зазначає, що «незнання законів не звільняє від юридичної відповідальності». Тим самим ця частина Конституції генерує подвійний обов'язок щодо необхідності знання нормативно-правових актів: з одного боку зобов'язує громадян знати свої права і обов'язки, невиконання яких, насамперед обов'язку для громадян, може призвести до їхньої юридичної відповідальності; з іншого боку зобов'язує державну владу довести до громадян зміст нормативно-правових актів, що має забезпечити їх виконання громадянами і виникнення права влади діяти із застосуванням примусу громадян до їх виконання та притягнення, за необхідності, до юридичної відповідальності громадян у разі допущення правопорушення.

Зазначимо, що у розвинутих, демократичних країнах світу забезпечення громадянам доступу до публічної інформації є основним індикатором відкритості публічної влади. На сьогодні в Україні багато зроблено для створення умов доступу громадян до нормативно-правових актів. З цією метою в Україні впроваджено та функціонує ряд електронних баз нормативно-правових актів, що створює відповідні умови для доступу громадян до них.

Нині, незважаючи на воєнний стан в Україні, активно розвиваються інформаційно-пошукові системи, онлайн-консультації, інтернет-ресурси та бази даних, різні реєстри що значно полегшує роботу як правників, посадових і службових осіб органів державної влади, так і представників бізнесу та пересічних громадян. Так існують платні і безоплатні правові інформаційно-пошукові системи, найбільш популярні з яких є:

- платна спеціалізована інформаційно-правова система «Ліга: Закон» (<https://www.softcom.ua/ua/liga/system/liga-zakon.php>) з відповідними своїми системами (платформами) ІПС LIGA:ZAKON; LIGA 360: Бухгалтер; LIGA 360: Юрист; LIGA 360: Керівник; LIGA 360: HR; LIGA 360: PR; VERDICTUM; CONTR AGENT. Дана інформаційна система дозволяє з легкістю виявляти і ви-

вчати не тільки Законодавство України, а й інформаційну правову базу зарубіжних країн. А це просто необхідно представникам ділових кіл, які займаються або планують зайнятися зовнішньоекономічною діяльністю;

- правова інформаційно-пошукова система «Нормативні акти України» (НАУ, <http://www.nau.kiev.ua/>). Функціонує трьома мовами – українською, російською, англійською. На даний час не працює;
- платний програмний комплекс «Експерт-Юрист» (<http://www.expertsoft.com.ua/laws/>). База даних містить нормативні акти, видані органами влади України, СРСР (існують документи органів влади колишнього СРСР щодо України), а також документи міжнародного характеру;
- сайт (офіційний портал) Верховної Ради України (<https://zakon.rada.gov.ua/>) – офіційна інтернет-сторінка, яка містить в собі перелік проектів законодавства, саме Законодавство та Тезаурус «EUROVOC» (Українська), а також міжнародні акти;
- Єдиний державний реєстр нормативно-правових актів (www.reestrna.gov.ua) Міністерства юстиції України. Є довгостроковим проектом розвитку системи надання правової інформації в Україні. Функціонування даного Реєстру забезпечує офіційність, достовірність, контрольність, актуальність і повноту правової інформації, яка надається юридичним та фізичним особам, що позитивно впливає на підвищення правової свідомості та правової культури громадян.

Окрім нормативно-правових актів вищих та центральних органів державної влади, є ще і локальні (місцеві) акти органів самоврядування, які висвітлюються на їхніх офіційних веб-сайтах.

На нашу думку забезпечення вільного доступу до нормативно-правових актів має розумітись у тому числі і як його безоплатність для громадян. За умов децентралізації нинішньої державної влади обов'язок надання правової інформації шляхом організації вільного доступу до відповідних реєстрів нормативно-правових актів має забезпечуватись органами місцевого самоврядування. У той же час, якщо розуміти реалізацію зазначеної функції у контексті всієї діяльності держави та її органів, то повинна бути створена та діяти Єдина централізована система, що забезпечує ведення та доступ користувачів до реєстрів нормативно-правових актів на рівні усієї України (Національний рівень), відповідні ресурси органів місцевого самоврядування повинні входити до такої системи.

В контексті проведення реформи децентралізації питання доступу до нормативно-правової інформації, яка створюється органами місцевого самоврядування, набуває додаткової актуальності, тому, що на місцевий рівень передано додаткові повноваження та ресурси внаслідок чого кількість рішень, що приймають органи та посадові особи на місцевому рівні значно збільшується. Таким чином, є актуальним питання створення єдиної бази нормативно-правової інформації державних та органів місцевого самоврядування.

Для України, створення національної системи нормативно-правових актів не є проблемою. Адже, на сьогодні існує більше десятка нормативно-правових електронних систем і баз даних, як державних органів, так і приватних, які на безоплатній або оплатній основі надають відповідні інформаційні послуги. Крім того є відповідний європейський досвід у цьому питанні.

Україна має передумови для створення своєї національної консолідованої системи нормативно-правових актів. Її можна створити двома шляхами:

- перший, створити спеціалізований, консолідований веб-портал, який поєднає в собі систему веб-порталів органів державної влади та регіональних органів місцевого самоврядування. Ведення такого порталу та його наповнення доручити Міністерству цифрової трансформації чи Міністерству юстиції України;
- другий, використати веб-портал Верховної Ради України, який вже є наполовину консолідованим порталом, оскільки інтегрований до веб-порталів органів державної влади і містить в собі нормативно-правові акти усіх органів державної влади. Залишилося лише його доопрацювати та інтегрувати до нього веб-портали регіональних органів місцевого самоврядування (муніципальні веб-портали). Його ведення та наповнення продовжувалося б Апаратом парламенту за нинішнього сприяння Державної наукової установи «Інституту інформації, безпеки і права Національної академії правових наук України [4].

Другий шлях видається більш прагматичним і менш затратним, більш ефективним для громадян України та для власників веб-порталів публічної влади. І це був би лише перший крок. А наступним було б доцільним інтегрувати згаданий портал з веб-порталами Європейського Союзу, що цілковито є реальним. Саме через головний представницький веб-портал було б доцільно поєднати національну та європейську системи правової інформації. Як піде розвиток цього процесу – покаже час. Відповідні пропозиції Інститутом направлені.

Список використаних джерел

1. Демократія. Енциклопедія сучасної України. Encyclopedia of Modern Ukraine. URL: <https://esu.com.ua/article-21478> (дата звернення: 01.04.2023).
2. Демократія. Політологічна енциклопедія. Навчальний посібник Книга II / Укладачі: Карасевич А. О., Шачковська Л. С. Умань.: ПП Жовтий О. О., 2016. 560 с. URL: <https://dspace.udpu.edu.ua/bitstream/6789/5265/1/%d0%a5%d1%80%d0%b5%d1%89%d0%b5%d0%bd%d0%bd%d1%8f%202.pdf> (дата звернення: 01.04.2023).
3. Конституція України: Закон України від 28 червня 1996 р. №2254к/96-ВР / Верховна Рада України. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
4. Корж І. Ф., Ланде Д. В., Лихоступ С. В. Консолідована система нормативно-правової інформації в умовах децентралізації державної влади в Україні – невід’ємна складова демократії: моног.Київ; Одеса : Фенікс, 2020. 388 с.

Ланде Д. В.

*доктор технічних наук, професор,
керівник наукового центру правової
інформації Державної наукової
установи «Інститут інформації,
безпеки і права НАПрН України»
ORCID: 0000-0003-3945-1178*

СЕМАНТИЧНЕ ІНДЕКСУВАННЯ ДОКУМЕНТІВ В ГАЛУЗІ ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ

Системи генеративного штучного інтелекту (СГШІ), такі як ChatGPT (<https://chat.openai.com/>), стають все більш поширеними в різних галузях. Можливості у виділенні основних концепцій та іменних сутностей роблять ChatGPT корисним у фактографічних системах, зокрема в медицині та економіці [1]. СГШІ з зовнішніми системами, такими як геоінформаційні [2], системи аналізу та візуалізації графіків і мереж. В роботі [3] показано, як можна створювати мережі зв’язків між персонажами літературних творів.

Такі СГШІ, як ChatGPT, зазвичай називають великими мовними моделями (LLM). Ці системи використовують глибоке навчання та моделі генерації мови для створення зрозумілих людині відповідей на текстові

запити. Вони тренуються на великих обсягах даних (Big Data). Принципи роботи таких систем включають розуміння тексту, генерацію відповідей та покращення якості моделі за допомогою зворотного зв'язку та додаткового навчання.

Мета роботи – є представлення нових можливостей обробки правової інформації із застосуванням систем генеративного штучного інтелекту, зокрема, ChatGPT, для вирішення задач семантичного індексування і побудови семантичних мап, що дозволяє розглядати такі системи як корисний аналітичний інструмент в галузі права, зокрема, для здійснення парламентського контролю.

Доповідь присвячена опису методики семантичного індексування і створення каузальних мереж, отриманих шляхом багаторівневої декомпозиції поняття «Парламентський контроль» за допомогою системи ChatGPT, а також візуалізації та аналізу цих мереж за допомогою спеціально створеної програми LegalGraph (<https://bigsearch.space/legal.html>). Сформовану мережу можна розглядати як семантичну карту, де кожен її вузол або зв'язок є гіперпосиланням, що веде до юридичної пошукової системи.

Парламентський контроль – це система, яка дозволяє парламентарям контролювати діяльність уряду. Ця система є важливою для забезпечення прозорості та підзвітності уряду перед народом [4]. Загалом, парламентський контроль на базі СГШ має потенціал для революціонізації сфери парламентського контролю. Ця технологія може допомогти парламентарям бути більш ефективними та прозорими, а також може допомогти їм приймати більш обґрунтовані рішення. Для того, щоб мінімізувати ризики застосування СГШ, необхідно розробити чіткі правила щодо використання. Ці правила повинні враховувати такі аспекти, як прозорість, відповідальність та справедливість.

Основна проблема, яка виникає при створенні семантичних карт, полягає в тому, що зазвичай для цього потрібні великі ресурси та залучення експертів. Запропонований підхід створення рою віртуальних експертів [5] може суттєво спростити і прискорити цей процес.

Формування семантичної мапи

Прикладом моделі предметної області «Парламентський контроль», в якості якої можна представити мережевий масив даних, який буде зручним для обробки комп'ютером, є направлена зважена мережа термінів. Якщо нас цікавить проблематика парламентського контролю, тому треба запросимо у сервісу ChatGPT декомпозиувати це поняття і видати відомі їй часткові поняття, що складають суть парламентського контр-

олно. Тобто центральним вузлом майбутньої мережі має стати поняття «Парламентський контроль». Після цього для кожного такого часткового поняття також здійснюється декомпозиція. Такий процес може тривати нескінченно, але в роботі зупинимося лише на трьох рівнях. Незважаючи на ієрархічне формування такої мережі, вона загалом не буде строго ієрархічною структурою, а скоріше квазіієрархічною. Деякі часткові поняття при декомпозиції різних понять можуть співпадати.

Найчастіше при використанні ГСШ сутності або пари сутностей (а саме це потребується при побудові мережевих структур) можна витягувалися безпосередньо з навченої моделі системи. Промпт для виявлення сутностей – результатів декомпозиції основного поняття може мати такий вигляд:

ГСШ видає відповідь такого вигляду:

Система ChatGPT може надати різні відповіді під час обробки тексту в різний час, і всі вони розумні з точки зору людської логіки. Кожну з цих відповідей можна сприйняти як відповідь штучного експерта. Узагальнивши відповіді багатьох таких експертів, можна отримати більш повну і точну відповідь. Тому наведений промпт можна задати системі декілька разів, запустивши тим самим «рій віртуальних агентів». Багаторазове виконання дозволяє отримати різні відповіді, багато з яких співпадуть. Із статистичного погляду, – це самі достовірні результати. У разі розгляду первинного поняття «Парламентський контроль», отримуємо такі поняття, як «ПАРЛАМЕНТ», «КОНТРОЛЬ», «НАГЛЯД», «ВИКОНАВЧА ВЛАДА», «ЗВІТНІСТЬ» тощо.

Після виконання першого етапу – отримання результату декомпозиції, для кожного із отриманих часткових понять здійснюється подальша декомпозиція за допомогою промπτів типу:

При цьому система ChatGPT може допомогти отримати зміст CSV-файлу (поля, розділені точкою з комою), а саме:

ВИКОНАВЧА ВЛАДА; ВИКОНАННЯ ЗАКОНІВ

ВИКОНАВЧА ВЛАДА; РЕГУЛЮВАННЯ ГАЛУЗЕЙ ГОСПОДАРСТВА

ВИКОНАВЧА ВЛАДА; РОЗРОБКА ТА ВИКОНАННЯ БЮДЖЕТУ

ВИКОНАВЧА ВЛАДА; ЗОВНІШНІ СПРАВИ

ВИКОНАВЧА ВЛАДА; НАЦІОНАЛЬНА БЕЗПЕКА

...

Такого типу відповіді можуть слугувати інформаційною основою для побудови графових структур — семантичних мапа, які одночасно є джерелом посилань, тому що кожний вузол і кожний зв'язок цієї мережі містить гіперпосилання на відповідні запити до пошукової систем порталу

Верховної Ради України (<https://zakon.rada.gov.ua/laws>). Кожне екстраговане поняття може розглядатись як вузол мережі. Крім того, з подібним промтом можна звернутися до декількох систем штучного інтелекту, серед яких ChatGPT, Bard (<https://bard.google.com/chat>), GPT Free (<https://gptfree.co>) тощо.

Аналіз і візуалізація семантичної мапи

Аналіз мереж є важливим методом для розуміння взаємозв'язків між об'єктами та виявлення зв'язків між ними, що може значно полегшити дослідження конкретної сфери. Для проведення аналізу та візуалізації мереж, спільно з системами, подібними до ChatGPT, можна використовувати сучасні графові інструменти, такі як Gephi [7]. Однак при використанні таких програмних продуктів аналітики стикаються з двома труднощами: потребою встановлення програм, що не завжди можливо, особливо при обмеженнях на встановлення стороннього програмного забезпечення, та потребою досконально вивчити особливості функціонування цих систем, розібратися в численних параметрах, режимах розміщення графів, кластеризації тощо.

Для вирішення цих проблем на основі бібліотеки системи GrahViz розроблено програму LegalGraph, доступного наразі в Інтернет за адресою <https://bigsearch.space/legal.html>. Ця програма забезпечує первинний аналіз і відображення графів, інформація про які відповідає формату CSV (від англ. Comma-Separated Values – значення, розділені комою), кожен запис в якому відповідає парі сутностей. При цьому кожному вузлу і ребру графа у відповідність ставиться гіперпосилання на законодавчу базу даних, розміщену в Інтернеті.

На Рис. 1 показано результат — фрагмент семантичної мапи предметної області «Парламентський контроль», який було сформовано на ресурсів сервісу ChatGPT. Як бачимо, ця мережа квазієрархічна, до вузлів, що поєднують різні часткові поняття, тобто є транзитними, відіграють особливу роль в процесі парламентського контролю виявилися такі: «КОНТРОЛЬ ЗА ВИКОНАВЧОЮ ВЛАДОЮ»; «ЗВІТНІСТЬ ВИКОНАВЧОЇ ВЛАДИ»; «ПАРЛАМЕНТСЬКІ СЛУХАННЯ»; «АУДИТ БЮДЖЕТНИХ ВИТРАТ» тощо.

Програмою формується відображення орієнтованих графів, вузли ранжуються за ступенем і розфарбовуються, визначається товщина і напрямок ребер. При цьому формується зображення графа у форматі SVG, що дає можливість формувати гіперпосилання, що ведуть до пошукових форм системи Верховної Ради України. з вузлів і ребер графа. Реалізація гіперпосилань надає можливість перегляду нормативних документів,

які, з одного боку надає інформаційне розкриття поняття або зв'язку, а з іншого, підтверджує коректність побудови семантичної мапи.

Висновки

Створення семантичної мапи на основі технології генеративного штучного інтелекту і системи LegalGraph може допомогти юристам при використанні правових знань при здійсненні парламентського контролю завдяки зручному доступу до інформації; структуруванні та візуалізації знань; зв'язкам між різними сутностями і документами.

Використання методики семантичного індексування і формування семантичних мап може сприяти покращенню рівня парламентського контролю завдяки зручному охопленню всієї понятійної бази і швидкому доступу до відповідної нормативно-правової інформації.

Рисунок 1 – Фрагмент мережі понять, що відповідають тематиці «Парламентський контроль»

Використана література

1. Lande, Dmitry and Strashnoy, Leonard, Concept Networking Methods Based on ChatGPT & Gephi (April 17, 2023). SSRN. Available at <http://dx.doi.org/10.2139/ssrn.4420452>
2. Tamilla Triantoro. Graph Viz: Exploring, Analyzing, and Visualizing Graphs and Networks with Gephi and ChatGPT (March 30, 2023). ODSC Community. Available at <https://opendatascience.com/graph-viz-exploring-analyzing-and-visualizing-graphs-and-networks-with-gephi-and-chatgpt/>
3. Solat J. Sheikh, Sajjad Haider, Alexander H. Levis, On semi-automated extraction of causal networks from raw text, Engineering Applications of Artificial Intelligence, Volume 123, Part A, 2023, 106189, ISSN 0952-1976, <https://doi.org/10.1016/j.engappai.2023.106189>.
4. Інформатика парламентського контролю : посібник / Д. В. Ланде, В. М. Фурашев, С. М. Брайчевський. – Київ 2022. – 256 с. ISBN 978-966-2344-80-6
5. Dmytro Lande, Leonard Strashnoy. GPT Semantic Networking: A Dream of the Semantic Web – The Time is Now – Kyiv: Engineering, 2023. – 168 p. ISBN 978-966-2344-94-3.
6. Ken Cherven. Mastering Gephi Network Visualization. – Packt Publishing, 2015. ISBN 78-1-78398-734-4.

Брайчевський С. М.

*кандидат фізико-математичних
наук провідний науковий співробітник
Державної наукової установи
«Інститут інформації, безпеки і права
НАПрН України»*

ШТУЧНИЙ ІНТЕЛЕКТ ТА АНАЛІЗ МЕРЕЖЕВОГО КОНТЕНТУ У ПАРЛАМЕНТСЬКОМУ КОНТРОЛІ

Парламентський контроль як особлива форма державного контролю за діяльністю органів виконавчої влади та посадових осіб є особливо актуальним в наших умовах, в першу чергу, через два ключові чинники. Перший – це програма децентралізації [1], яка вже кілька років успішно проводиться в Україні і призводить до перерозподілу повноважень між різними органами. Другий – воєнний стан, який передбачає певні обмеження громадянських прав і свобод, а отже знижує рівень контролю за діяльністю влади з боку громадських організацій та фізичних осіб. Парламентський контроль в цих складних умовах повністю зберігає свої можливості, а отже і ефективність.

З іншого боку, технічні можливості парламентського контролю стрімко зростають в контексті цифрової трансформації [2] українського суспільства. Адже сучасні цифрові технології дозволяють на практиці здійснювати те, що ще кілька років тому виглядало нездійсненними мріями.

Останні досягнення в сфері інформаційних технологій дозволяють ставити питання про використання штучного інтелекту в практичній площині. Нижче ми обговоримо один із можливих напрямків в цій сфері.

Очевидно, що виключно важливу роль в плані здійснення парламентського контролю відіграють генерація і споживання публічної інформації [3]. Дійсно, оскільки правопорушення не афішуються самими порушниками, джерелом відомостей про них, як правило, є різноманітні публікації щодо їхніх наслідків.

Одним з важливих напрямків досліджень в цій сфері, на нашу думку, є аналіз мережевого контенту. Останнім часом ми бачимо, що сучасному суспільстві мережеві технології набувають все більшого і більшого значення не лише в плані суспільних комунікацій, але й в загальних інформаційних процесах. Мережеві інформаційні ресурси швидко стають основою збирання, накопичення обробки та поширення інформації. Мережні інструментальні засоби відкривають все більш широкий доступ до різноманітних джерел, в тому числі і тих, що традиційно відносяться до категорії корпоративних. Тепер часто електронну копію документа про-

стіше знайти в мережі, ніж його оригінал в бібліотеці чи іншому сховищі друкованих матеріалів. І цьому не в останню чергу сприяє те, що доступ до мережі знаходиться у нас, безпосередньо на робочому місці.

Тому не дивно, що мережеві інформаційні ресурси стають основним джерелом формування картини світу. А це, в свою чергу, означає, що ми, аналізуючи мережевий контент, можемо отримати практично всі відомості щодо потрібної нам теми.

З сучасної точки зору соціальні комунікації являють собою складне явище, що містить ряд компонентів різної природи [5-6]. Але для нас важливо те, що в їхній основі завжди лежить процес обміну інформацією в різноманітних формах, в тому числі електронних. І тією мірою, як в наше життя впроваджуються нові інформаційні технології, вони починають грати все більшу роль в комунікативних процесах.

З технічного боку в сфері аналізу мережевого контенту існує дві основні проблеми. Перша пов'язана з його структурою, а друга – з його обсягом.

Проблема структури мережевого контенту полягає в тому, що він містить інформацію різного рівня структуризації і в різному форматі. Ця обставина вкрай ускладнює машинну обробку даних, які ми можемо отримати безпосередньо з мережевих ресурсів. Частково ми торкалися цієї проблеми в [4].

Для ілюстрації зупинимся на одному аспекті даної проблеми: наявності принципово різних одиниць інформації. Як конкретний приклад наведемо якісну різницю між характером новинної інформації та вмісту соціальних мереж.

Основною інформаційною одиницею новин є документ. Ми не будемо заглиблюватися в строге визначення цього поняття, а скажемо лише (для нас саме це є важливим), що документ являє собою цілісний інформаційний продукт, призначений для кінцевого використання будь-яким споживачем. Він має загальні структурні елементи (автор, заголовок, анотація, основний текст, дата публікації, джерело тощо), наявність яких ми очікуємо і легко розпізнаємо за типовими засобами форматування. З точки зору змісту головним для нас є те, що документ (розрахований на довільного споживача) має мінімальну контекстну залежність: щоб його зрозуміти, нам достатньо лише орієнтуватися в загальній суспільній ситуації. Документ або взагалі не передбачає знання інших документів, або (якщо воно бажане), як правило, надає споживачеві можливість ознайомитися з ними за допомогою гіперпосилань. Зауважимо також, що активне використання гіпертексту у вигляді гіперпосилань є важливою особливістю мережевих ресурсів. Таким чином, аналіз документальних

масивів якщо і викликає труднощі, то в основному технічного характеру. Адже контент документів генерується так, щоб забезпечити максимальну ефективність сприйняття змісту.

Інформаційною одиницею соціальних мереж є пост. Він, взагалі кажучи, являє собою довільний фрагмент тексту, що не має акцентованих початку та кінця, а також характерних структурних елементів, типових для документів (автор, заголовки тощо). Прикладом може бути, скажімо, «Супер! Підтримую!». Безперечно, цей текст несе в собі зміст, можливо навіть суттєвий. Але навряд, чи довільний споживач його зрозуміє.

На відміну від документа окремий пост не повинен мати визначений змісту. За певних умов пост, фактично, може бути документом (тобто повноцінний документ автор може викласти в соціальну мережу). Але разом з тим існує значний за обсягом сегмент контенту соціальних мереж, який містить набори взаємопов'язаних постів, що реалізують обговорення тієї чи іншої теми кількома учасниками. В цьому сегменті зміст мають неперервні ланцюжки постів, часто різних авторів. Кожна ланка такого ланцюжка є реакцією на попередні пости, а всі вони разом взяті формують специфічний контекст. Тому такі пости є контекстно залежними. І головна складність полягає в тому, що ми не можемо визначити ступінь такої залежності. Іншими словами, для повноцінного аналізу такого контенту нам необхідно відстежувати послідовності постів (змістовні ланцюжки), які мають окреслені початок і кінець, але при цьому можуть формуватися групою незалежних один від одного авторів. А це доволі складна задача. Нажаль, вона суттєво ускладнюється обсягом даних.

Проблема обсягу інформації добре відома – він настільки великий, що її практично неможливо зібрати й обробити людиною, навіть колективно фахівців. При значному збільшенні кількості працівників неможливо забезпечити належну координацію їх дій, а отже неодмінно буде втрачена цілісність бачення окремої ситуації. Тому для опрацювання публічної інформації так чи інакше необхідно застосовувати сучасні інформаційні технології.

Функціональні можливості стандартних технологій обмежені тим, що при обробці інформації використовуються виключно формальні методи, наприклад фільтрація даних за наявністю (відсутністю) окремого слова або групи слів, що мають одне й те саме значення. Але часто зміст тексту не зводиться до прямого значення слів, з яких він складається. Так, наприклад, вислів «від радості злетів до небес» не можна сприймати буквально. Щоб отримати справжні відомості, які містяться в тексті, потрібно його розуміти. А розуміння як таке не досягається формальними засобами.

Є підстави вважати, що розуміння змісту даних, принаймні в деякому сенсі, може бути досягнуто в системах штучного інтелекту. Зараз нас не цікавить, як саме досягається таке розуміння і в чому полягає його природа. Для усвідомлення загальної ідеї можемо запропонувати простий тест, який наочно ілюструє роботу машини, здатної до розуміння повідомлень. Нехай маємо деяку чорну скриню, за роботою якої спостерігає експертна група фахівців в певній предметній області. На вхід чорної скрині подається текст, що відноситься до даної предметної області та, на думку членів експертної групи, має цілком визначений конкретний зміст. Цей зміст надає можливість зробити вибір довільної кількості елементів із загального їх набору і ранжувати їх за ступенем відповідності поставленій задачі (постановка якої також міститься в тексті). Передбачається, що в тексті в явному вигляді відсутні можливі варіанти вибору. Чорна скриня виводить послідовність чисел, що визначають номери елементів в порядку ранжування. Такий самий вибір роблять фахівці з експертної групи. Будемо вважати, що машина розуміє текст, якщо її результат в середньому збігатиметься з результатами експертів. Як саме машина це робить, для нас значення не має.

В нашому випадку це означає, що машина може, отримавши довільний текст, дати йому правову оцінку шляхом вибору одного або кількох (залежно від задачі) варіантів характеристики певної правової ситуації.

Саме така постановка задачі, на наш погляд, широкі перспективи в сфері аналізу мережевого контенту.

Література

1. Реформа децентралізації. <https://www.kmu.gov.ua/diyalnist/reformi/efektivne-vryaduvannya/reforma-decentralizaciyi> (дата звернення 21.04.2023)
2. Цифрова трансформація. <https://www.kmu.gov.ua/diyalnist/mizhnarodna-dopomoga/coordination/cifrova-transformaciya> (дата звернення 21.04.2023)
3. ЗАКОН УКРАЇНИ Про доступ до публічної інформації (Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314) URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text> (дата звернення 21.04.2023)
4. Брайчевський С. М. Уніфікація структури правової інформації в умовах децентралізації. Матеріали Першої «Парламентський контроль в умовах децентралізації державної влади та цифрової трансформації в Україні: стан та проблеми» 30 березня 2021 року. Київ. С. 40-43. URL: http://ippi.org.ua/sites/default/files/zbirnik_tez_konferenciyi__30.03.2021_0.pdf (дата звернення 21.11.2022)

5. Різун В. В. Начерки до методології досліджень соціальних комунікацій. Психолінгвістика. 2012. Вип. 10. С. 305-314. URL: http://nbuv.gov.ua/UJRN/psling_2012_10_44 (дата звернення 14.11.2022)

6. Холод О. М. Соціальні комунікації: соціо- і психолінгвістичний аналіз. 2011. Львів: ПАІС/ 2011. 288 с. URL: <http://194.44.152.155/elib/local/sk784391.pdf> (дата звернення 14.11.2022)

Vitalii Andreichuk

*Candidate of Sciences in Public
Administration Research Scientist of the
International Research and Training
Center of Information Technologies and
Systems of the National Academy of
Sciences of Ukraine and the Ministry of
Education and Science of Ukraine*

APPLICATION OF ARTIFICIAL INTELLIGENCE METHODS IN THE TASKS OF PARLIAMENTARY CONTROL IN MODERN CONDITIONS

The use of artificial intelligence techniques can be useful in many aspects of parliamentary oversight, including information analysis, data discovery and analysis, and monitoring government performance.

One of the main aspects of parliamentary oversight is analyzing the large amount of information that comes to parliament. Artificial intelligence techniques, such as machine learning and natural language processing, can help identify key topics and priorities that require parliamentary attention, as well as save time and effort.

Another important aspect of parliamentary oversight is data discovery and analysis. AI techniques can help to automatically collect and analyze data from various sources, such as social media, news sites, and government databases, allowing parliamentarians to draw informed conclusions.

Finally, AI methods can be useful for monitoring government activities. For example, analyzing video recordings of government meetings can help identify problems with compliance with procedures and rules, as well as illegal behavior.

However, it is worth noting that the use of artificial intelligence methods in parliamentary oversight should be done with due regard to ethical and legal aspects. These methods should not violate the privacy of citizens

and parliamentary officials and should be used only to support democratic processes and protect human rights.

Some examples of the use of artificial intelligence methods in parliamentary oversight tasks in the world.

Artificial intelligence (AI) can be used to support parliamentary functions [1].

For example, in France, in February 2021, the Parliamentary Commission on Digital Transformation was established to study and recommend the use of AI and other digital technologies in parliamentary oversight. The French Parliamentary Assembly uses AI robots to support the work of MPs. The robots provide automatic speech recognition and translation of texts into different languages, as well as analyze large amounts of data.

In Finland, the Parliamentary Working Group on Artificial Intelligence was established in 2019 to research and develop recommendations on the use of AI in parliamentary control.

And in the UK, a new Science and Technology Select Committee was established in September 2020 to research and recommend the use of AI and other new technologies in the parliamentary process. AI tools are used to automatically analyze information on legislative activities, as well as to detect misconduct by MPs.

AI is also used in the legislative process in many legislative bodies around the world [2].

For example, in Canada, in 2018, the Center for Parliamentary Science was established to offer AI tools to help parliamentary committees understand complex issues. The AI tools are used to analyze parliamentary sessions, video materials from meetings, and committee reports. AI models help to identify key topics discussed in the parliament and determine the attitude of MPs to these topics.

In Japan, a program was launched in 2020 that uses AI to analyze transcripts of parliamentary meetings and automatically create summary documents. AI tools are used to analyze government reports and legislative documents. AI models help to quickly find key phrases and information related to specific topics.

In the United States, machine learning methods are used to analyze a large number of bills under consideration in Congress. AI models are used to predict the chances of success of bills and to identify political trends. There are also studies on AI in parliaments that look at projects and innovations [3].

These examples show that parliaments around the world are beginning to use AI methods to improve their performance and understanding of complex issues under consideration.

The main stakeholders in the application of artificial intelligence methods in the tasks of parliamentary control in Ukraine can be:

- The Verkhovna Rada of Ukraine – as a legislative body, it is interested in using the latest technologies to improve the efficiency and quality of the Parliament’s work.
- Committees of the Verkhovna Rada of Ukraine – responsible for conducting parliamentary control over the activities of the government and other executive bodies, so they may be interested in using AI methods to improve the efficiency of their work.
- The Government of Ukraine – responsible for the implementation of laws and decisions of the Verkhovna Rada, so it may be interested in using AI methods to improve control over its activities and increase their efficiency.
- Ministry of Digital Transformation of Ukraine – responsible for the development and implementation of information technologies, including AI.
- The State Service of Special Communications and Information Protection of Ukraine, which is responsible for data protection and cybersecurity.
- State Statistics Service of Ukraine – responsible for collecting and processing statistical information that can be used for parliamentary oversight.
- The National Academy of Sciences of Ukraine and higher education institutions may conduct research in the field of AI application in parliamentary oversight and train specialists in this area.
- Civil society organizations and experts – may be interested in monitoring the activities of the government and other executive authorities, and therefore may act as stakeholders in the application of AI methods in parliamentary oversight tasks.
- IT companies and startups that develop and implement artificial intelligence systems.

The conditions of martial law require a more efficient and prompt response to complex and unpredictable situations that arise. The use of artificial intelligence methods in the tasks of parliamentary control can be an important tool for increasing the efficiency and responsiveness of response to such situations.

Artificial intelligence can help automate the process of collecting and analyzing a large amount of data that is important for decision-making under martial law. For example, artificial intelligence can help track and analyze information on troop movements, armed conflicts, the state of the economy,

and other social processes, which can help respond to situations faster and more efficiently.

In addition, the use of artificial intelligence methods can provide more accurate and objective data analysis, which can help avoid erroneous conclusions and decisions. For example, artificial intelligence can be used to automatically identify risks and predict the consequences of various decisions.

Thus, the use of artificial intelligence methods in the tasks of parliamentary control can be an important tool for increasing the efficiency and responsiveness of response to complex and unpredictable situations that arise under martial law.

Artificial intelligence methods can be used in the tasks of parliamentary control in the post-war reconstruction of Ukraine for various purposes, for example

- Monitoring corruption risks: Machine learning and data analysis techniques can be used to identify where the greatest risks of corruption and malpractice in public administration and governance are, which can help the parliament take appropriate measures to prevent them.
- Monitoring social issues: AI can be used to analyze social data to identify problem areas, for example, in healthcare, housing and utilities, education, social protection, etc.
- State budget analysis: AI methods can be used to analyze the distribution of public funds and determine the effectiveness of government programs, which can help parliament make better decisions on budget policy.
- Document flow automation: AI can be used to automate the processing of a large number of documents, which helps to reduce the labor intensity of the process and increase the speed of work.

Thus, artificial intelligence methods can be a useful tool to support parliamentary control in the current conditions of martial law and in the post-war reconstruction of Ukraine, which contributes to more efficient and transparent governance.

List of references

1. Ziouvelou, Xenia & Giannakopoulos, George & Giannakopoulos, Vassilis. (2022). Artificial Intelligence in the Parliamentary Context. In book: Smart Parliaments Data-Driven Democracy (pp.43-53). Publisher: European Liberal Forum (ELF). December 2022.

2. Saari, Muthanna. (2020). IR 4.0. in parliament: Conceptualising the application of artificial intelligence and machine learning in the parliament of

Malaysia's parliamentary questions. International Journal of Law, Government and Communication. 5. 124-137. 10.35631/IJLGC.5200010.

3. Artificial Intelligence: Innovation in parliaments. URL. <https://www.ipu.org/innovation-tracker/story/artificial-intelligence-innovation-in-parliaments>

Костенко О. В.

доктор філософії (Ph.D.) з юридичних наук, завідувач наукової лабораторії теорії цифрової трансформації і права наукового центру цифрової трансформації і права Державної наукової установи «Інститут інформації, безпеки і права НАПрН України».

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЗІ ШТУЧНИМ ІНТЕЛЕКТОМ ЯК СУЧАСНИЙ ІНСТРУМЕНТАРІЙ ЕФЕКТИВНОГО ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ

Парламентський контроль є основою сильної демократичної системи як процес забезпечення виконання парламентом своїх повноважень в суспільних інтересах. Він передбачає моніторинг дій органів державної влади і місцевого самоврядування та їх коригування у відповідності до інтересів суспільства та законодавства. Ефективність парламентського контролю базується на наступних ключових факторах. Перш за все, повноваження, надані парламенту, мають бути достатньо потужними, щоб забезпечити ефективність контролю. По-друге, дотримання принципу прозорості діяльності уряду, що забезпечується регулярними інформаційними звітами парламенту та громадськості. По-третє, високою компетентністю та незалежністю парламентаріїв навіть за умов політичного тиску. Крім того, необхідна модернізація і цифровізація традиційних форм парламентського контролю, таких як комітети та слухання, з метою підтримки балансу захисту прав і свобод громадян під час цифровізації суспільних відносин, особливо із застосуванням технологій штучного інтелекту (далі – AI), шляхом прийняття сучасних законів.

AI відноситься до класу інформаційно-комунікаційних систем, які функціонують за алгоритмами, що моделюють інтелект людини. Важливість застосування AI в процесах парламентського контролю полягає

в його здатності допомагати в аналізі політик, ідентифікації потенційних проблем і формулюванні відповідних реакцій парламенту, виявленні ризиків в діяльності органів державної влади, наданні неупередженого аналізу великих обсягів даних окремих галузей, виявлення закономірностей тощо.

Використання методів AI в парламентському контролі надасть численні переваги, а саме:

- сприятиме підвищенню прозорості та підзвітності парламентського контролю;
- виявлятиме аномалії в даних, відстежувати закономірності та контролювати події в реальному часі, перш ніж вони набудуть негативного контексту або деструктивного результату;
- своєчасно визначатиме та коригуватиме тенденції і моделі у таких сферах, як державний та місцеві бюджети, ефективність законодавства, соціальний вплив економічних реформ тощо;
- аналізуватиме дані з державних веб-сайтів, щоб точно визначити сфери, які потрібно вдосконалити, роблячи інформацію більш доступною для громадськості;
- підвищуватиме ефективність і точність у процесі прийняття рішень, що призведе до кращих результатів для суспільства;
- автоматизуватиме різні завдання, такі як аналіз даних і звітність, надаватиме узагальнену аналітичну інформацію, яку парламентаріям важко побачити через складність і кількість даних;
- зменшуватиме робоче навантаження та вивільнить час законодавців та парламентарів для оптимізації посадових обов'язків, що призведе до економії бюджетних коштів;
- аналізуватиме та формуватиме шаблони мовлення для підвищення якості парламентських дебатів, а також створювати для парламентарів зворотний зв'язок у режимі реального часу щодо своїх виступів для їх подальшої оптимізації;
- забезпечуватиме об'єктивний аналіз даних та виявлення проблем, пов'язаних з корупцією, шахрайством або будь-якими іншими правопорушеннями, що зміцнить довіру між парламентом і громадянами та призведе до більш надійного демократичного процесу;
- підвищуватиме ефективність законотворчих процесів шляхом ефективного виконання таких завдань, як розшифрування сесій, аналіз відмінностей між законопроектами, поправками та поточними законами, здійснення аналізу на відповідність нормам законодавства Європейського Союзу та міжнародних нормативно-правових актів.

Є кілька прикладів того, як AI використовується для підвищення ефективності та дієвості парламентів.

Так, Палата представників США запровадила інструмент AI для автоматизації процесу аналізу розбіжностей між законопроектами, поправками та поточними законами, що дозволило бачити їх вплив на сферу застосування закону. Технологія AI здатна інтерпретувати посилання на правові положення, описані в законопроектах, і отримувати ці положення, а також тлумачити і виконувати поправкові інструкції. Інструмент, вже доступний для Офісу законодавчого радника Палати представників Сполучених Штатів [1].

Токійський Національний вищий інститут політичних досліджень (GRIPS) розробив систему, яка використовує дані з Парламенту Японії, щоб зробити парламентські відео доступними для пошуку, використовуючи новітні методи розпізнавання мовлення.

Парламент Південно-Африканської Республіки вивчає можливість використання чат-бота, щоб допомогти членам парламенту інформацією про статус конкретного законопроекту, резолюції, питання чи процесу розгляду.

Палата представників Нідерландів впровадила систему «Speech2Write», яка пропонує своєму Управлінню парламентської звітності (PRO) можливість не просто перетворювати голос у текст, але й замість цього «перекладати» голос у письмові звіти.

Найближчим часом парламент Естонії збирається представити проєкт HANS – систему штучного інтелекту, яка стане важливим інструментом в роботі законодавців здійснюючи декодування стенограм на основі алгоритмів розпізнавання мови, що підвищить ефективність і точність стенограм сесійних сеансів [2].

Слід зазначити, що впровадження технологій AI містить і певні ризики, які формуються менше в технологічній площині, а більше в соціальній.

Останні дослідження, що ґрунтуються на серії проєктів із моделювання електорату та генерації «алгоритмічних шаблонів» виборчих думок – основи ефективного соціоакінгу, свідчать про те, що мовні моделі, навчені на «медіа-дієтах», можуть прогнозувати громадську думку. На стику виборчих технологій та соціології виборів дослідники навчилися створювати алгоритмічні копії соціальних груп, які перевели соціоакінг з теоретичної до практичної площини. Соціоакінг – це методика навчання алгоритмів, здатних на агрегованому рівні відігравати роль універсальних вікон у людському мисленні лише на рівні соціальних груп. Аналізуючи bigdata соціокультурного досвіду демографічної групи,

можна отримати розподіл відповідей моделі, що корелюється з розподілом відповідей людей під час опитування цієї групи. Тобто, можна тренуватися виявляти когнітивні аномалії різних соціальних груп на їх алгоритмічних моделях. А виявивши ці аномалії, цілеспрямовано формувати вплив на свідомість людей, маніпулюючи ними у потрібному векторі.

На початку 2023 року «революція ChatGPT» несподівано відкрила колосальні можливості впливу ChatGPT на політичні судження людей. Дослідження показало, що переконливість AI у політичних питаннях не поступається професійним політтехнологам, а здатність AI грати на відтінках індивідуальних переваг конкретних людей дозволяє переконувати людей навіть у найгостріших поляризованих питаннях політики.

Виступаючи у ролі «медіа-дієтолога», мовна модель AI виділяє приховані від нас тонкощі мови, що дозволяє мовній моделі здійснювати тонке настроювання свідомості людей на ті чи інші світоглядні та політичні сфери уподобань.

Тепер технологія соціохакингу має повний набір інструментів впливу на соціальні групи:

- формувач алгоритмічної копії соціальної групи – свого роду полігон на якому тренується та налаштовується мовна модель;
- конструктор «алгоритмічних шаблонів», які формують контент, що легко сприймається;
- генератор «медіа-дієти», яку потрібно транслювати таргетованій соціальній групі;
- набір прийомів переконань, які ґрунтуються на когнітивних особливостях таргетованої соціальної групи з метою точкового впливу на свідомість та подальшої маніпуляції людьми у потрібному векторі [3].

Фактично використання технологій AI для соціохакингу та «медіа-дієт» можливо застосовувати для прямого та опосередкованого впливу на парламентарів.

Сьогодні Україна одна із небагатьох країн, яка не створила та затвердила власну Стратегію розвитку штучного інтелекту [4], «Білу книгу впровадження AI» та Державну або галузеві моделі розвитку AI на короткостроковий та довгостроковий період. Алгоритми AI в Україні створюються лабораторно і застосовуються вузькоспеціалізовано та хаотично, а також не мають системності і не обліковуються (ліцензуються, маркуються тощо).

Вважаємо вкрай актуальним та необхідним у найкоротші терміни активізувати вирішення проблемних питань технічного, етичного, соціального та правового застосування AI, перш за все в органах державної влади.

Література.

1. Artificial Intelligence: Innovation in parliaments. URL: <https://www.ipu.org/innovation-tracker/story/artificial-intelligence-innovation-in-parliaments> (дата звернення: 19.04.2023).
2. Introducing HANS, the new AI support tool for Estonian lawmakers. URL: <https://e-estonia.com/hans-ai-support-tool-for-estonian-parliament/> (дата звернення: 20.04.2023).
3. Eric Chu, Jacob Andreas, Stephen Ansolabehere, Deb Roy. Language Models Trained on Media Diets Can Predict Public Opinion. Cornell University, May 2023. DOI: <https://doi.org/10.48550/arXiv.2303.16779>.
4. Костенко О. Аналіз національних стратегій розвитку штучного інтелекту. Інформація і право. 2022. № 2(41). С. 58–69.

Майстренко І. А.

науковий співробітник Державної наукової установи «Інститут інформації, безпеки і права НАПрН України»

Фурашев В. М.

*кандидат технічних наук, старший науковий співробітник, перший заст. директора Державної наукової установи «Інститут інформації, безпеки і права НАПрН України»
ORCID: 0000-0001-7205-724X*

СУБ'ЄКТИ ТА ОБ'ЄКТИ ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ В УМОВАХ СОЦІАЛЬНИХ ТРАНСФОРМАЦІЙ

Конституція України чітко та однозначно визначила головного суб'єкта парламентського контролю, суб'єкта, якому громадяни країни делегували здійснення своїх професійних та об'єктивних функцій з розвитку та захисту держави, суспільства та людини.

Це твердження підтверджується основними, принциповими положеннями Конституції України – Основного закону країни, а саме:

- Україна є суверенна і незалежна, демократична, соціальна, правова держава (ст.1);
- права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною

- за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави. (ст. 3);
- носієм суверенітету і єдиним джерелом влади в Україні є народ. Народ здійснює владу безпосередньо і через органи державної влади та органи місцевого самоврядування. Право визначати і змінювати конституційний лад в Україні належить виключно народові і не може бути узурповане державою, її органами або посадовими особами. Ніхто не може узурпувати державну владу. (ст.5);
 - в Україні визнається і діє принцип верховенства права. Конституція України має найвищу юридичну силу. Закони та інші нормативно-правові акти приймаються на основі Конституції України і повинні відповідати їй. Норми Конституції України є нормами прямої дії. Звернення до суду для захисту конституційних прав і свобод людини і громадянина безпосередньо на підставі Конституції України гарантується. (ст.8);
 - народне волевиявлення здійснюється через вибори, референдум та інші форми безпосередньої демократії. (ст. 69);
 - **єдиним органом законодавчої влади в Україні є парламент – Верховна Рада України** (ст. 75);

Таким чином, Верховна Рада України – єдиний колективний представник народовладдя країни, а тому є головним суб'єктом народного контролю в системі державного управління у вигляді парламентського контролю.

Загально відомо, що контроль — одна з основних функцій системи управління. У даному випадку, парламентський контроль здійснюється на основі спостереження за поведінкою системи суспільних відносин з метою забезпечення оптимального її функціонування (вимірювання досягнутих результатів і співвіднесення їх із очікуваними результатами). На основі даних контролю здійснюється адаптація системи, тобто прийняття оптимальних нормативно-правових та організаційно-управлінських рішень.

Конституція України визначає наступні узагальнені національні **об'єкти** такого контролю, зокрема:

- земля, її надра, атмосферне повітря, водні та інші природні ресурси, які знаходяться в межах території України, природні ресурси її континентального шельфу, виключної (морської) економічної зони є об'єктами права власності Українського народу. Від імені Українського народу права власника здійснюють органи державної влади та органи місцевого самоврядування в межах, визначених цією Конституцією. Кожний громадянин має право користу-

ватися природними об'єктами права власності народу відповідно до закону. Власність зобов'язує. Власність не повинна використовуватися на шкоду людині і суспільству. Держава забезпечує захист прав усіх суб'єктів права власності і господарювання, соціальну спрямованість економіки. Усі суб'єкти права власності рівні перед законом. (ст. 13);

- земля є основним національним багатством, що перебуває під особливою охороною держави. Право власності на землю гарантується. Це право набувається і реалізується громадянами, юридичними особами та державою виключно відповідно до закону. (ст. 14);
- суспільне життя в Україні ґрунтується на засадах політичної, економічної та ідеологічної багатоманітності. Жодна ідеологія не може визнаватися державою як обов'язкова. Цензура заборонена. Держава гарантує свободу політичної діяльності, не забороненої Конституцією і законами України. (ст. 15);
- забезпечення екологічної безпеки і підтримання екологічної рівноваги на території України, подолання наслідків Чорнобильської катастрофи – катастрофи планетарного масштабу, збереження генфонду Українського народу є обов'язком держави. (ст. 16);
- захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. Оборона України, захист її суверенітету, територіальної цілісності і недоторканності покладаються на Збройні Сили України. Забезпечення державної безпеки і захист державного кордону України покладаються на відповідні військові формування та правоохоронні органи держави, організація і порядок діяльності яких визначаються законом. Збройні Сили України та інші військові формування ніким не можуть бути використані для обмеження прав і свобод громадян або з метою повалення конституційного ладу, усунення органів влади чи перешкоджання їх діяльності. Держава забезпечує соціальний захист громадян України, які перебувають на службі у Збройних Силах України та в інших військових формуваннях, а також членів їхніх сімей. На території України забороняється створення і функціонування будь-яких збройних формувань, не передбачених законом. На території України не допускається розташування іноземних військових баз. (ст. 17);
- правовий порядок в Україні ґрунтується на засадах, відповідно до яких ніхто не може бути примушений робити те, що не передбаче-

- но законодавством. Органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України. (ст. 19);
- кожна людина має право на вільний розвиток своєї особистості, якщо при цьому не порушуються права і свободи інших людей, та має обов'язки перед суспільством, в якому забезпечується вільний і всебічний розвиток її особистості. (ст.23);
 - громадянин України не може бути позбавлений громадянства і права змінити громадянство. Громадянин України не може бути вигнаний за межі України або виданий іншій державі. Україна гарантує піклування та захист своїм громадянам, які перебувають за її межами. (ст. 25);
 - кожна людина має право на свободу та особисту недоторканність. Ніхто не може бути заарештований або триматися під вартою інакше як за вмотивованим рішенням суду і тільки на підставах та в порядку, встановлених законом. У разі нагальної необхідності запобігти злочинів чи його перепинити уповноважені на те законом органи можуть застосувати тримання особи під вартою як тимчасовий запобіжний захід, обґрунтованість якого протягом сімдесяти двох годин має бути перевірена судом. Затримана особа негайно звільняється, якщо протягом сімдесяти двох годин з моменту затримання їй не вручено вмотивованого рішення суду про тримання під вартою. Кожному заарештованому чи затриманому має бути невідкладно повідомлено про мотиви арешту чи затримання, роз'яснено його права та надано можливість з моменту затримання захищати себе особисто та користуватися правничою допомогою захисника. Кожний затриманий має право у будь-який час оскаржити в суді своє затримання. Про арешт або затримання людини має бути негайно повідомлено родичів заарештованого чи затриманого. (ст.29);
 - не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права

вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації. (ст. 32);

- усі мають право направляти індивідуальні чи колективні письмові звернення або особисто звертатися до органів державної влади, органів місцевого самоврядування та посадових і службових осіб цих органів, що зобов'язані розглянути звернення і дати обґрунтовану відповідь у встановлений законом строк. (ст. 40);
- кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності. Право приватної власності набувається в порядку, визначеному законом. Громадяни для задоволення своїх потреб можуть користуватися об'єктами права державної та комунальної власності відповідно до закону. Ніхто не може бути протиправно позбавлений права власності. Право приватної власності є непорушним. Примусове відчуження об'єктів права приватної власності може бути застосоване лише як виняток з мотивів суспільної необхідності, на підставі і в порядку, встановлених законом, та за умови попереднього і повного відшкодування їх вартості. Примусове відчуження таких об'єктів з наступним повним відшкодуванням їх вартості допускається лише в умовах воєнного чи надзвичайного стану. Конфіскація майна може бути застосована виключно за рішенням суду у випадках, обсязі та порядку, встановлених законом. Використання власності не може завдавати шкоди правам, свободам та гідності громадян, інтересам суспільства, погіршувати екологічну ситуацію і природні якості землі. (ст.41);
- кожен має право на підприємницьку діяльність, яка не заборонена законом. Підприємницька діяльність депутатів, посадових і службових осіб органів державної влади та органів місцевого самоврядування обмежується законом. Держава забезпечує захист конкуренції у підприємницькій діяльності. Не допускаються зловживання монопольним становищем на ринку, неправомірне обмеження конкуренції та недобросовісна конкуренція. Види і межі монополії визначаються законом. Держава захищає права споживачів, здійснює контроль за якістю і безпечністю продукції та усіх видів послуг і робіт, сприяє діяльності громадських організацій споживачів. (ст. 42).

Наведені узагальнені національні об'єкти парламентського контролю, цілком зрозуміло, розраховані на спокійний та стабільний розви-

ток людини, суспільства та держави. Але не завжди так буває, тому Конституція України передбачає, що «в умовах воєнного або надзвичайного стану можуть встановлюватися окремі обмеження прав і свобод із зазначенням строку дії цих обмежень. Не можуть бути обмежені права і свободи, передбачені статтями 24, 25, 27 – 29, 40, 47, 51 – 52, 55 – 63 цієї Конституції» (ст. 64).

Більше деталізовані об'єкти парламентського контролю наведені у статті 85 та інших статтях Конституції України.

Необхідно також відзначити, що «Верховна Рада України для здійснення законопроектної роботи, підготовки і попереднього розгляду питань, віднесених до її повноважень, **виконання контрольних функцій** відповідно до Конституції України створює з числа народних депутатів України комітети Верховної Ради України. Верховна Рада України у межах своїх повноважень може створювати тимчасові спеціальні комісії для підготовки і попереднього розгляду питань. Верховна Рада України для проведення розслідування з питань, що становлять суспільний інтерес, утворює тимчасові слідчі комісії, якщо за це проголосувала не менш як одна третина від конституційного складу Верховної Ради України. Висновки і пропозиції тимчасових слідчих комісій не є вирішальними для слідства і суду. Організація і порядок діяльності комітетів Верховної Ради України, її тимчасових спеціальних і тимчасових слідчих комісій встановлюються законом.» (ст. 89). Тобто комітети Верховної Ради України не наділяються самостійними контрольними повноваженнями, вони можуть лише сприяти Верховній Раді України у здійсненні повноважень щодо парламентського контролю, виконуючи певні дії допоміжного (інформаційного, експертного, аналітичного тощо) характеру.

З огляду на вище викладене можна зробити наступні ВИСНОВКИ та ПРОПОЗИЦІЇ:

1. Наведене досить повно та всебічно відображає об'єкти парламентського контролю з метою забезпечення сталого розвитку людини, суспільства та держави у «спокійних умовах».

2. Сьогоднішня сучасність характерна наявністю воєнного стану по всій території країни, що не може не відобразитися на пріоритетності об'єктів парламентського контролю, а також на законодавчо затверджених організаційно-технологічних процесах підготовки та проведення парламентського контролю.

3. Пропонується розглянути питання стосовно **тимчасового**, на період дії в країні воєнного або надзвичайного стану **здійснення комітетами** Верховної Ради України **парламентського контролю** за тематикою найбільш невідкладних його об'єктів, не порушуючи положень ст. 64,

частини першої ст. 157 та частини першої ст. 85 Конституції України. Крім того, необхідно звернути увагу на положення Рішення Конституційного Суду України у справі за конституційним поданням 58 народних депутатів України щодо відповідності Конституції України (конституційності) положень пунктів 3, 4, 5, 6 статті 9, пунктів 3, 4, 5 статті 10, підпункту «г» пункту 1 статті 24, пункту 3 статті 26 Закону України “Про організаційно-правові основи боротьби з організованою злочинністю”, пункту 10 статті 14, статті 33-1 Закону України “Про комітети Верховної Ради України”.

Список використаної літератури

1. Конституція України, *Відомості Верховної Ради України (ВВР)*, 1996, № 30, ст. 141, URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

2. Про Регламент Верховної Ради України: Закон України від 10.02.10 р. № 1861-VI, редакція від 31.03.23 р. URL: <https://zakon.rada.gov.ua/laws/show/1861-17#Text>

3. Про комітети Верховної Ради України: Закон України від 04.04.95 р. № 116/95-ВР, редакція від 31.03.23 р. URL: <https://zakon.rada.gov.ua/laws/show/116/95-%D0%B2%D1%80#Text>

4. Рішення Конституційного Суду України у справі за конституційним поданням 58 народних депутатів України щодо відповідності Конституції України (конституційності) положень пунктів 3, 4, 5, 6 статті 9, пунктів 3, 4, 5 статті 10, підпункту “г” пункту 1 статті 24, пункту 3 статті 26 Закону України “Про організаційно-правові основи боротьби з організованою злочинністю”, пункту 10 статті 14, статті 33-1 Закону України “Про комітети Верховної Ради України” URL: <https://zakon.rada.gov.ua/laws/show/v016p710-10#Text>

Лихоступ С. В.

кандидат економічних наук, старший науковий співробітник, провідний науковий співробітник Державної наукової установи «Інститут інформації, безпеки і права НАПрН України»

ОСНОВИ СИСТЕМИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ В ПРОЦЕСАХ РОЗВИТКУ СОЦІАЛЬНИХ СТРУКТУР УКРАЇНИ

Розвиток України, як активного співучасника та складовою частиною Європейського союзу повинен бути спрямований в рамках стабільної соціальної політики розвитку суспільства з урахуванням сучасних та перспективних тенденцій ринкової економіки, що призводить до позитивних тенденцій у задоволенні потреб та якості життя громадян. А тому в процесах створення та реалізації таких вимог визначається першочергова потреба у нормативно-законодавчому формуванні основ та у моделювання структур динамічного розвитку соціальних структур суспільства у відповідності до демократичних принципів управління державою.

Соціальна структура суспільства – це відносно постійна модель соціальних класифікацій у визначеному суспільстві. Основні елементи соціальної структури суспільства: соціальні групи, соціальні шари, соціальні спільноти та соціальні інститути пов'язані між собою соціальними відносинами, носіями яких є люди. Слід відзначити, що гідний рівень соціально-економічного розвитку суспільства в першу чергу визначається раціональним станом функціонування соціально – нормативного управління всіма складовими суспільства, розпочинаючи із органів управління соціальними структурами суспільства та закінчуючи регулюванням економічних відносин між окремими виробничо – господарчими структурами. В такому випадку для ефективного управління системою соціальних структур країни необхідно створення системи їх нормативно – правового забезпечення в мінливих умовах розвитку європейської та світової економіки, а також з урахуванням динамічних принципів до вимог та стандартів життя окремих громадян в цих умовах.

Така система уявляється як логіко – структурований граф, що включає в себе такі виділені підсистеми як: визначення стратегії та формування концепції комплексу нормативно – правового розвитку суспільства; складання сукупності вимог та обмежень до розробки та запровадження окремих пакетів нормативно – правового забезпечення в різних со-

ціальних структурах суспільства; створення нормативно – правових документів у відповідності до вимог європейського товариства; оперативне регулювання структури нормативно- правових документів та їх змісту в мінливих розвитку суспільства; визначення порядку використання та рівня відповідальності за ефективністю реалізації нормативно – правових документів.

По-перше, складання стратегії та формування концепції комплексу нормативно – правового розвитку суспільства означає розробку таких законодавчих документів, які реалізують цілий рядок принципів надійного розвитку соціальної держави, а саме. Це, перш за все, сукупність нормативних актів, що відображують вимоги та умови досягнення соціального та економічного достатку громадян завдяки соціальній рівності, трудової зацікавленості в досягненні гідного рівня життя. В такій структурі документів повинні бути передбачені нормативно – правові документи, що гарантують соціальний захист громадян, охорону їх здобутків, соціального забезпечення та гідного рівня життя, що визначається справедливими принципами розподілу здобутків суспільства за результатами колективної праці. Важливими регулюючими нормативними документами при цьому повинні бути такі, що гарантують вільний розвиток особистості в умовах забезпечення гарантій по досягненню рівних можливостей, але також і відповідної соціальної активності, трудової солідарності та відповідальності кожного громадянина за свою діяльність. При цьому в таких документах повинні бути фіксовані шляхи та можливості до рівного доступу громадян до громадських та соціальних інституцій, розвитку професійних можливостей у різних сферах трудової діяльності із використанням суспільних ресурсів.

Реалізація таких нормативно – правових документів повинна бути підтверджена системою актів про соціальну відповідальність суб'єктів бізнесу та різних структур підприємницької діяльності за результати використання своїх виробничих спроможностей, принципів регулювання справедливого розподілу результатів колективної праці, що сприяє подальшій активізації використання виробничого потенціалу та розвитку соціальної сфери окремих соціальних груп суспільства. Головний фактор, що формує концепцію таких нормативно – правових документів – це захист прав та інтересів окремих громадян в соціальних та виробничо – бізнесових структурах суспільства.

Звичайно, в підтримання пакету цих нормативно – правових документів є створення таких, що забезпечують уникнення або пом'якшення впливу на суспільство та кожного громадянина негативних економічних наслідків і ризиків в управлінні суспільною працею. Але при цьому про-

відним принципом в процесі формування таких нормативно – правових документів є надання гарантій розвитку гармонійних принципів розвитку відносин між різними соціальними групами, що забезпечують партнерську відносини, порозуміння та злагодженість у досягненні результатів.

В підсистемі складання сукупності вимог та обмежень до розробки та запровадження окремих пакетів нормативно – правового забезпечення в окремих соціальних структурах повинна фігурувати домінанта надання всіх прав та свобод в демократичному суспільстві при умові гідного життя. При цьому в таких документах повинні бути чітко визначені форми відповідальності окремих осіб за невідповідність їх діяльності всупереч порушеним нормам суспільства. До критеріальних вимог розвитку таких нормативно – правових актів слід віднести також обґрунтовані принципи до забезпечення динамічних умов розвитку людини, захисту її культурних та національних традицій. Реалізація та підтримання цих документів знаходить підтвердження в пакеті нормативно – правових документів, що визначають міри відповідальності за негативні наслідки соціально – економічних умов населення органів державної влади та місцевого самоврядування. І, на кінець, в нормативно – правових документах, що визначають вимоги до розвитку соціальних структур суспільства, повинні розвинути та інтегровані до міжнародного права обов'язки держави та соціальних інституцій у їх формуванні та відповідальності за свою діяльність.

Центральною, пов'язуючою та регулюючою підсистемою є підсистема власне створення нормативно – правових документів у відповідності до вимог України, як незалежної держави, так і європейського товариства. На сьогоднішній день це найбільш активна підсистема, що породжує як багато сподівань, так і нарікань. Сподівання – тому що певний нормативний документ надає надію на вирішення чи регулювання певних ситуацій певної проблеми. Але, з іншого боку, локальне, як правило, хаотичне чи вольове прийняття ряду нормативно – правових документів призводить до породження ще до більш за заплутаного клубка проблем. А тому системність у створенні та відпрацюванні нормативно – правових документів з урахуванням принципу причинно – наслідкових подій має надзвичайне значення. Розгляд функціонування такої важливої підсистеми заслуговує надзвичайної уваги, так як вона повинна бути орієнтована на вирішення актуальних, сьогоденних питань розвитку суспільства, орієнтирів на перспективу його покращання, що можливе тільки при умові ретельного перехресного пов'язання умов функціонування всіх ключових задач до конкретної проблеми нормативно – правових документів.

Непередбачуваність та складність процесів розвитку суспільства вимагає постійного та оперативного регулювання структури нормативно – правових документів та їх змісту в мінливих умовах розвитку суспільства, що може складати слідуючу умовну підсистему. Група таких нормативно – правових документів формує як би захисні основи для життєдіяльності членів суспільства.

Перш за все в такій підсистемі формуються документи, що визначають шляхи розвитку ділового партнерства, соціальної інтеграції праці та виробництва. В таких документах повинні бути викладені гарантії що до реалізації різних форм використання трудового потенціалу, формування та інтеграції соціальної інфраструктури при умові партнерства та взаємної згоди між окремими верстами населення.

Мова йде про викладення в таких документах цілої низки соціальних, політичних та економічних гарантій в широкому розумінні цього контексту. Важливе місце при цьому займає ідея про створення захисного механізму людини від можливих порушень прав та свобод, економічних негараздів, правопорушень злочинного чи антисоціального характеру. В таких документах відслідковується домінуюча нота про реалізацію державних заходів, форм надання захисту та ліквідації лиха шляхом проведення державної політики надання гарантій та необхідних послуг. Особливість таких документів полягає у викладенні можливих форм соціально – економічної безпеки та розвиток варіантів можливого її усунення та мінімізації завданої шкоди. Також це група документів, що спрямована на формалізацію та викладення форм дій що до захисту вразливих форм суспільства та надання їм необхідної допомоги.

Нарешті підсистема визначення порядку та рівня відповідальності за ефективністю реалізації нормативно – правових документів в принципі формує механізм втілення в практику державних і місцевих органів таких документів. Акцент створення такого механізму полягає у практичних діях реалізації законодавчих та нормативних документів управління державою з метою досягнення соціальних основ життєздатності України. Конкретні дії в цьому напрямку включають багато напрямків, розпочинаючи з удосконалення чинного законодавства, розвитку форм соціального партнерства, дослідження ефективних методів покращання економічного положення та інші.

Характерні ознаки системного підходу до створення нормативно – правового забезпечення основ регулювання функціонування та розвитку соціальних структур України можливо дослідити в ряді державних документів, наприклад, [1,2,3,4,5,6,7]. Звичайно, в процесі створення певного нормативного акту не використовуються тільки домінуючі ознаки

виділених вище підсистем. Але використання певних базових статей, що формують створення конкретного нормативного акту, дає змогу чітко його трактувати та ефективно використати на практиці.

Список використаних джерел

1. Про державні соціальні стандарти та державні соціальні гарантії : Закон України від 05.10.2000 №2017III. URL:<https://zakon.rada.gov.ua/show/2017-14#Text>.

2. Про прожитковий мінімум: Закон України від 15.07.1999 №966-XIV. URL:<https://zakon.rada.gov.ua/show/966-14#Text>.

3. Про загальнообов'язкове державне пенсійне страхування: України від 09.07.2003 №1058-IV. URL:<https://zakon.rada.gov.ua/show/1058-15#Text>.

4. Про соціальні послуги: Закон України від 17.01.2019р. № 2671-VIII. URL:<https://zakon.rada.gov.ua/show/2671-19#Text>.

5. Про соціальний діалог України: Закон України від 23.12.2010р. №2862-IV. URL:<https://zakon.rada.gov.ua/show/2862-17#Text>.

6. Деякі питання надання соціальних послуг шляхом соціального замовлення: Постанова Кабінету Міністрів України від 01.06.2020 р. № 450. URL:<https://zakon.rada.gov.ua/show/450-2020-%D0%BF#Text>.

7. Конституція України: прийнята на V сесії Верховної Ради України 28 чер. 1996 р. (зі змінами) URL:<https://zakon.rada.gov.ua/show/254%D0%BA/96-%D0%B2%D1%80>.

Радзівська О. Г.

кандидат юридичних наук, старший дослідник, провідний науковий співробітник Державної наукової установи «Інститут інформації, безпеки і права НАПрН України»

ПАРЛАМЕНТСЬКИЙ КОНТРОЛЬ ЗА ДОДЕРЖАННЯМ ІНФОРМАЦІЙНИХ ПРАВ ЛЮДИНИ В УМОВАХ ВОЄННОГО СТАНУ

Питання додержанням конституційних прав і свобод людини і громадянина є надзвичайно важливими у сучасному демократичному світі, а забезпечення їх дотримання є пріоритетним завданням держави. Важливою складовою у питаннях забезпечення дотримання прав і свобод є сис-

тема дієвого моніторингу та контролю. Відповідно до статті 101 Конституції України парламентський контроль за додержанням конституційних прав і свобод людини і громадянина здійснює Уповноважений Верховної Ради України з прав людини. Якщо права та свободи останньої порушено органами державної влади, органами місцевого самоврядування та їх посадовими і службовими особами, а також юридичними та фізичними особами, вона може звернутися до Уповноваженого Верховної Ради України з прав людини відповідно до Закону України «Про Уповноваженого Верховної Ради України з прав людини». Таке право гарантоване статтею 55 Конституції України.

В епоху активної цифровізації суспільних відносин та в умовах повномасштабної війни перед Уповноваженим Верховної Ради України з прав людини стоїть важливе завдання — моніторинг додержання інформаційних прав, і запобігання їх порушенням. З урахуванням нових викликів та задля найкращого захисту прав громадян під час війни було вирішено переглянути структуру Офісу Уповноваженого. Так, була створена посада Представника Уповноваженого з інформаційних прав та сформовано окремий структурний підрозділ – Департамент моніторингу додержання інформаційних прав. Діяльність цього структурного підрозділу Уповноваженим Верховної Ради України з прав людини зосереджена на трьох основних напрямках моніторингу додержання прав людини в інформаційній сфері, а саме:

- прав на доступ до інформації;
- права на звернення та запит до органів державної влади та органів місцевого самоврядування;
- права на захист персональних даних особи та її конфіденційної інформації.

Певні складності під час війни спостерігаються у питаннях реалізації права особи на доступ до інформації. Зокрема, це стосується:

- обмеження доступу до публічної інформації;
- зловживань у питаннях реалізації права громадян на запит до органів державної влади;
- обмеження доступу до суспільно важливої інформації;
- обмеження доступу до інформації навчального характеру та порушення права на освіту на окупованих територіях.

Серед усіх звернень громадян до Уповноваженого Верховної Ради України з прав людини щодо порушення їх прав велику частину займають саме порушення інформаційних прав. Зокрема, право на доступ до публічної інформації та право на звернення до органів влади становили четверть від всіх звернень громадян у 2022 році. Моніторинг дотримання

інформаційних прав в Україні в умовах воєнного стану у 2022 та 2023 роках свідчить про задовільний проте недостатній рівень забезпечення. Наприклад, середній рівень дотримання вимог законодавства щодо оприлюднення публічної інформації на офіційних веб-сайтах розпорядників публічної інформації у 2022 році становив лише 55%. Порівняльний аналіз моніторингу стану забезпечення інформаційних прав в умовах воєнного стану в 2022 та 2023 роках, здійснений в рамках проекту «Права людини для України», виконаний ПРООН в Україні та Офісом Уповноваженого Верховної Ради України з прав людини, свідчить про погіршення ситуації з оприлюдненням публічної інформації на офіційних веб-сайтах розпорядників публічної інформації у 2023 році. Середній рівень дотримання вимог законодавства щодо оприлюднення публічної інформації на офіційних веб-сайтах розпорядників публічної інформації у 2023 році склав лише 50%, що на 5% нижче рівня в 2022 році. Серед публічної інформації, яку моніторили на офіційних веб-сайтах була така суспільно-необхідна інформація, як:

- місця укриття, прихистку, наявність у них ліків та продуктів харчування;
- про воєнні загрози з боку агресора та необхідність евакуації населення в межах територіальної юрисдикції;
- про режим та особливості функціонування органів, підприємств та установ, які надають адміністративні та інші послуги, в умовах воєнного стану;
- щодо процесу доставки, розподілу та розповсюдження гуманітарної допомоги.

У 2022 році лише у 2% розпорядники публічної інформації оприлюднили на своїх офіційних веб-сайтах всі зазначені категорії інформації у повному обсязі, 13% – частково оприлюднили більшість із категорій інформації, 55% – частково оприлюднили одну із категорій інформації, а 30% – не оприлюднили вказану інформацію. Тоді як моніторинг 2023 року встановив, що жоден офіційний веб-сайт розпорядника публічної інформації не оприлюднив у повному обсязі всі категорії суспільно-важливої та необхідної інформації в умовах воєнного стану. Частково оприлюднили більшість із категорій інформації розпорядники публічної інформації у 2023 році на своїх офіційних веб-сайтах у 21% випадків, 54% – частково оприлюднили одну із категорій інформації, не оприлюднили вказану інформацію у 25%.

Стан забезпечення прав громадян на отримання інформації шляхом звернень та інформаційних запитів також свідчить про порушення прав громадян на доступ до інформації. За результатами моніторингу на

усний запит у 2022 році громадяни отримали відповідь лише у 52% випадків, у 2023 році – у 55%, на усне звернення – 48% у 2022 році та 55% у 2023 році. Трохи краща ситуація із запитом на інформацію в письмовій формі (електронна пошта) спостерігалась у 2022 році: на письмовий запит отримано відповідь у 77% випадків, на письмове звернення – 79%. Однак у 2023 році показники моніторингу показують тенденції до значного регресу у доступі до інформації шляхом звернень та інформаційних запитів у письмовій формі. Зокрема, у 2023 році письмовий запит на інформацію був задовільнений лише у 57% випадків, письмове звернення – у 60%. Це свідчить про погіршення стану забезпечення прав громадян на інформацію шляхом звернень та інформаційних запитів у письмовій формі.

Також лише частково забезпечене органами державної влади та місцевого самоврядування право громадян на особистий прийом. Із матеріалів моніторингу лише у 41% випадків право на особистий прийом забезпечене на належному рівні та частково у 17% випадків у 2022 році, а також 42% і 18% відповідно у 2023 році. Тоді як відмовлено у реалізації права на особистий прийом у 29% випадків у 2022 році та 23 % випадків у 2023 році. У 13% у 2022 році та 17% у 20223 році на запити про особистий прийом громадян органи державної влади та місцевого самоврядування відповіді взагалі не надали.

Крім актуальних питань доступу громадян до інформації, яка є вкрай важливою в умовах воєнного стану проблематичним залишається, як і раніше, питання реалізації права на захист персональних даних особи та її конфіденційної інформації. Це стосується:

- правомірності збору персональних даних та конфіденційної інформації про особу, особливо в мережі Інтернет, та соціальних медіа;
- правомірності використання персональних даних та конфіденційної інформації про особу;
- належного захисту персональних даних при зберіганні та обробці.

Про це свідчать дані Щорічної доповіді про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2022 році Уповноваженого Верховної Ради України з прав людини. Зокрема, 60% звернень до Уповноваженого Верховної Ради України з прав людини в інформаційній сфері за 2022 рік пов'язано з незаконною обробкою персональних даних, 12% – стосувалися порушення процедури обробки персональних даних суб'єктами владних повноважень [1]. 28% звернень громадян до Уповноваженого Верховної Ради України з прав людини у 2022 році стосувалися порушення права на доступ до інформації про себе.

Питання доступу до повної, неупередженої та актуальної інформації у період війни може стати критичним, а її відсутність призвести до тяжких наслідків. Водночас, як і захист чутливої інформації в умовах воєнного стану є надзвичайно важливим елементом забезпечення національної безпеки. Однак, усі заходи протидії інформаційним викликам не можуть зазіхати на інформаційні права громадян, гарантовані національним та міжнародним правом, так само, як не можуть обмежувати інформаційні свободи особи. Тому питання моніторингу дотримання інформаційних прав громадян, особливо в умовах дії режиму воєнного стану, є надзвичайно важливою складовою у забезпеченні інформаційної безпеки, що дозволяє вчасно виявити наявні проблеми і напрацювати рекомендації щодо їх усунення.

Література

1. Щорічна доповідь про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2022 році Уповноваженого Верховної Ради України з прав людини URL: <https://ombudsman.gov.ua/report-2022/informatsiini-prava#doctup-do-informatsii>

Білан І. А.

*науковий співробітник Українського
науково-дослідного інституту
спеціальної техніки та судових
експертиз СБУ*

ПАРЛАМЕНТСЬКИЙ КОНТРОЛЬ ЗА ДІЯЛЬНІСТЮ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Характерною ознакою демократичної держави є наявність системи органів, які здійснюють контрольні функції у сфері діяльності спеціальних служб. Важливу роль у цій системі, незалежно від форми державного правління, відіграють законодавчі органи. Наявність дієвого парламентського контролю гарантує функціонування спеціальних служб у межах чинного законодавства і є запобіжником порушення ними конституційних прав і свобод людини та громадянина [1].

В Україні засади парламентського контролю за діяльністю СБУ визначені Конституцією України, законами України «Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави», «Про національну безпеку», «Про Службу безпеки

України», «Про розвідувальні органи України», «Про контррозвідувальну діяльність», «Про оперативно-розшукову діяльність».

За законодавством України Служба безпеки України підпорядковується Президентові України та підконтрольна Верховній Раді України (ст. Закону України «Про Службу безпеки України», ч. 2 ст. 19 Закону України «Про національну безпеку України»).

Стаття 85 Основного закону України визначила, що до повноважень Верховної Ради України належить, зокрема, затвердження загальної структури, чисельності, визначення функцій СБУ. Внесені у грудні 2004 р. зміни до Конституції України у напрямку парламентсько-президентської форми правління уточнили межі правовідносин між Верховною Радою і СБУ[1].

Згідно з п. 12-1 ст. 85 Конституції України до компетенції Верховної Ради України віднесено призначення на посаду та звільнення з посади за поданням Президента України Голови Служби безпеки України. Відповідно до статті 101 Конституції України парламентський контроль за додержанням конституційних прав і свобод людини і громадянина здійснює Уповноважений Верховної Ради України з прав людини, повноваження якого визначаються законом.

Закон України «Про демократичний цивільний контроль над Воєною організацією і правоохоронними органами держави» містить окремий розділ III «Демократичний цивільний контроль», який визначає основні положення парламентського контролю з боку Верховної Ради України за діяльністю органів сектору безпеки. Цим Законом встановлені особливості у здійсненні цього контролю щодо спеціальних служб, який має проводитися з дотриманням вимог законів України «Про Службу безпеки України», «Про розвідувальні органи України», «Про контррозвідувальну діяльність», «Про оперативно-розшукову діяльність».

Відповідно до ст. 3 Закону України «Про Службу безпеки України» діяльність Служби безпеки України, її органів і співробітників ґрунтується на засадах законності, поваги до прав і гідності особи, позапартійності та відповідальності перед народом України. Постійний контроль за діяльністю Служби безпеки України, дотриманням нею законодавства здійснюється Верховною Радою України (ст. 31 цього Закону).

21 червня 2018 року Верховною Радою України прийнято Закон України «Про національну безпеку України» № 2469-VIII, який набрав чинності 08.07.2018. Відповідно до ст. 6 «Контроль, що здійснюється Верховною Радою України» цього Закону Верховна Рада України:

- здійснює парламентський контроль та приймає закони України, які визначають і регулюють діяльність органів сектору безпеки і

оборони та їхні повноваження, а також затверджує відповідні бюджетні асигнування та приймає рішення щодо звіту про їх використання;

- створює комітети Верховної Ради України, до повноважень яких належить, зокрема, забезпечення контролю за діяльністю органів сектору безпеки і оборони [2].

Згідно з цим законодавчим актом, профільний парламентський комітет має наступні повноваження: аналіз ходу виконання ухвалених Верховною Радою України законів і постанов у сфері національної безпеки і оборони; інформування з цих питань та внесення у встановленому порядку на розгляд Верховної Ради України, Президента України, Кабінету Міністрів України пропозицій щодо вирішення наявних у цих сферах проблем та усунення причин, що їх породжують. Службою безпеки України подаються до Верховної Ради України щорічні письмові звіти про діяльність складових сектору безпеки і оборони (ч. 5 ст. 6 Закону).

Для вивчення, підготовки і попереднього розгляду окремих питань у сфері національної безпеки і оборони, Верховна Рада України уповноважена створювати тимчасові спеціальні комісії, а для проведення розслідування з питань, що становлять суспільний інтерес, – тимчасові слідчі комісії [2].

У свою чергу, народні депутати України можуть: здійснювати право законодавчої ініціативи щодо правового регулювання проблем національної безпеки і оборони; брати участь в обговоренні законопроектів та інших питань, пов'язаних з обороною і безпекою держави, на засіданнях Верховної Ради України, «Днях Уряду України», парламентських слуханнях, у парламентських комітетах і комісіях; звертатися на сесії Верховної Ради України із запитом з питань національної безпеки і оборони до керівників органів державної влади, у тому числі до посадових осіб військових формувань, правоохоронних органів, які зобов'язані у встановлений законом термін повідомити народного депутата України про результати розгляду його запиту [3].

Парламентський контроль за СБУ є важливою складовою реформування останньої.

Ст. 92 проекту Закону України «Про Службу безпеки України (реєстр. № 3080 від 18.02.2020) визначає особливості здійснення парламентського контролю, згідно з якими Верховна Рада України:

- здійснює парламентський контроль за діяльністю Служби безпеки України, в тому числі через уповноважені парламентські комітети, компетенція яких визначається Законом України «Про комітети

Верховної Ради України», іншими законами України та постановами Верховної Ради України;

- приймає закони України, які визначають і регулюють її діяльність та повноваження, а також затверджує відповідні бюджетні асигнування та приймає рішення щодо звіту про їх використання [4].

Наведені особливості визначають межі парламентського контролю за діяльністю спецслужби, які в цілому узгоджуються з європейськими стандартами у цій сфері та законодавчими підходами, вробленими у зарубіжних країнах.

Хоча обсяг повноважень парламентських органів з контролю за діяльністю спецслужб у різних країнах значно різниться залежно від певного історичного розвитку та національної політичної культури.

У деяких країнах (наприклад, США та Велика Британія) профільні парламентські комітети мають право не лише контролювати дотримання законодавства та витрати бюджетних коштів, але й визначати політику та організацію роботи спецслужб. Існує практика делегування парламентом своїх повноважень у сфері контролю за діяльністю спецслужб спеціально утвореним органам або урядовим структурам (наприклад, Норвегія, Бельгія, Канада) [1].

Вважаємо перспективним напрямком вітчизняного законодавця розробку та прийняття Закону України «Про парламентський контроль за дотриманням вимог Конституції та законів України в діяльності спеціальних служб та правоохоронних органів», який би визначав чіткі межі парламентського контролю за діяльністю всіх спецслужб та правоохоронних органів держави.

Здатність парламенту та суспільства в цілому контролювати спеціальні служби є лакмусовим папірцем для перевірки на справжність демократії та верховенства права [1].

Список використаних джерел

1. Паливода В. Парламентський контроль за діяльністю спеціальних служб: іноземний та національний досвід, висновки для України. Аналіт. доповідь. НІСД. URL:<https://niss.gov.ua/en/node/3059>.

2. Про національну безпеку: Закон України від 21 червня 2018 року № 2469-VIII. URL:<https://zakon.rada.gov.ua/laws/show/2469-19#Text>.

3. Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави : Закон України від 19 червня 2003 року №975-IV. URL:<https://zakon.rada.gov.ua/laws/show/975-15/print>.

4. Про Службу безпеки України: законопроект (реєстр. № 3080 від 18.02.2020). URL:<https://itd.rada.gov.ua/billInfo/Bills/Card/1226>.

Дорогих С. О.

кандидат юридичних наук, старший науковий співробітник Державної наукової установи «Інститут інформації, безпеки і права НАПрН України»

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН УКРАЇНИ В УМОВАХ ВІЙНИ

Питання захисту персональних даних громадян України були актуальними ще до початку агресії росії до України 24 лютого 2022 року.

Одним із стратегічних завдань, яке було поставлено у «Стратегії кібербезпеки України» від 14 травня 2021 року [1], було «підвищення ефективності системи захисту персональних даних громадян шляхом гармонізації законодавства України з відповідним законодавством ЄС та посилення відповідальності за порушення встановлених вимог».

Цілком зрозуміло, що під час активної фази збройного протистояння російській агресії проблеми захисту персональних даних громадян України тільки збільшилися. Відповідно ці проблеми потребують осмислення й комплексного реагування у тому числі через правове регулювання суспільних відносин, пов'язаних зі збором, збереженням, обробкою, передачею та захистом персональних даних громадян України.

Окрім того, що персональні дані можуть бути використанні злочинцями та шахраями, під час війни, персональні дані можуть бути використані для інформаційного впливу як на населення так і на окремі його верстви, як наприклад, військовослужбовці ЗСУ та члени їх сімей з метою поширення дезінформації, панічних чуток, дестабілізації внутрішньої соціально-політичної ситуації. Завдяки збору персональних даних, щодо політичних настроїв ворог може вираховувати та знищувати патріотично налаштованих українських громадян на тимчасово окупованій території. Навіть після завершення або припинення збройного конфлікту, персональні дані можуть бути використані для подальшого інформаційного впливу, просування російських наративів, просування політичних сил, які просуватимуть проросійські наративи.

Зазначимо, що із зростанням обсягу персональних даних, які особа залишає про себе у мережі Інтернет, зростає їх цінність для злочинців та держав, які використовують їх як зброю у гібридних та війнах та збройних конфліктах. Зростає й обсяг витоків персональних даних. Так, Індекс споживчої довіри Thales за 2022 показав, що 33% людей у всьому світі постраждали від витоку даних. Дані мільярдів людей були розкриті та вкрадені [2].

Одними з найбільших ресурсів, які займаються накопиченням персональних даних та які являють собою велику проблему є соціальні мережі. Найбільш популярні соціальні мережі, такі як Facebook чи Instagram містять більше ніж чотири мільярди акаунтів [3]. Цінність даних у соціальних мережах полягає у тому, що вони містять не тільки анкетні дані щодо особи, а й зображення з ним, зображення пов'язані з його роботою, місяцями перебування та відпочинку, його знайомими тощо. Аналіз вподобайок, перепостів та матеріалів, що були розміщені у стрічці користувача, може дозволити скласти психологічний портрет особи, отримати уявлення про його політичні та світоглядні вподобання. В ідеалі ці дані не повинні бути використані проти законних інтересів людини й використовуються, наприклад, для контекстної реклами. Але на практиці ці дані можуть бути використані проти інтересів особи, а зібрані у великих обсягах – проти інтересів суспільства та держави.

У той же час рівень захисту даних у соціальних мережах та загальна політика використання персональних даних володільцями соціальних мереж викликає багато питань.

Так витоки з найбільших світові соціальних мереж, таких як, наприклад, Facebook, сягали десятки й сотні мільйони акаунтів користувачів. Та сама мережа Facebook була у центрі скандалу, пов'язаного з доступом до персональних даних третім особам. «Найчастіше використовуваний у світі застосунок для обміну повідомленнями WhatsApp, ймовірно, постраждав від витоку даних, що торкнувся близько 487 мільйонів його користувачів, якщо вірити публікації в даркнеті [4]. Вразливість, яка була присутня в API Twitter у 2021 році, викликала витік даних, який розкрив інформацію про особистий профіль користувачів, торкнувшись не менше 5,4 мільйона з приблизно 200-300 мільйонів користувачів платформи (на той момент) [5]. Й інформація про подібні витоки надходить регулярно.

Наступною проблемою пов'язаною з соціальними мережами, яка потребує відповідного врегулювання є використання соціальних мереж для компрометації державних установ пов'язаних з безпековою сферою для подальшої шпигунської діяльності. Велика кількість інцидентів, пов'язаних з соціальними мережами змусило Міністерство оборони США розробити спеціальні політики, пов'язані як із правилами офіційної присутності співробітників у соціальних мережах так і правил поведження службовцями під час особистого використання соціальних мереж.

Також окремий напрям діяльності Міністерства оборони США полягає у відстеженні фейкових акаунтів, які створюються від імені посадо-

вих осіб та військовослужбовців для подальшої атаки на інших співробітників Міністерства оборони [6].

Нагадаю, що останній резонансний витік таємних документів, який стався у квітні цього року, пов'язаний саме з тим, що військовослужбовець США розмістив таємні документи у соціальній мережі.

Вищезазнані проблеми вимагають правового впорядкування питань, пов'язаних з діяльністю організацій, які володіють соціальними мережами, у яких зареєстровані громадяни України, а саме:

- відповідальність таких організацій за збереження персональних даних;
- перехоплення керування акаунтами громадян України та їх відновлення, а також створення фейкових акаунтів від імені громадян України;
- інформування про витоки, що сталися;
- місце збереження персональних даних громадян України й унеможливлення фізичного знаходження серверів з персональними даними на території країн, державні служби яких можуть перехоплювати та викрадати персональні дані тощо.

Бажано, щоб при регулюванні перерахованих проблем законодавство України було гармонізовано з відповідним законодавством країн Європейського Союзу, Великобританії та Сполучених Штатів, як головних стратегічних союзників України у сфері безпеки.

Зазначимо, що незважаючи на те, що світові гіганти в інформаційній сфері мають мільярдні статки та значний вплив, але вже існує велика практика притягнення їх до відповідальності у країнах Європи. Наведемо лише декілька прикладів введення санкцій на найбільших гравців ринку світових соціальних мереж, що відбулися наприкінці 2022 – початку 2023 років.

На початку 2023 року Французьке агентство захисту даних наклало штраф у розмірі 5 мільйонів євро на платформу коротких відео соціальних мереж TikTok, заявивши, що китайська компанія порушила національний закон про конфіденційність, що обмежує моніторинг активності веб-браузера [7]. Також Франція наклала найбільший за рік штраф на техгіганта Microsoft у сумі 60 млн євро за політику збору даних користувачів у пошуковику Bing. Французький регулятор заявив, що після розслідування виявив, що «коли користувачі відвідували цей сайт, файли cookie зберігалися на їхньому терміналі без згоди, при цьому ці файли використовувалися, серед іншого, в рекламних цілях [8]. Ірландська комісія із захисту даних (DPC) оштрафувала Meta на 265 мільйонів євро (275,5 мільйона доларів) за масовий витік даних Facebook у 2021 році, в

результаті якої було розкрито інформацію сотень мільйонів користувачів по всьому світу [9].

Отже, на нашу думку, Україна також повинна регулювати відносини, пов'язані з захистом персональних даних громадян України у світових соціальних мережах, диктувати ті правила, які би відстоювали законні інтереси громадян України.

Підсумовуючи, відмітимо, що вищепераховані проблеми – лише окремі епізоди в сфері захисту персональних даних громадян. Окрім них є багато інших пов'язаних проблем, як наприклад, придбання й використання спеціального програмного забезпечення, призначеного для зламу смартфонів та відстеження осіб у рамках боротьби із злочинністю, для відстеження опозиційних політиків та журналістів авторитарними режимами; цілеспрямований збір персональних даних такими країнами як Китай, Росія та деякі інші для шпигування та впливу на внутрішні політичні процеси у демократичних країнах тощо.

Все це потребує системного правового врегулювання та гармонізації законодавства України про захист персональних даних із законодавством провідних західних країн.

Список використаних джерел

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 р. № 447/2021 URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>.

2. Millions of Emails Leaked in Crypto Data Breach; Google, Apple Release Device Security Updates. *Techstrong Group Inc.* URL: <https://securityboulevard.com/2022/12/millions-of-emailsleaked-in-crypto-data-breach-google-apple-release-device-security-updates>.

3. Anna Delaney. Facebook, Instagram Blasted for 'Lame' Security Practices. *Information Security Media Group, Corp.* URL: <https://www.govinfosecurity.com/facebook-instagram-blasted-forlame-security-practices-a-21022>.

4. Scott Ikeda. Nearly 500 Million WhatsApp Records Allegedly Stolen in Data Leak, Offered on Dark Web for a Few Thousand Dollars. *CPO Magazine.* URL: <https://www.cpomagazine.com/cyber-security/nearly-500-million-whatsapp-recordsallegedly-stolen-in-data-leak-offered-on-dark-web-for-a-few-thousand-dollars>.

5. Scott Ikeda. Data Leak Exposes Private Profile Information of 5.4 Million Twitter Users, Dumped for Free on Underground Forum. *CPO Magazine.* URL: <https://www.cpomagazine.com/cyber-security/data-leak->

exposes-private-profileinformation-of-5-4-million-twitter-users-dumped-for-free-on-underground-forum.

6. Brian Kime. PERSPECTIVE: Military Leaders Must Lead from the Front on Social Media's Strategic Opportunities and Risks. *Homeland Security Today*. URL: <https://www.hstoday.us/subject-matter-areas/cybersecurity/perspective-militaryleaders-must-lead-from-the-front-on-social-medias-strategic-opportunities-and-risks>.

7. Akshaya Asokan. French CNIL Fines TikTok 5 Million Euros for Cookie Policies. *Information Security Media Group, Corp.* URL: <https://www.govinfosecurity.com/frenchcnil-fines-tiktok-5-million-euros-for-cookie-policies-a-20928>.

8. Франція оштрафувала Microsoft на 60 мільйонів євро. *UA. NEWS*. URL: <https://ua.news/ua/technologies/frantsiya-oshtrafovala-microsoft-na-60-millionov-evro>.

9. Bill Toulas. Meta fined €265M for not protecting Facebook users' data from scrapers. *Bleeping Computer®*. URL: <https://www.bleepingcomputer.com/news/security/meta-fined-265m-fornot-protecting-facebook-users-data-from-scrapers/>. 28.11.2022.

Лазор О. Д.

*доктор наук з державного управління,
професор, професор кафедри публічного
управління та адміністрування
Вінницького державного педагогічного
університету імені Михайла
Коцюбинського*

Лазор О. Я.

*доктор наук з державного управління,
професор, професор кафедри публічного
управління та адміністрування
Вінницького державного педагогічного
університету імені Михайла
Коцюбинського*

ОПРИЛЮДНЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ ФІЗИЧНОЇ ОСОБИ: ПРАВОВЕ РЕГУЛЮВАННЯ ПИТАНЬ

З питань отримання, опрацювання, розпорядження різного роду інформації про фізичну особу законодавець прийняв низку нормативно-

правових актів щодо регулювання цієї сфери діяльності. Найбільшим масивом інформації про фізичну особу здебільшого володіють роботодавці, яким самі працівники дозволяють опрацювати свої персональні дані, часом і не замислюючись про наслідки. Проте, до сьогодні чинним законодавством чітко не врегульовано окремі питання, зокрема і відмови особи від надання такої згоди.

Надаючи свої персональні дані та відповідно згоду на їх опрацювання, працівник має право знати з якою метою відбуватиметься вказана процедура, кому може бути передана ця інформація і для чого, на яких підставах та за яких умов особа може відкликати опрацювання своїх персональних даних та які будуть наслідки вчинених ним таких дій.

Так, з одного боку, відповідно до ст. 302 Цивільного Кодексу України [5], фізична особа має таке право вільно збирати, зберігати, використовувати та поширювати інформацію, зокрема щодо своєї особистості. Однак, такі дії стосовно іншої фізичної особи, а саме щодо її особистого життя, за відсутності від неї такої згоди – не допускаються. Адже, фізична особа має право на особисте життя, визначає його, як і можливість ознайомлення з ним інших осіб, або не надає такої можливості, оскільки має право «на збереження у таємниці обставин свого особистого життя», що підтверджуються положеннями ст. 301 цього ж Кодексу. Лише за умови, що обставини особистого життя фізичної особи «містять ознаки правопорушення, що підтверджено рішенням суду, а також за її згодою», можуть бути розголошені іншими особами.

Водночас, відповідно до ч. 2 ст. 302 Цивільного Кодексу України, фізична особа, яка поширює інформацію, зобов'язана переконатися в її достовірності та зробити покликання на джерело. Якщо інформація отримана з офіційних джерел, зокрема від суб'єктів владних повноважень, то у такому випадку це звільняє фізичну особу, яка поширює інформацію, від необхідності перевірки її достовірності та відповідальності за необхідності спростування наданої інформації.

Відповідно до ч. 5 ст. 4 Закону України «Про захист персональних даних» [2], «Розпорядник персональних даних може обробляти персональні дані лише з метою і в обсязі, визначених у договорі». У більшості договорів із роботодавцем не зазначено, що він, як розпорядник, може поширювати ці персональні дані без відповідної згоди.

Згідно із ч. 2 ст. 5 цього ж Закону «Персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. Не є конфіденційною інформацією персональні дані, що стосуються здійснення особою, уповноваженою на виконання функцій держави або місцевого самоврядування, посадових або службових повноважень».

Позиція законотворця щодо сутності конфіденційної інформації викладена у ст. 7 Закону України «Про доступ до публічної інформації» [1], де з її змісту зрозуміло, що конфіденційною є та інформація «доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов». Водночас нормами цієї статті конкретизуються дії розпорядників інформації щодо її поширення за умови відсутності такої згоди, тобто «лише в інтересах національної безпеки, економічного добробуту та прав людини».

З урахуванням останніх змін від 03.11.2022 р. абз. 1 ч. 2 ст. 21 Закону України «Про інформацію» [3] сутність конфіденційної інформації дещо розширена, а саме конфіденційною вважається інформація:

- про фізичну особу;
- доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень;
- визнана такою на підставі закону.

Якщо інформація про фізичну особу вважається конфіденційною, а отже є інформацією з обмеженим доступом, а відтак може поширюватися лише за бажанням (згодою) відповідної особи, у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом.

З огляду на викладене вище, інформація про працівників, які не належать до суб'єктів владних повноважень і які згоди щодо поширення персональних даних не надавали, розповсюджувати чи передавати її розпорядником заборонено.

В абзаці 3 ч. 1 ст. 6 Закону України «Про захист персональних даних» [2] чітко визначено, що за умови зміни визначеної мети обробки персональних даних на іншу – нову мету, яка є несумісною з попередньою, для подальшого опрацювання відповідної інформації володілець персональних даних зобов'язаний «отримати згоду суб'єкта персональних даних на обробку його даних відповідно до зміненої мети, якщо інше не передбачено законом».

Одним із актуальних питань є оприлюднення заробітної плати службовців різного штибу, інформація, якою часто цікавляться журналісти. У ч. 1 ст. 13 Закону України «Про доступ до публічної інформації» [1] зазначено посади осіб, заробітна плата яких не належить до категорії конфіденційної інформації, а саме: «керівника, заступника керівника, особи, яка постійно або тимчасово обіймає посаду члена виконавчого органу чи входить до складу наглядової ради». Указані

особи заповнюють та подають відповідні декларації, що є їй у широкому доступі та відповідно не складає труднощів у їх пошуку. Заробітні плати усіх інших працівників, посади яких у цьому переліку відсутні – є конфіденційною інформацією й оприлюднюються лише за згодою володільця цих даних.

Водночас норми ст. 31 Закону України «Про оплату праці» [4] також вказують на те, що: «Відомості про оплату праці працівника надаються будь-яким органам чи особам лише у випадках, передбачених законодавством, або за згодою чи на вимогу працівника», підтверджуючи тим самим конфіденційність цієї інформації.

Відповідно до положень ст. 11 Закону України «Про інформацію» [3], лише Центральний орган виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику, під час здійснення повноважень щодо верифікації та моніторингу державних виплат не потребує згоди фізичних осіб на отримання та обробку персональних даних.

Хибною є позиція, що Закон України «Про доступ до публічної інформації» забороняє обмежувати доступ до інформації про розпорядження бюджетними коштами, оскільки заробітна плата та інші виплати (премії, матеріальна допомога тощо) посадовим та службовим особам є витратами з бюджету. У цій частині необхідно розрізняти особливості організаційно-правового статусу працівників відповідної організації, установи чи підприємства як володільців персональних даних, врешті як і самого органу публічної влади.

Чинне законодавство, а саме положення ст. 10 Закону України «Про доступ до публічної інформації» гарантують кожній особі, яка має право: знати у період збирання інформації, але до початку її використання, які відомості про неї та з якою метою збираються, як, ким і з якою ціллю вони використовуються, передаються чи поширюються, крім випадків, встановлених законом.

Убезпечує від неправомірних дій володільця персональних даних і положення ч. 3 ст. 10 цього ж закону, де передбачено, що розпорядники інформації, які володіють інформацією про особу, зобов'язані: «вживати заходів щодо унеможливлення несанкціонованого доступу до неї інших осіб».

Підсумовуючи викладений аналіз законодавчих норм, необхідно розуміти, що працівник, надаючи згоду на опрацювання персональних даних роботодавцеві, аж ніяк не означає, що розпорядник може поширювати чи оприлюднювати відому йому інформацію про особу без додаткових узгоджень із суб'єктом персональних даних.

Список використаних джерел

1. Про доступ до публічної інформації : Закон України від 13 січня 2011 року № 2939-VI. URL : <https://zakon.rada.gov.ua>
2. Про захист персональних даних : Закон України від 1 червня 2010 року № 2297-VI. URL : <https://zakon.rada.gov.ua>
3. Про інформацію : Закон України від 2 жовтня 1992 року № 2657-XII. URL : <https://zakon.rada.gov.ua>
4. Про оплату праці : Закон України від 24 березня 1995 року № 108/95-ВР. URL : <https://zakon.rada.gov.ua>
5. Цивільний Кодекс України від 16 січня 2003 року № 435-IV. URL : <https://zakon.rada.gov.ua>

Заславська Л. В.

старший науковий співробітник

Державної наукової установи

«Інститут інформації, безпеки і права

НАПрН України»

ПРОБЛЕМИ ПРИТЯГНЕННЯ ДО ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА РОЗПОВСЮДЖЕННЯ АНТИУКРАЇНСЬКОЇ ПРОПАГАНДИ В УМОВАХ ВОЄННОГО СТАНУ

Вільний доступ до інформації та свобода слова є одними з найважливіших принципів демократичного суспільства. Однак у сучасному світі ці принципи нерідко стикаються з проблемами та викликами, зокрема з розповсюдженням пропаганди. Питання протидії пропаганді та її впливу на суспільство є актуальними у світі і в Україні також, особливо з урахуванням складної політичної та геополітичної ситуації в країні. Україна, як і інші країни світу, має свої власні проблеми у цій сфері. Особливо гострою є ця проблема в контексті сьогоденішнього повномасштабного збройного вторгнення РФ на територію України.

Однією з ключових проблем, які виникають у контексті протидії пропаганді, є питання притягнення до відповідальності за її розповсюдження. Це питання має велике значення для забезпечення правопорядку та свободи слова в Україні. Головною проблемою при притягненні до відповідальності осіб за поширення пропаганди в Україні є складність визначення того, що саме є пропагандою та масштабів її впливу. Російська пропаганда, зокрема, була та є на сьогодні важливою проблемою в Укра-

їні, коли Кремль зображував Україну як державу, яка страждає на корупцію, безвладдя та бідність [1]. Однак пропаганда може маскуватися під проукраїнські наративи, що ускладнює виявлення та притягнення до відповідальності винних [2]. Крім того, пропаганда часто представляє себе як законну точку зору, що ускладнює розмежування між пропагандою та свободою слова. Як наслідок, визначення пропаганди та її масштабів є складним питанням, яке потребує ретельного розгляду та юридичної експертизи.

Іншою значною проблемою при притягненні до відповідальності осіб за поширення пропаганди в Україні є відсутність чіткої правової бази та механізмів реалізації. Незважаючи на те, що українські законодавці активно формують правову базу для протидії російській пропаганді, все ще існує потреба в більш комплексному підході для вирішення цього питання [3]. Крім того, бракує ресурсів і досвіду для забезпечення дотримання існуючих законів, що ускладнює притягнення осіб до відповідальності за поширення пропаганди.

На сьогоднішній день існує чимало важелів у законодавстві України щодо боротьби з пропагандою, а саме: Закон України № 2265-IX «Про заборону пропаганди російського нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну», норми Кримінального кодексу, що містять подібні склади злочинів: щодо колабораційної діяльності (стаття 111-1), публічні заклики до агресивної війни (стаття 436), виготовлення, поширення комуністичної, нацистської символіки (стаття 436-1) та виправдання чи визнання правомірною агресією (стаття 436-2) [4]. Наразі у Верховній Раді зареєстрований проєкт Закону України № 7215 про внесення змін до Кримінального кодексу України та Кримінального процесуального кодексу України щодо відповідальності за пропаганду російського неонацистського тоталітарного режиму, акту агресії проти України з боку Російської Федерації як держави терориста. Законодавці пропонують додати нову статтю до Кримінального кодексу України, що передбачає відповідальність як за пропаганду російського режиму, так і за використання забороненої символіки держави-терориста. Серед санкцій – обмеження або позбавлення волі на строк до 5 років, з конфіскацією майна або без такої, а за наявності кваліфікуючих ознак (серед яких використання медіа) – до 10 років позбавлення волі. Але чи правомірними є такі обмеження? З огляду на те, що російська агресія не припиняється та продовжує забирати життя тисяч українців, а з боку представників органів влади рф все частішають заклики до геноциду проти українсько-

го народу, заборона на поширення пропаганди російського нацистського тоталітарного режиму є виправданою для захисту національної безпеки України [3].

Також великою проблемою у боротьбі з пропагандою на сьогоднішній день є використання соціальних мереж та месенджерів для розповсюдження фейкової та пропагандистської інформації. Така інформація може впливати на громадську думку та створювати додаткові проблеми для збереження миру та стабільності в країні. 19 квітня 2023 року Верховна Рада оприлюднила Проект Закону № 9923 «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо встановлення відповідальності за окремі дії проти основ національної безпеки України». Проект пропонує притягувати користувачів онлайн-платформ до кримінальної відповідальності за використання облікових записів для поширення недостовірної інформації та втручання в діяльність органів влади задля захисту інформаційної безпеки України [5]. На жаль згаданий законопроект має багато дискусійних питань, зокрема, щодо порушення прав «споживачів» інтернет-платформ.

Наразі в Україні існує ряд нормативно-правових актів, які регулюють відповідальність за розповсюдження пропаганди та встановлюють вимоги до ЗМІ та їхньої діяльності. Проте законодавство, що регулює цю сферу, має свої недоліки та не завжди є ефективним у практичному застосуванні. З одного боку, притягнення до відповідальності за поширення пропаганди може бути ефективним інструментом боротьби з дезінформацією та захисту національної безпеки. З іншого боку, можливість застосування цього інструменту може порушувати свободу слова. Крім того, багато випадків порушення правових норм у питаннях протидії пропаганді залишаються без належної уваги з боку правоохоронних органів, що призводить до того, що пропаганда поширюється далі.

Очевидно, що необхідно продовжувати удосконалювати правове поле у питання протидії пропаганді в Україні як на законодавчому так і на рівні підзаконних правових актів. Створювати нові механізми протидії розповсюдженню пропаганди. Крім того, необхідно підвищити рівень усвідомленості населення щодо шкідливості пропаганди та наслідків її розповсюдження, тобто системно формувати та підвищувати інформаційну грамотність своїх громадян.

Також важливим є забезпечення відповідної реакції правоохоронних органів на порушення законів про пропаганду. Необхідно забезпечити більшу підтримку та розвиток спеціалізованих підрозділів правоохоронних органів, які займаються боротьбою з пропагандою та розповсюдженням фейкової інформації.

У цілому, розв'язання проблеми притягнення до відповідальності за розповсюдження пропаганди потребує комплексного підходу, що передбачає удосконалення законодавства, підвищення рівня усвідомленості населення та забезпечення ефективної діяльності правоохоронних органів.

Список використаних джерел

1. Мета російської пропаганди – посіяти зневіру і параною. Як протидіяти. Режим доступу: https://texty.org.ua/articles/70089/Meta_rosijskoji_propagandy_posijaty_zneviru_i-70089/. Дата звернення 9.05.2023 р.

2. Російська пропаганда – як розпізнати та протистояти. Режим доступу: <https://suspilne.media/343150-raketi-zapuskae-rosia-a-agresiu-mi-remikaemo-na-ukrainu-kropivnicka-naukovica-pro-rosijsku-propagandu//>. Дата звернення 9.05.2023 р.

3. Україна проти рашизму: нове законодавство для протидії російській пропаганді? Режим доступу: <https://dslua.org/publications/ukraina-protu-rashyzmu-nove-zakonodavstvo-dlia-protydii-rosiyskiy-propahandi/>. Дата звернення 9.05.2023 р.

4. Кримінальний Кодекс України. Режим доступу: https://zakon.rada.gov.ua/laws/show/2341-14?find=1&text=110#w1_6. Дата звернення 9.05.2023 р.

5. Криміналізація ботів чи заборона анонімності та дискусій в соцмережах: що пропонує Проект № 9923? Режим доступу: <https://dslua.org/publications/proekt-9923/> Дата звернення 9.05.2023 р.

Дурач О. А.

старший викладач Вінницького

національного аграрного

університету, голова

Великоновосілівського районного суду

Донецької області

ПРОБЛЕМНІ ПИТАННЯ СУДОВОГО РОЗГЛЯДУ ВІЙСЬКОВИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

До початку військових дій у Державі, на сході України, існувала ілюзія щодо непотрібності військової підготовки громадян, збройних сил, військової юстиції, військових судів. Проведення на Сході України анти-терористичної операції, подальше вторгнення ворога на територію Дер-

жави 24.02.2022 р. змусило переосмислити необхідність у таких інституціях.

Однією зі вказаних інституцій, яка потребує певної підготовки у сфері безпосереднього розгляду військових кримінальних правопорушень і є судова система.

Логічним завершенням досудового розслідування вказаної категорії кримінальних правопорушень є передача справи до суду, який буде здійснювати швидкий, справедливий та неупереджений розгляд вказаних справ. При цьому суд повинен мати відповідний фах, достатню компетенцію для прийняття правильних та обґрунтованих рішень.

Починаючи з 2014 року, суди трьох інстанцій розглядають провадження щодо військових кримінальних правопорушень. Натомість, до теперішнього часу, умови для своєчасного та ефективного розгляду вказаної категорії справ не створені.

Так, не можна забувати про такий важливий і необхідний критерій розгляду вказаних справ, як швидкість. Саме забезпечення швидкості розгляду військових кримінальних правопорушень сприятиме повноті та об'єктивності їх розгляду. Обвинувачені, свідки по даним справам після вчинення більшості вказаних правопорушень продовжують виконувати свої військові обов'язки, забезпечення їх явки до суду зумовлено певними складнощами, у будь-якому випадку, потрібен бути дотриманий баланс між нагальністю розгляду кримінального провадження та необхідністю військовослужбовця (неважливо в якому статусі) бути присутнім при виконанні бойових завдань. Потрібно також враховувати, що зі плином часу втрачається можливість щодо забезпечення повноцінного розгляду справи, з викликом свідків, які пам'ятатимуть обставини подій, та й самих обвинувачених, які психологічно зосереджені не лише на розгляді проваджень щодо них, а головним чином на військових подіях, що є зрозумілим. Тут у нагоді стає можливість дистанційного розгляду кримінальних проваджень, на практиці, військовослужбовець під час розгляду справи прибуває до суду, найбільш територіально наближеного до його локації для участі у розгляді справи у режимі відеоконференції. Натомість, справжньою проблемою є можливість проведення відеоконференції зі вказаними учасниками лише з приміщення суду. Так, відповідно до вимог ч. 1 ст. 336 КПК України судове провадження може здійснюватися у режимі відеоконференції під час трансляції з іншого приміщення, у тому числі яке знаходиться поза межами приміщення суду (дистанційне судове провадження), у разі неможливості безпосередньої участі учасника кримінального провадження у судовому провадженні за станом здоров'я або з інших поважних причин; необхід-

ності забезпечення безпеки осіб; проведення допиту малолітнього або неповнолітнього свідка, потерпілого; необхідності вжиття таких заходів для забезпечення оперативності судового провадження; наявності інших підстав, визначених судом достатніми. При цьому з метою забезпечення реалізації положень вказаної статті КПК України та встановлення єдиного порядку роботи з технічними засобами відеозапису ходу і результатів процесуальних дій, проведених у режимі відеоконференції під час судового засідання (кримінального провадження), Наказом Державної судової адміністрації України від 15 листопада 2012 року № 155 було затверджено Інструкцію про порядок роботи з технічними засобами відеозапису ходу і результатів процесуальних дій, проведених у режимі відеоконференції під час судового засідання (кримінального провадження) (далі-Інструкція). Пунктом 1.2.1 вище вказаної Інструкції передбачено, що учасники судового процесу (кримінального провадження) можуть брати участь у процесуальних діях у режимі відеоконференції лише за наявності технічної можливості для її проведення у відповідних судах, державних органах чи установах. Обов'язок забезпечити проведення відеоконференції покладається на суд, який отримав судові рішення про проведення відеоконференції, незалежно від спеціалізації та інстанції суду, який прийняв таке рішення (п. 5 Інструкції). Лише в цьому випадку може бути забезпечено реалізацію положень ч. 4, 6 ст. 336 КПК, яка передбачає обов'язок суду, судового розпорядника або секретаря судового засідання (службової особи установи попереднього ув'язнення або виконання покарань) вручити особі, яка бере участь у судовому засіданні в режимі відеоконференції, пам'ятку про її процесуальні права та перевірити її документи, що посвідчують особу. Виходячи з викладеного, у кримінальному провадженні всі питання проведення процесуальних дій у режимі відеоконференції (дистанційне судове провадження) під час судового провадження визначено ст. 336 КПК України. Однак, проведення відеоконференції зв'язку під час судового засідання за участі сторін поза межами приміщення суду за допомогою власних технічних засобів учасників цією нормою не передбачено». Таким чином, враховуючи навантаженість судді суду, наприклад, першої інстанції (який, до речі, розглядає справи кримінальні, цивільні, про адміністративні правопорушення та деякі категорії адміністративних проваджень), при цьому з тих чи інших причин у судовій системі вакантними є понад дві тисячі посад суддів, кількість цих вакансій збільшується із кожним днем у зв'язку з поданням суддями заяв або про відставку, або про звільнення за власним бажанням, а також беручи до уваги обмежену кількість залів судових засідань інших судів, на яких покладається обов'язок забезпечити відеоконферен-

цію під час розгляду вказаних проваджень, таке поняття як швидкість і своєчасність розгляду даних кримінальних правопорушень нівелюється. Можливим виходом з даної ситуації є забезпечення можливості участі обвинувачених та свідків по вказаним провадженням за допомогою відеоконференції з власних засобів. При цьому доцільно було би покласти обов'язок вручення відповідних пам'яток про їх процесуальні права на сторону обвинувачення під час проведення досудового розслідування.

Також, нагальним постає питання щодо якості розгляду вказаних кримінальних проваджень. З 2014 р. року судді мають певний досвід розгляду даних проваджень, але його не можна вважати достатнім. Періодично, з початку повномасштабної війни, проводяться семінари та тренінги з судьями з цих питань. До участі у вказаних тренінгах запрошуються викладачі національної школи суддів, судді вищих інстанцій. Натомість, не згадуються судді, які працювали у колишніх військових судах, які були ліквідовані у 2010 році, проте, вважаю, що їх досвід також повинен враховуватись.

З огляду на наведене, шляхом вирішення проблемних питань розгляду військових кримінальних правопорушень, вважаю відновлення роботи військових судів або у формі окремої палати при судах апеляційної та касаційної інстанції та визначення окремої юрисдикції певної кількості суддів першої інстанції, зі звільненням їх від розгляду інших категорій справ, або у формі відновлення роботи повноцінних військових судів на постійній основі, або лише на період воєнного стану. У такому випадку, буде забезпечуватись в повній мірі вимога щодо швидкості, своєчасності (за умови внесення змін в КПК України щодо можливості участі учасників справи у режимі відеоконференції), ефективності та якості розгляду вказаних категорій справ (судді спеціалізуюватимуться лише на розгляді кримінальних військових кримінальних правопорушень).

І, для довідки, хочу зазначити наступне. За 2013 рік до суду направлено 265 справ про військові кримінальні правопорушення; за 2014 рік – 904, за 2015 рік – 3139, за 2016 рік – 3420, за 2017 рік – 3572, за 2018 рік – 2505, за 2019 рік – 2701, за 2020 рік – 1842, за 2021 рік – 2009, за 2022 рік – 2822. Вказану інформацію отримано мною у відповідь на запит до офісу Генерального прокурора України від 04.04.2023 р. З наведених даних можна прослідкувати не лише статистичні дані щодо військових кримінальних правопорушень, а й динаміку порушених проваджень, які надійшли до суду в залежності від інтенсивності бойових дій на території Держави. Виходячи з цього, можна моделювати конструкцію, за якою можливе відновлення роботи військових судів в Україні.

Качинський А. Б.

*доктор технічних наук, професор,
радник Секретаря РНБО України
на громадських засадах, Рада
національної безпеки і оборони
України*

Шаповалов А. А.

*виконуючий обов'язки керівника
Центру протидії дезінформації при
Раді національної безпеки і оборони
України*

СУЧАСНІ МЕТОДИ АНАЛІЗУ ПРОПАГАНДИСТСЬКИХ КАМПАНІЙ В УМОВАХ ВІЙНИ

Сучасні дослідники зазначають, що аналіз пропаганди – це серйозне дослідження, спрямоване на визначення цілі пропагандистської кампанії [1; 2; 3; 4]. Однак в умовах війни окремої оцінки заслуговує робота Джоуэта Г., О'Доннела В. [5]. Автори запропонували план аналізу пропаганди з десяти кроків, що враховує використання сучасних мас медіа, де пропаганда розглядається як умисна та систематична спроба формування сприйняття, маніпуляції пізнанням і спрямування поведінки для досягнення реакції, бажаної пропагандисту.

Розглянемо такий підхід в контексті російсько-української війни.

Крок 1. Ідеологія і ціль пропагандистської кампанії

Історичні дослідження показали, що головною метою пропаганди є прийняття народом пропагандистської ідеології. Так після того, як нацисти захопили владу в 1933 році, Гітлер створив імперське міністерство народної освіти і пропаганди для впливу на громадську думку та поведінку населення Німеччини. Нацисти ефективно використовували пропаганду, щоб завоювати підтримку мільйонів німців за демократичного ладу, а згодом за диктатури, щоб організувати переслідування, розв'язати війну та здійснити геноцид. Ідеєю для ідеологічної системи нацизму була ідея расової вищості німецької нації, а також – виняткова роль держави у відродженні слави древнього Риму.

Наріжним каменем радянської пропаганди була ідеологія марксизму-ленінізму. Критики вважають марксизм-ленінізм догматичною тоталітарною ідеологією. Як і всяка релігійно-ідеологічна догматична система марксизм-ленінізм силоміць насаджувався як власному народові, так і залежним державам-сателітам.

Нині один з найпопулярніших промоутерів Кремля – Ігор Ашманов, пояснює російській аудиторії, що гугл, фейсбук і твітер – ідеологічна зброя, націлена на росію [1]. Його велика ідея – «цифровий суверенітет»: уряд контролює, до якої інформації має доступ населення. На його думку, інформаційний суверенітет недосяжний поки немає ідеології, що захищає ваші підходи у перешкоджанні одним потоком інформації на користь інших.

Повномасштабне вторгнення росії в Україну показало, що реальні погляди господаря Кремля, які він прищепив і мільйонам росіян, значно жорстокіші й небезпечніші, ніж політична ностальгія за СРСР під православними іконами. Сукупність цих поглядів утворюють ідеологію «рашизму». Рашизм – це дивна постмодерністська суміш куди увійшли шовіністичний і великоросійський світогляд давно неіснуючої російської імперії, ностальгія за СРСР, реваншистські настрої пострадянських силовиків, псевдоісторичні екскурсії Путіна, а також православ'я з одночасним вшануванням Миколи II і Сталіна. Культурно відстала, варварська Московія історично завжди здійснювала агресивну експансію щодо України. Очевидно, що нинішня ідеологія рашизму базується на цьому історичному досвіді москви, а базовою ідеєю є консервація культурної відсталості і руйнування розвинутих цивілізацій.

Метою пропаганди може бути агітація людей до прийняття переконань і поглядів, які сприяють переконанням і поглядам пропагандиста, або прояву визначених моделей поведінки.

Крок 2. Контекст, у якому здійснюється пропаганда

Для здійснення успішної пропагандистської кампанії, її ідеологія має відповідати атмосфері часу та настроям цільової аудиторії. Аналіз пропаганди має обов'язково включати дослідження історичного підґрунтя. Особливо це стосується міфів, історичних стереотипів як моделей соціальних дій.

Аналітик, який аналізує пропаганду, має докладно знати події, що мали місце, їх сприйняття аудиторією. Оцінювати перспективи розвитку світової соціальної й економічної системи, панівні соціальні настрої, конкретні проблеми, їх відчуття громадськістю, обмеження, що не дають змогу їх вирішити, основних гравців у боротьбі за владу.

Крок 3. Ідентифікація пропагандиста

Швидше всього, джерелом пропаганди є установа, заклад, лідер або агентом є пропагандист. Щодо відкритості пропаганди: часом вдається легко ідентифікувати пропагандистську організацію; коли ідентичність організації прихована, до тих пір поки не будуть встановлені всі факти, – це може стати складним завданням.

Коли пропагандист – людиною, принципи ідентифікації його особи можна знайти в пропонованій ним ідеології, цілях і контексті пропагандистського повідомлення. Гірша ситуація, коли ця людина є агентом або «прикриттям» для справжнього пропагандиста. В такому разі використовуються спеціальні методи дослідження або здійснюються спеціальні заходи.

Крок 4. Структура пропагандистської організації

Враховуючи важливість даного кроку аналізу пропаганди, для кожного випадку його необхідно розглядати окремо.

Крок 5. Цільова аудиторія

Донедавна цільовою аудиторією для пропагандиста була масова аудиторія, але зараз це не так. Завдяки пропаганді та майстерній роботі з соцмережами ІДІЛ змогла домогтися глобальної присутності та стати потужним каналом вербунку. Вивірені, гарно змонтовані відео були націлені на молодих невдоволених мусульман не лише в арабському світі та Центральній Азії, але й у решті Азії і, зокрема, в іммігрантських ісламських спільнотах в Європі та Північній Америці.

Сучасні інформаційні технології разом з маркетинговими дослідженнями надивовиж легко дають змогу ідентифікувати цільову аудиторію (наприклад, списки масової Email-розсилки можна легко придбати й погодити з реакцією аудиторії на звернення ЗМІ). Використовуючи такий підхід, терористичні організації збирають інформацію про користувачів, які переглядають їх веб-сайти. З іншого боку, мас-медіа можуть створювати власну аудиторію.

Пропагандист вибирає цільову аудиторію, рахуючись з потенційною ефективністю: його повідомлення спрямовані, в першу чергу, на аудиторію, яка у випадку позитивної реакції, буде йому корисна.

Очевидно, що масова комунікація в різній формі буде задіяна й надалі, але вона буде використовуватися в комбінації з іншими типами аудиторії, такими як невеликі групи, групи по інтересах, групи культурних і політичних еліт, лідери думок, групи окремих реципієнтів тощо.

Крок 6. Методи використання мас-медіа

На перший погляд, завдання ідентифікації та дослідження джерела інформації щодо здійснення пропаганди, може видатися легким. Сучасна пропаганда використовує всі можливі засоби масової інформації, тому аналітик вивчає всю сукупність ЗМІ, яку використовує пропагандист.

Для того щоби визначити цілі пропагандиста аналітик має порівнювати різні повідомлення, що надходять з одного й того самого джерела. Також він має досліджувати комунікаційні потоки від одного джерела інформації до іншого, від ЗМІ до груп і до окремих осіб. Досліджувати

взаємовідносини між ЗМІ та людьми, приділяючи увагу способам використання мас-медіа.

Крок 7. Спеціальні методи для максимізації впливу

Сукупність методів пропагандиста для впливу на цільову аудиторію вкрай різноманітна [1; 2; 3]. Ми притримуємося думки цих авторів про те, що пропаганду необхідно оцінювати за її цілями. А це можуть бути бажані пропагандистом настанови, переконання, цінності або зміна поведінки.

Схильність аудиторії: створення відгуку. Повідомлення є більш впливовими, коли вони відповідають уже усталеним думкам, схильностям і переконанням. За рахунок чого вони стають більш актуальними: виходять, швидше, зі самої аудиторії, ніж зовні.

Довіра до джерела. Авторитетна думка ефективна при встановленні законності змін і пов'язана з контролем інформації. Люди схильні рівнятися на авторитетні особи щодо знань і напрямків діяльності поведінки.

Лідери громадської думки. Лідери громадської думки користуються довірою людей.

Заохочування та покарання. Це ще один практичний спосіб схвалення ідей або ідеології.

Монополія на джерело комунікації. У людей не викликають підозру джерела- монополісти комунікації, а повідомлення є послідовними та повторюваними.

Візуальні символи влади. Пропагандисти давно активно використовують візуальні символи влади: прапори, герби, різну ідеологічну символіку тощо. Так, коли російський пропагандист Соловійов у себе в телеграм-каналі стверджує, що український герб – це «нацистський символ». У той час, про схожість свастики та рашистської нашивки «Z», що стала символом російського вторгнення в Україну, годі й говорити.

Використання мови. Використання мови, яка пов'язана з авторитетними фігурами, надає авторитет тому, що описує ця мова. Словесна символізація впливає на реципієнта у відповідності до його асоціацій, що виникають у нього у зв'язку зі символами. У такий спосіб пропагандист використовує мову, яка може допомогти мобілізувати її прихильників до закликів до сепаратизму, відокремлення тощо і сатанізувати супротивника. Саме мовний фактор росія використала як головний привід до агресії – пояснивши її потребою захисту російськомовних громадян в Україні.

Музика як пропаганда. Музика та реакція на неї вкрай ефективним способом пропаганди. З погляду пропагандиста, музика ефективна тому, що вона поєднує в собі звук, слова і повторюється до тих пір, поки не засвоється слухачем.

Збудження емоцій. Емоції та повтор – два наріжних камені пропаганди. Також часто зазначають, що емоції – це головна зброя пропаганди, яка тісно пов'язана з емоційною мовою й презентаціями.

Крок 8. Реакція аудиторії на різні методи

Тут аналітик шукає докази реакції цільової аудиторії на пропаганду. В першу чергу це стосується її поведінки. Вона може проявлятися у результатах голосування, організації груп підтримки, участі в мітингах, активній участі у блогосфері, поширенні символіки пропагандиста тощо [6].

Крок 9. Контр-пропаганда

Найкраща контр-пропаганда – правда. Успішна реалізація даного кроку можлива тільки за умови вільної конкуренції ЗМІ [7].

Як показали останні соціологічні опитування в росії, більшість її населення підтримує політику путіна. Очевидно, що російська збройна агресія проти України може тривати довго. Тому необхідно шукати шляхи зміни настроїв російського суспільства, активізувати антивоєнний рух. Для цього Україна має здійснювати активну контр-пропагандистську кампанію. Вона має бути орієнтована насамперед на групи населення росії, які, з одного боку, менше зомбовані, з іншого – здатні на активні антивоєнні виступи.

Крок 10. Ефекти й аналіз

Досягнення цілі є самим важливим результатом пропагандистської кампанії [8]. Тому вибір індикаторів, що відображають зміни параметрів масової свідомості суспільства під її впливом у вигляді зручної для оцінки досягнутих результатів, є вкрай важливим завданням аналітика. Важливим тут є системний підхід.

На практиці для оцінки результатів впливу можна скористатися результатами аналізу частоти повідомлень ЗМІ, контент аналізу, соціологічних опитувань. Окремо аналізується зростання числа прихильників ідеології пропагандиста.

Використана література

1. Померанцев П. Це не пропаганда. Подорож на війну проти реальності / Пер. з англ. О. Форостина. Київ: Yakaboo, 2020. 285 с.
2. Лайнбарджер П. М. Э. Психологическая война. Теория и практика обработки массового сознания / Пер. с англ. Е. В. Ламановой. Москва: ЗАО Центрполиграф, 2013. 445 с.
3. Литвиненко О. Інформаційні впливи та операції. Теоретико-аналітичні нариси. Київ: НІСД, 2003. 240 с.
4. Почепцов Г. Информационные войны. Новый инструмент политики. Москва: Алгоритм, 2015, 256 с.

5. Джоуэт Г., О'Доннел В. Пропаганда и убеждение / Пер. с англ. О. И. Ткаченко. Харьков: «Гуманитарный центр», 2021. 496 с.
6. Уебстер Ф. Теория информационного общества. Москва: Аспект Пресс, 2004. 398 с.
7. Грант Дж. Не верю. Как увидеть правду в море дезинформации. 12 уроков здорового скепсиса. Пер. с англ. Е. Бакушева. Москва: Альпина Паблишер, 2017. 296 с.
8. Макдональд Г. Правда. Как политики, корпорации и медиа формируют нашу реальность, выставляя факты в выгодном свете. Пер. с англ. Н. Мезина. Москва: Альпина Паблишер, 2019. 368 с.

Данильян О. Г.

*доктор філософських наук,
професор, завідувач кафедри
філософії Національного юридичного
університету імені Ярослава Мудрого*

Дзьобань О. П.

*доктор філософських наук, професор,
головний науковий співробітник
Державної наукової установи
«Інститут інформації, безпеки і права
Національної академії правових наук
України»*

МЕРЕЖЕВІ ВІЙНИ ЯК СОЦІОКУЛЬТУРНЕ ТЛО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасне буття соціальних систем, динамізм і специфіка якого обумовлені інтенсивним розвитком інформаційних технологій і мережевих комунікацій, кардинальним чином змінило характер розв'язання конфліктів та ведення війни, про що яскраво свідчить широкомасштабна війна Росії проти України. сучасні російсько-українська війна продемонструвала стирання меж між власне воєнною і мирною формами протидії держав. Сучасне суспільство оперативню формує й нові стратегічні категорії у будівництві й застосуванні збройних сил, такі як: «інформаційна війна», «мережева війна», «мережецентрична війна», «інформаційні операції» тощо.

Поняття мережевої війни – це новий якісний рівень розуміння цілей і завдань сучасної війни, збройних конфліктів. У сутнісному плані ме-

режева війна зводиться до особливої форми ведення конфліктів, коли їх учасники застосовують мережеві форми організації, доктрини, стратегії та технології, максимально пристосовані до умов сучасного етапу розвитку інформаційного суспільства.

У концепції мережевих війн основним поняттям є термін «мережа» – новий інформаційний простір, у якому і розгортаються основні стратегічні операції (війни) як розвідувального, так і воєнного характеру, а також відбувається їхнє медійне, дипломатичне, економічне, технічне та інше забезпечення.

Мережева війна здійснює тотальне руйнування базових характеристик певної нації у всіх типах геополітичних просторів і здійснюється, як правило, у прихованій формі. У зв'язку з цим, загострюється проблема дослідження характерних особливостей і принципів мережевих війн і їх впливу на безпеку особистості, суспільства й держави.

Повномасштабна війна Росії проти України яскраво демонструє наступні характерні особливості мережевої війни:

- об'єктивація інформаційної сфери (інформаційна сфера – така ж сфера бойових дій, як повітряно-космічний, морський і наземний простір);
- асиметричний характер, тобто держава, що має невеликі збройні сили, може завдати серйозної шкоди державі, яка значно перевершує її за кількістю збройних сил;
- ведення просторово локалізованої мережевої війни безпосередньо або побічно впливає на події в міжнародному масштабі;
- мережева війна суттєво впливає на когнітивні й емоційні процеси людей, на їх сприйнятливність і оцінку подій, на рішення, що приймаються;
- неясність і невизначеність правил застосування, відсутність повноцінних даних про можливості, швидкість та ефективність реакції радіоелектронних засобів і окремих елементів різних комп'ютерних систем;
- наявність труднощів у розпізнаванні навмисних і ненавмисних (випадкових) дій і процесів у кіберпросторі;
- необхідність одночасного використання сил і засобів операцій як для впливу на супротивника, так і для захисту своїх збройних сил і сил союзників;
- відстань до цілі впливу не має значення;
- противник може наносити атаки анонімно і приховано;
- метою мережевої війни є забезпечення ефективності бойових дій в умовах мережевого управління військами тощо;

- успіх мережевої війни ґрунтується на методології використання інтегрованих можливостей усіх сил інформаційних операцій, сил їх забезпечення або пов'язаних з їх застосуванням.

Відмітною рисою мережевої війни є наступна: те, що раніше сприймалося як звичайні партизанські війни й заколоти, тепер плавно переходить у форму соціальної мережевої війни і стає глобальною війною. Спостерігаються так звані «мікродії» і «сутички»: різного роду публічні й масові заходи, сюжети у ЗМІ, вміло нав'язані діалоги й переговори, збройні зіткнення тощо. Війна поширюється у багатовимірному просторі: у політиці, культурі та економіці, науці й технологіях, на вулицях міст і у мережі Інтернет. У цій війні в хід йдуть і вбивства, і терористичні акти, і цілком демократичні дебати, статті у пресі й спроби політичних переворотів (події в Молдові у березні 2023 року). І усе це поєднується з прямими ракетними та авіаударами.

Цілком зрозуміло, що мережева інтервенція суттєво позначається на суспільному житті, структурі соціуму, специфіці відносин усередині нього, функціонуванні основних інститутів тощо. Різні мережеві структури (мас-медіа, транснаціональні корпорації, релігійні організації, політичні еліти, спецслужби) інтегруються у загальну, гнучку й різноманітну мережу, що ставить під загрозу суверенітет і політичну незалежність цілих держав і народів.

Як свідчить досвід російсько-української війни, основною ідеєю мережевої війни є інформаційний вплив на людину і суспільство з метою управління та регулювання суспільних процесів країною-агресором, руйнування базових цінностей народу й держави, національної, конфесійної та культурної ідентичності, також, створення інформаційного та ідеологічного вакууму, який має обмежувати стратегічний вибір країни у глобалізованому світі й зробити її частиною системи контролю з боку агресора. У зв'язку з цим, фронт мережевої війни (окрім реальної лінії фронту) розташовується у ментальному просторі, де метою супротивника є руйнування традиційних базових цінностей нації й імплантація власних. Ще військовий китайський теоретик Чтуге Лян, який жив у III ст. до н.е. писав: «У військових діях атака на уми – головне завдання, атака на укріплення – завдання другорядне».

Мережева війна тісно пов'язана з інформаційною або інформаційно-психологічною війною, оскільки в сучасному суспільстві інформаційно-психологічна війна є невід'ємною складовою соціально-політичних відносин і тим фактором, який може помітно змінити спрямованість геополітичних і соціокультурних процесів. Крім того, інформаційно-психологічна війна змінює сам інформаційний простір, призводить до

економічного, політичного, культурного відчуження частини території держави і перерозподілу інших видів стратегічно важливих ресурсів.

Об'єктом інформаційно-психологічної війни є як масова, так і індивідуальна свідомість. Досвід сучасної російсько-української війни дає можливість виділити наступні основні складові впливу на масову й індивідуальну свідомість: дезінформування, лобіювання, маніпулювання, пропаганда, управління кризами, шантаж. Тому, у процесі психологічних операцій, як правило, використовуються інформаційно-пропагандистські акції, спрямовані на дестабілізацію суспільного життя, розкладання зсередини, що готують ґрунт для успішного здійснення політичних, економічних і військових дій. Основним завданням подібних операцій є вплив на суспільну думку і настрої, ціннісні орієнтації, погляди, соціально-психологічний клімат.

Таким чином, у процесі мережевої та інформаційно-психологічної війни важливо посіяти у людей страх і невпевненість перед майбутнім. Як правило, використовується дезінформація орієнтована на зміну моделей людської поведінки, наведення страху на максимальну кількість людей за допомогою максимального інформування. ЗМІ ж доносять до читачів, глядачів і слухачів жах усього того, що відбувається і може відбутися, який повинен зламати волю суспільства й індивіда до опору агресору. Інформаційна війна трансформується у війну смисловою.

У статті «Перша смислова війна у світі (Україна, Крим, Росія)» Г. Почепцов зазначає, що смислова війна у нормі є використанням чужих слів. Експансія ж Росії трималася на старих, а не нових для аудиторії сенсах, на активації й утриманні радянських ментальних конструкцій. Російсько-українська смислова війна реалізувалася у постійній реінтерпретації того, що відбувається, коли з двох альтернативних джерел для описання обирається те, яке більше відповідає запланованим цілям війни. Наприклад, посилення негативної характеристики супротивника: «бойовики», «карателі», «каральна операція» тощо. Практично ті ж самі наративи використовуються російськими ідеологами і сьогодні.

Таким чином, мережева війна – це ефективний засіб впливу, за яким слідує реальні геополітичні зміни. Фронт мережевої війни розташовується у ментальному просторі, де метою супротивника є руйнування традиційних базових цінностей даної нації і імплантація власних.

Аналіз концепції «мережецентричної війни» і досвіду широкомасштабної війни Росії проти України дозволяє зробити висновок, що це не новий специфічний спосіб або форма ведення війни, а лише спосіб інтеграції технічних засобів розвідки, автоматизації управління і вогневого ураження за допомогою інформаційно-телекомунікаційних мереж

зв'язку та передачі даних з метою підвищення ефективності ведення бойових дій шляхом узгодження та координації дій наявних сил і засобів на основі єдиного інформаційного простору і прискорення, внаслідок цього, темпів операції й ефективності ураження супротивника.

Одна з цілей впливу мережевих війн на суспільство – це руйнування смислової єдності світу й людини, руйнування базових цінностей народу й держави, національної, конфесійної та культурної ідентичності.

Тому, мережева війна є фактором формування соціальних страхів і «екзистенційного вакууму», оскільки інформаційний простір активно впливає на суспільні відносини і безпосередньо на сферу безпеки.

Кірієнко В.

*аспірант, Державна наукова установа
«Інститут інформації, безпеки і права
НАПрНУ»*

ПРОТИДІЯ ІНФОРМАЦІЙНІЙ АГРЕСІЇ ТА ІНФОРМАЦІЙНІЙ ПРОПАГАНДИ

У сучасному світі інформація стала одним із цінних ресурсів. Проте, вона також може бути використана для досягнення певних негативних цілей, таких як інформаційна агресія та інформаційна пропаганда. Ці дії можуть бути дуже небезпечними, оскільки можуть вплинути на сприйняття суспільства відповідного змісту та суттєво змінити його поведінку.

Законодавче визначення терміну «Інформаційна агресія» відсутнє, лише є його визначення у Вікіпедії: це – незаконні дії до однієї зі сторін в інформаційній сфері, спрямовані на нанесення конкретної, відчутної шкоди в окремих областях діяльності іншої сторони шляхом обмеженого і локального за своїми масштабами застосування сил [1].

Під терміном «Інформаційна пропаганда» розуміється поширення пропаганди, за допомогою дезінформації та фейкових новин через засоби масової інформації [2, с. 155]. Ці явища можуть мати різні форми, що включають фейки, міфи, конспірології, злочинну діяльність та інше. Найбільш небезпечні, є ті форми, що засновані на ненависті, дискримінації та порушенні прав людини. Одним із способів боротьби з інформаційною агресією та пропагандою є підвищення рівня медійної освіченості населення. Люди мають розрізняти достовірну інформацію від недостовірної, перевіряти джерела та аналізувати інформацію перед тим, як робити висновки та приймати рішення із відповідного питання.

Медійна освідченість має включати в себе розуміння існування різних типів медіа, а також знання про методи факт – чекінгу (з англ. Fact checking – перевірка фактів), та здатність критично оцінювати інформацію, що надходить з різних джерел. Медійна освідченість має засновуватися на знанні, проте, як інформація поширюється в мережі Інтернет, та як це впливає на її достовірність. Ще одним із способів боротьби з інформаційною агресією та пропагандою є підвищення рівня захищеності від кібератак. Інформаційні атаки можуть бути спрямовані на керівництво країни, наукові установи, бізнес структури, засоби масової інформації. Це може призвести до витоку інформації з обмеженим доступом, інформації, яка містить державну таємницю, також можуть бути втрачені фінансові активи, а також, можуть бути втрачені персональні дані.

Щоб запобігти настанню негативних наслідків, організації та установи мають підвищувати рівень захисту від кібератак, наприклад, шляхом використання програмного забезпечення для захисту від вірусів та шкідливих програм, захисту від крадіжки даних та зломів, а також мають навчати працівників методам запобігання кібератакам. Для цього Уряд України має приділяти особливу увагу насамперед в боротьбі з інформаційною агресією та пропагандою, яку веде Російська Федерація.

Важливим також є залучення громадян до боротьби з інформаційною агресією та інформаційною пропагандою. Для цього повідомлення про пропаганду та недостовірну інформацію мають бути поширені через медіа-засоби та соціальні мережі. Важливо, щоб такі повідомлення мали достовірне джерело та були зрозумілі та доступні для всіх громадян.

Підсумовуючи вище викладене, необхідно зазначити, що боротьба з інформаційною агресією та інформаційною пропагандою є дуже важливим завданням для України, особливо в період широкомасштабного, збройного нападу Російської Федерації. Це вимагає підвищення медійної освідченості у населення, критичного його мислення, забезпечення належного його захисту від кібератак. Усі заходи повинні проводитися у тісній співпраці Уряду з відповідними громадськими та міжнародними організаціями, щоб забезпечити ефективну боротьбу з інформаційною агресією та інформаційною пропагандою, та захистити громадян України від її шкідливих наслідків, і тим самим забезпечити національну безпеку.

Література:

1. Інформаційна агресія // Вікіпедія: вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/Інформаційна_агресія (дата звернення: 21.04.2023).

2. Драбюк С. С. Пропаганда та її види. Шляхи протидії пропаганді. *Аналітично – порівняльне правознавство*. 2022. №1. С. 153-157. URL: <http://app-journal.in.ua/wp-content/uploads/2022/05/30.pdf> (дата звернення 21.04.2023).

Васько В. А.

аспірант ДНУ ШБП НАПрН України

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ: ОГЛЯД ПРАВОВИХ ПРОБЛЕМ

Початкове застосування технології блокчейн полягало у створенні безпечної та розподіленої системи для однорангових транзакцій з використанням криптовалют, але за останні роки потенційне застосування останньої значно розширилось, відтак блокчейн перетворився на універсальну технологію. Однією з головних її переваг є децентралізація, яка дозволяє досягти максимальної безпеки даних та інформації про транзакції, оскільки жоден окремих учасник мережі не може змінити відомості записані у блокчейн. Це робить її вагомим інструментом для сфер соціального життя, де довіра, безпека та прозорість є критично важливими. Саме тому державний сектор може стати однією з ключових галузей застосування технології блокчейн. Уже зараз уряди та парламенти в усьому світі вивчають потенційні варіанти її використання у сфері публічного управління.

Технологія блокчейн має значний потенціал для трансформації багатьох державних послуг, починаючи від застосування цифрової валюти та платежів і закінчуючи створенням надійних державних реєстрів, безпечних і прозорих систем голосування, децентралізованих систем управління та обміну даними у нотаріаті, медицині, освіті тощо [1]. Проте фактичне використання технології блокчейн в державному секторі залишається на низькому рівні, оскільки існує значна кількість правових та організаційних проблем на шляху її широкомасштабного застосування.

До загальних проблеми застосування технології блокчейн науковці традиційно відносять наступні [2,3]:

1) масштабованість – поточна архітектура блокчейну має обмежені можливості для одночасної обробки великої кількості даних, що може призвести до повільного підтвердження транзакцій, високих комісій та перевантаження мережі;

2) енергоспоживання – технологія блокчейн вимагає значних обчислювальних потужностей, що призводить до високого енергоспоживання;

3) здатність до взаємодії – різні блокчейн-мережі часто використовують відмінні протоколи та стандарти, що ускладнює їхню взаємодію між собою;

4) недостатню розвиненість технологічної інфраструктури – це може створювати бар'єри для обміну даними та співпраці між різними суб'єктами у випадку застосування ними технології блокчейн;

5) прийняття користувачами – багато людей все ще не знайомі з цією технологією і можуть не використовувати її через побоювання щодо складності, безпеки та надійності.

Та головною проблемою застосування технології блокчейн у державному секторі є суттєва загроза усунення державних органів від прийняття управлінських рішень. Оскільки створюючи автономну розподілену систему публічного управління, блокчейн може відсторонити суб'єктів владних повноважень від здійснення ним владних функцій замінивши їх алгоритмічною системою консенсусу [4].

Таким чином, технологічні особливості блокчейну ускладнюють управління ним для державного сектору, але не всі науковці так вважають, тому з цього приводу в літературі зустрічаються дві протилежні точки зору. Так деякі дослідники стверджують, що блокчейн може забезпечити більш демократичні моделі управління, дозволяючи громадянам та іншим зацікавленим сторонам брати активну участь у здійсненні публічно-владних управлінських функцій [5]. Потенційно це може призвести до більшої прозорості та підзвітності в державному управлінні, а також сприяти зміцненню довіри до публічних інституцій. З іншого боку, деякі вчені висловлюють занепокоєння, що застосування блокчейну в державному управлінні може призвести до втрати контролю і нагляду з боку державних установ, а також потенційно підірвати демократичні принципи, які лежать в основі державного управління [6]. Також існує ризик того, що системи, засновані на блокчейні, можуть бути вразливими до маніпуляцій або атак, особливо якщо вони не підтримуються та/або не захищені належним чином.

На перший погляд цю фундаментальну проблему можна вирішити шляхом створення закритого (приватного) блокчейну в якому певною мірою є можливість здійснювати вагомий контроль над системою. Проте, застосування технології блокчейн у державному секторі вимагає врахування багатьох умов, що стосуються зокрема і політичних пріоритетів, конфіденційності, пропускнуої здатності, безпеки тощо. Ці компромісні умови залежать від функцій, котрі здійснюють суб'єкти публічної влади, тому вони не можуть мати однакове значення для всього державного апарату. Таким чином, залежно від специфіки державних органів та послуг

які вони надають є недоцільним створення виключно закритих (приватних) блокчейн-рішень. До того ж, як і в публічних (відкритих) так і в приватних (закритих) блокчейнах правила і механізми функціонування самої мережі встановлюються на початковому етапі розробки системи, відповідно будь-які подальші зміни в управлінні останньою вимагатимуть обов'язкової згоди уповноважених користувачів.

Однак, незважаючи на складність цих проблем, у цілому вони можуть бути вирішені. Проте, щоб успішно та ефективно застосовувати технологію блокчейн у сфері публічного управління, найголовніше необхідно знайти рішення щодо низки правових проблем, які є значно комплекснішими [7]. Перш за все, відсутність чіткої нормативно-правової бази в цьому аспекті породжує невизначеність щодо наступних питань.

1) Ідентифікація осіб надавачів та набувачів державних послуг – ідентифікація або перевірка особи є ключовим питанням, коли мова йде про здійснення будь-яких правочинів в мережі Інтернет, включаючи дії із застосуванням технології блокчейн. Верифікація особи допомагає запобігти шахрайству, захистити конфіденційну інформацію і гарантувати, що правочини вчиняють правоздатні та дієздатні особи. Наразі основні протоколи найпоширеніших відкритих блокчейн-проектів не вимагають жодних ідентифікаційних даних під час створення акаунту. Це в свою чергу створює значні правові перешкоди щодо отримання державних послуг та безпосередньої участі в публічному управлінні. Тому існують різні підходи щодо вирішення цієї проблеми. Один з них полягає у створенні центрального органу, який буде керувати системою ідентифікації учасників блокчейн-мереж, що може допомогти забезпечити перевірку ідентичності сторін, які беруть участь у правочинах, а також безпеку та надійність системи. А інший підхід полягає в тому, щоб сам блокчейн керував системою ідентифікації, за умови, що технічні ідентифікаційні дані користувачів у блокчейні будуть мати таку ж саму юридичну силу, як і традиційні способи. До того ж вирішення цієї проблеми може запобігти й іншим потенційним правовим проблемам, котрі породжуються у разі втрати доступу до акаунту.

2) Перевірка законності вчинених правочинів – блокчейн не може самостійно здійснювати попередню перевірку дотримання правових вимог учасниками мережі. Ця проблема є найбільш актуальною в контексті ведення державних реєстрів переважно пов'язаних з операціями щодо нерухомості. Наприклад, державна реєстрація договору купівлі-продажу нерухомого майна може передбачати виконання низки юридичних вимог, включаючи перевірку дієздатності продавця, наявності оригінальних документів на право власності щодо предмету договору, відсутності обя-

жень на об'єкт нерухомості, забезпечення дотримання правил зонування або землекористування тощо. Для вирішення цієї проблеми критично важливо залучати до блокчейн-систем сторонніх контролерів, таких як юристи, нотаріуси або регуляторні органи, які можуть перевіряти правочини та забезпечувати дотримання вимог законодавства.

3) Складність перетворення певних юридичних термінів і конструкцій у програмний код – хоча деякі правовідносини можна відносно легко відобразити у блокчейні, існує низка правочинів, які вимагають складного кодування. Наприклад, право спільної сумісної власності з різними частками, розпорядження майном за взаємною згодою, тимчасове володіння та інші види майнових угод можуть бути складними для представлення в коді. Аналогічно, такі правочини, як узурфрукт, сервітут, опціон також мають специфічні юридичні вимоги та умови, які неможливо повністю відобразити в коді. Для вирішення цієї проблеми знадобиться розробка додаткових правових стандартів, які можна буде використовувати в блокчейні.

4) Притягнення до юридичної відповідальності – традиційні правові системи покладаються на централізовані органи влади для вирішення спорів та притягнення винних осіб до відповідальності за їхні дії. Однак системи на основі блокчейну є децентралізованими, що ускладнює визначення юридичної відповідальності у разі виникнення спорів. Це викликає питання про відповідальність державних органів, розробників, користувачів та інших сторін, залучених до екосистеми блокчейну. Для вирішення цієї проблеми важливо створити чіткі правові рамки і правила, які регулюють використання технології блокчейн у державному секторі. Ці нормативні акти повинні включати положення про юридичну відповідальність у разі виникнення спорів, а також механізми їх вирішення.

5) Конфіденційність та безпека даних – системи на основі блокчейну є децентралізованими, а це означає, що дані зберігаються одночасно на декількох вузлах мережі. Хоча така розподілена архітектура забезпечує підвищений захист від спроб злову, вона також ускладнює контроль за тим, хто має доступ до інформації. Крім того, оскільки дані є незмінними, не існує способу повністю стерти інформацію, яка була занесена в блокчейн, навіть якщо вона була введена помилково або без належного дозволу. Ще однією проблемою, пов'язаною з безпекою даних у системах на основі блокчейну, є ризик публічного розголошення інформації з обмеженим доступом. У деяких випадках системи на основі блокчейну можуть бути повністю прозорими, що означає, що всі дані, внесені в блокчейн, доступні кожному користувачеві мережі. Хоча така прозорість може бути

корисною в системах голосування, вона також може призвести до витоку конфіденційної інформації, яку слід зберігати в таємниці. Одним із варіантів вирішення цих проблем є використання шифрування та контролю доступу, щоб обмежити коло осіб, які можуть отримати доступ до даних у блокчейні. Іншим рішенням є використання позамережевого сховища захищеної інформації, яке не повинно бути видимим в блокчейні.

Таким чином, виклик застосування технології блокчейн у публічному управлінні полягає в тому, щоб знайти баланс між необхідністю забезпечення прозорості й підзвітності та децентралізацією й механізмом консенсусу, забезпеченням конфіденційності й безпекою даних. Це також вимагає визначення ключових зацікавлених сторін, залучених до системи, і створення механізмів їхньої участі в процесі публічного управління. Досягнути цієї мети можна тільки у разі належного правового регулювання застосування технології блокчейн у державній сфері, але тут також необхідно враховувати так званий «парадокс управління» описаний В. Лехдонвіртом. З одного боку, децентралізована і прозора природа блокчейну покликана усунути потребу в централізованому органі, якому довіряють. А з іншого боку, ефективне управління блокчейн-системами у публічному секторі можливе тільки у випадку встановлення чітких правил і процедур з боку централізованих органів державної влади [8]. Відтак при нормативному регулюванні застосування технології блокчейн важливо мати чітке розуміння потенційного впливу останньої на публічне управління та функціонування державного апарату в цілому.

Отже, хоча технологія блокчейн і має величезний потенціал для трансформації державного сектору, успіх застосування блокчейн-рішень у публічній сфері залежить від знаходження правильного балансу між регулюванням і децентралізацією, установленням чітких правил щодо управління даними, механізмів притягнення винних осіб до відповідальності та вирішення спорів. Таким чином, ретельно зваживши, чим управляти (або не управляти) і як врегулювати це управління, органи публічної влади зможуть ефективно застосовувати технології блокчейн для стимулювання інновацій та покращення якості державних послуг. Натомість не вирішення насамперед правових проблем застосування цієї технології може призвести до того, що потенційні переваги від її використання у публічному управлінні будуть втрачені.

Список використаних джерел

1. Blockchain use cases for government. URL: <https://bit.ly/44cMIW9>
2. Levy A. 5 Problems With Blockchain Technology. URL: <https://bit.ly/3oN2pDc>

3. Five major challenges in the blockchain industry. URL: <https://bit.ly/4291aix>

4. De Filippi P., Mannan M., Reijers W. Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*. 2020. Vol. 62. P. 101284. URL: <https://doi.org/10.1016/j.techsoc.2020.101284>

5. Beck R., Müller-Bloch C., King J. L. Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*. 2018. P. 1020–1034. URL: <https://doi.org/10.17705/1jais.00518>

6. Atzori M. Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation*. 2017. Vol. 6, no. 1. P. 45–62. URL: https://doi.org/10.22495/jgr_v6_i1_p5

7. Blockchain Legal implications, questions, opportunities and risks. URL: <https://bit.ly/3Vjvd2s>

8. Lehdonvirta V. The blockchain paradox: Why distributed ledger technologies may do little to transform the economy. URL: <https://bit.ly/42axFKV>

Сердечна А. Ю.

старший викладач кафедри

кримінального права та кримінології

Національної академії СБ України

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ОБ'ЄКТ ЗЛОЧИННОГО ВПЛИВУ З БОКУ СИЛ ДЕРЖАВИ-АГРЕСОРА ТА ПЕРСПЕКТИВИ ЇЇ ЗАХИСТУ

Згідно Стратегії інформаційної безпеки, затвердженою Указом Президента України від 28.12.2021 року № 685/2021 інформаційна безпека України визначається як складова частина національної безпеки України.

Якщо аналізувати законодавчі новації воєнного часу, то можна зробити висновок, що більшість із прийнятих з березня 2022 року статей Кримінального кодексу України криміналізували суспільно небезпечні діяння, пов'язані з ворожим впливом на інформаційні відносини в нашому суспільстві. Так Законом України від 3.03.22 р. № 2108-IX [1] чинний КК України доповнено статтею 111–1; Законом України від 3.03.22 р. № 2110-IX [2] чинний КК України доповнено статтею 436–2; Законом

України від 24.03.22 року № 2160-IX [3] чинний КК України доповнено статтею 114-2.

Що ж саме криміналізовано з тих діянь, які створюють загрозу тим або іншим суспільним відносинам у сфері інформаційної безпеки? Вказані діяння можна умовно поділити на групи, запропоновані авторами практичного посібника з кваліфікації злочинної колаборації [4; с. 26-30].

1) злочинна колаборація в інформаційному просторі, спрямована на вирішення стратегічних завдань держави-агресора щодо формування викривленої оцінки та виправдання її злочинної агресії:

- публічне заперечення громадянином України здійснення збройної агресії проти України, встановлення та утвердження тимчасової окупації частини території України (ч. 1 ст. 111-1 КК України);
- здійснення громадянином України пропаганди у закладах освіти незалежно від типів та форм власності з метою сприяння здійсненню збройної агресії проти України, встановленню та утвердженню тимчасової окупації частини території України, уникненню відповідальності за здійснення державою-агресором збройної агресії проти України (ч. 3 ст. 111-1 КК України);
- організація та проведення заходів політичного характеру у співпраці з державою-агресором та/або його окупаційною адміністрацією, спрямованих на підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань та/або на уникнення нею відповідальності за збройну агресію проти України (ч. 6 ст. 111-1 КК України);
- здійснення інформаційної діяльності у співпраці з державою-агресором та/або його окупаційною адміністрацією, спрямованої на підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань та/або на уникнення нею відповідальності за збройну агресію проти України (ч. 6 ст. 111-1 КК України);
- виправдовування, визнання правомірною, заперечення збройної агресії рф проти України, розпочатої у 2014 році, у тому числі шляхом представлення збройної агресії російської федерації проти України як внутрішнього громадянського конфлікту (ч. 1 ст. 436-2 КК України);
- виправдовування, визнання правомірною, заперечення тимчасової окупації частини території України (ч. 1 ст. 436-2 КК України);
- глорифікація осіб, які здійснювали збройну агресію рф проти України, розпочату у 2014 році, представників збройних формувань рф, іррегулярних незаконних збройних формувань, озброєних банд та груп найманців, створених, підпорядкованих, керо-

ваних та фінансованих рф, а також представників окупаційної адміністрації рф, яку становлять її державні органи і структури, функціонально відповідальні за управління тимчасово окупованими територіями України, та представників підконтрольних рф самопроголошених органів, які узурпували виконання владних функцій на тимчасово окупованих територіях України (ч. 1 ст. 436–2 КК України);

- виготовлення, поширення матеріалів, у яких міститься виправдовування, визнання правомірною, заперечення збройної агресії рф проти України, розпочатої у 2014 році, у тому числі шляхом представлення збройної агресії рф проти України як внутрішнього громадянського конфлікту, виправдовування, визнання правомірною, заперечення тимчасової окупації частини території України, а також глорифікація осіб, які здійснювали збройну агресію рф проти України, розпочату у 2014 році, представників збройних формувань рф, іррегулярних незаконних збройних формувань, озброєних банд та груп найманців, створених, підпорядкованих, керованих та фінансованих рф, а також представників окупаційної адміністрації рф, яку становлять її державні органи і структури, функціонально відповідальні за управління тимчасово окупованими територіями України, та представників підконтрольних рф самопроголошених органів, які узурпували виконання владних функцій на тимчасово окупованих територіях України (ч. 2 ст. 436–2 КК України);

2) злочинна колаборація, спрямована на підтримку окупаційної влади, впроваджені державою-агресором на захоплених територіях, реалізацію її рішень та сприяння незаконній діяльності створених нею органів:

- публічні заклики громадянина України до: а) підтримки рішень та/або дій держави-агресора, збройних формувань та/ або окупаційної адміністрації держави-агресора; б) співпраці з державою-агресором, збройними формуваннями та/ або окупаційною адміністрацією держави-агресора; в) невизнання поширення державного суверенітету України на тимчасово окупованій території України (ч. 1 ст. 111–1 КК України);
- дії громадян України, спрямовані на впровадження стандартів освіти держави-агресора у закладах освіти (ч. 3 ст. 111–1 КК України);
- публічні заклики до проведення незаконних виборів та/або референдумів на тимчасово окупованій території (ч. 5 ст. 111–1 КК України);

3) злочинна колаборація, спрямована на надання представнику держави-агресора необхідної допомоги чи інформації, які можуть бути використані для завдання шкоди охоронюваним законом інтересам:

- поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, у тому числі про їх переміщення територією України, якщо така інформація не розміщувалася (не поширювалася) у відкритому доступі Генеральним штабом Збройних Сил України, Міністерством оборони України, Головним управлінням розвідки Міністерства оборони України чи Службою безпеки України або в офіційних джерелах країн-партнерів, учинене в умовах воєнного або надзвичайного стану, з метою надання такої інформації державі, що здійснює збройну агресію проти України, або її представникам, або іншим незаконним збройним формуванням (ч. 3 ст. 114-2 КК України);
- поширення інформації про переміщення, рух або розташування Збройних Сил України чи інших утворених відповідно до законів України військових формувань, за можливості їх ідентифікації на місцевості, якщо така інформація не розміщувалася у відкритому доступі Генеральним штабом Збройних Сил України, Міністерством оборони України або іншими уповноваженими державними органами, вчинене в умовах воєнного або надзвичайного стану, з метою надання такої інформації державі, що здійснює збройну агресію проти України, або її представникам, або іншим незаконним збройним формуванням (ч. 3 ст. 114-2 КК України).

Як бачимо, інформаційна складова будь-якої з видів безпеки є занадто уразливим об'єктом, через який представники держави-агресора намагались зламати опір на окупованих територіях, насадити ворожі стандарти освіти, виправдати свої агресивні дії, надавши їм викривлені пояснення та поширюючи свої наративи як серед мешканців окупованих територій та України в цілому, так і серед своїх власних громадян та громадян іноземних держав. І тут необхідно зазначити, що проаналізовані законодавчі новації виявились досить ефективними, оскільки кількість осіб, притягнутих за вчинення кримінальних правопорушень, передбачених ст. ст. 111-1, 114-2 та 436-2 КК України, свідчить про правильність обраних напрямків кримінально-правової охорони.

Разом з цим, як вбачається, окремі напрями законодавчих новацій залишились без свого логічного завершення. Мова йде про положення Закону України від 22.05.22 року № 2265-IX «Про заборону пропаганди російського нацистського тоталітарного режиму, збройної агресії Росій-

ської Федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну» [5], де законодавець визнав рф державою-терористом, однією з цілей політичного режиму якої є геноцид Українського народу, фізичне знищення, масові вбивства громадян України, вчинення міжнародних злочинів проти цивільного населення, використання заборонених методів війни, руйнування цивільних об'єктів та об'єктів критичної інфраструктури, штучне створення гуманітарної катастрофи в Україні або окремих її регіонах.

При цьому пропаганду російського нацистського тоталітарного режиму, збройної агресії рф як держави-терориста проти України було заборонено, а використання символіки воєнного вторгнення російського тоталітарного режиму в Україну визнано окремим видом пропаганди російського нацистського тоталітарного режиму, збройної агресії рф як держави-терориста проти України. Як передбачено у ст. 3 вказаного вище Закону, винні у порушенні його вимог несуть відповідальність відповідно до закону. Разом з цим, відповідальності за заборонені законом дії не було впроваджено, з огляду на що норми закону на цей час мають переважно декларативний характер.

З огляду на вказане вище вважаємо перспективними напрямками подальших наукових розвідок – формування відповідних норм для їх впровадження в Особливу Частику КК України.

Список використаних джерел:

1. Про внесення змін до деяких законодавчих актів (щодо встановлення кримінальної відповідальності за колабораційну діяльність): Закон України від 3.03.2022 року № 2108-IX. URL: <https://zakon.rada.gov.ua/laws/show/2108-20#Text>.

2. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції: Закон України від 03.03.2022 № 2110-IX. URL: <https://zakon.rada.gov.ua/laws/show/2110-20#Text>.

3. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану: Закон України від 24.03.2022 № 2160-IX. URL: <https://zakon.rada.gov.ua/laws/show/2160-20#Text>.

4. Злочинна колаборація в умовах збройної агресії: практич. порадник з кримінально-правової оцінки та розмежування / за заг. ред. В. В. Малюка. Київ : Алерта, 2023. 312 с

5. Про заборону пропаганди російського нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну: Закон України від 22.05.2022 № 2265-IX. URL: <https://zakon.rada.gov.ua/laws/show/2265-20#Text>.

Горун О. Ю.

*головний науковий співробітник
Українського науково-дослідного
інституту спеціальної техніки та
судових експертиз СБУ*

ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі [1].

Кіберпростір визнано одним з можливих театрів воєнних дій. РФ залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури [1].

Посилюються загрози для критичної інфраструктури, пов'язані з погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвитку, несанкціонованим втручанням у її функціонування, зокрема фізичного і кіберхарактеру, триваючими бойовими діями, а також тимчасовою окупацією частини території України [2].

Рівень загрози кібератак проти України стрімко зріс в умовах непокритої агресії РФ проти України з лютого 2022 року. Особливо помітне зростання кількості кіберінцидентів і кібератак на державні інформацій-

ні ресурси та об'єкти критичної інфраструктури України з боку російських хакерів. Від початку повномасштабної війни на українську енергетику було здійснено понад 1,2 млн. кібератак [3].

Як зазначає Голова СБУ В. Малюк: «Україна бореться зі збільшенням кількості кібератак, причому Росія здійснює щонайменше 10 кібератак на день. У 2020 році СБУ зафіксувала 800 кібератак, у 2021 році – близько 2 тисяч. Але після вторгнення їх зафіксували понад 4500. Передусім масштабних кібератак зазнають: енергетичні, логістичні, військові об'єкти, а також бази даних державних органів та інформаційні ресурси» [4].

Кібератаки РФ спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності [1].

Під критичною інфраструктурою розуміється сукупність об'єктів такої інфраструктури. До об'єктів критичної інфраструктури відносяться: об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [5]. Відповідно до Закону України «Про критичну інфраструктуру» об'єкти критичної інфраструктури – це підприємства, установи й організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей [5].

Віднесення об'єктів критичної інфраструктури та формування переліку таких об'єктів здійснюється відповідно до приписів ст. 8 Закону України «Про критичну інфраструктуру» у порядку, встановленому Кабінетом Міністрів України, та має здійснюватися за сукупністю критеріїв, що визначають їх соціальну, політичну, економічну та екологічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку.

До таких критеріїв належать: 1) виконання функцій із забезпечення життєво важливих національних інтересів; 2) існування викликів і загроз, що можуть виникати щодо об'єктів критичної інфраструктури; 3) ймовірність завдання значної шкоди нормальним умовам життєдіяль-

ності населення; 4) уразливість таких об'єктів, тяжкість можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода здоров'ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення); соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства); державному суверенітету (зниження обороноздатності, дискредитація іміджу країни, дестабілізація системи державного управління та унеможливлення виконання державою своїх функцій); економіці (вплив на внутрішній валовий продукт, розмір економічних втрат, як прямих, так і непрямих); природним ресурсам загальнодержавного та місцевого значення; 5) масштабність негативних наслідків для держави, які впливають на діяльність стратегічно важливих об'єктів для кількох секторів життєзабезпечення чи призводять до втрати унікальних національно значущих активів, систем і ресурсів, матимуть тривалі наслідки для держави і позначається на діяльності ряду інших секторів; 6) тривалість ліквідації таких наслідків та дія подальшого негативного впливу на інші сектори держави; 7) вплив на функціонування суміжних секторів критичної інфраструктури [5].

Постановою Кабінету Міністрів України від 9 жовтня 2020 р. №1109 затверджено методику категоризації об'єктів критичної інфраструктури, яка визначає механізм та критерії віднесення об'єкта критичної інфраструктури до однієї з категорій критичності:

1) I категорія критичності – особливо важливі об'єкти, які мають загальнодержавне значення, значний вплив на інші об'єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації державного значення;

2) II категорія критичності – життєво важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення;

3) III категорія критичності – важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення;

4) IV категорія критичності – необхідні об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення[6].

Відповідно до ч.3 ст. 10 Закону України «Про критичну інфраструктуру» категоризація об'єктів критичної інфраструктури здійснюється секторальними органами у сфері захисту критичної інфраструктури відповідно до секторальної специфіки та вимог секторального законодавства [5].

Такі органи складають переліки всіх об'єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури, що віднесені до I, II, III і IV категорії критичності.

Використовуючи перелік секторів критичної інфраструктури, такі органи:

- ідентифікують об'єкти критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури;
- разом із оператором критичної інфраструктури здійснюють категоризацію об'єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури відповідно до згаданої вище методики [5].

Сформульований підхід до включення певних об'єктів до критичної інфраструктури, з одного боку, дозволяє системно вирішувати проблеми їхнього захисту, а з іншого – висуває на перший план завдання з'ясування та оцінки загроз та ризиків для окремих елементів з тим, щоб направити на відповідні ресурси насамперед туди, де ризики є найбільшими і де першочергові та подальші заходи будуть давати максимальний ефект [7, с.64].

Поряд з традиційними способами вчинення терактів і диверсій на таких об'єктах (вибухи, підпали) терористами широко розповсюджується новітні інформаційні технології для порушення штатних режимів роботи автоматизованих систем управління технологічними процесами. Дедалі більшого розповсюдження набуває політична вмотивована діяльність у формі кібератак на державні та корпоративні інформаційні ресурси [7, с.63].

Об'єкти критичної інфраструктури є складними з технічної точки зору. Відповідно, складними є й вимоги до кіберзахисту таких об'єктів.

Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури затверджені постановою Кабінету Міністрів України від 19 червня 2019 р. №518. Вони визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури [8]. Кіберзахист об'єкта критичної інфраструктури забезпечується шляхом впровадження на об'єкті критичної інформаційної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю[8].

Проблема запровадження комплексного підходу до розв'язання проблем захищеності критичної інфраструктури, звичайно, виходить далеко за межі лише понятійного та методологічного апарату. На перше місце висувається завдання створення дієвого механізму координації зусиль

органів влади, спрямованих на недопущення втрати чи завдання невинної шкоди ключовим (вузловим) елементам критичної інфраструктури внаслідок дії негативних факторів будь-якого походження, або техногенного, або природного, або соціально-політичного, або будь-якої комбінації з їх числа [9, с. 3].

Перспективним напрямом подальших наукових досліджень має стати формування нових індикаторів потенційних ризиків та загроз об'єктам критичної інфраструктури.

Список використаних джерел

1. Стратегія кібербезпеки України: затвердж. Указом Президента України від 26 серпня 2021 року № 447. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>.

2. Стратегія національної безпеки України: затвердж. Указом Президента України від 14.09.2020 р. №393. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>.

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

4. From war crimes, to spies and cyberattacks: Ukraine's domestic spy chief on fighting Russia across all fronts. URL: https://www.independent.co.uk/news/world/europe/ukraine-russia-war-crimes-putin-b2290489.html?fbclid=IwAR3Yj6FwG_EXHS8i1-205WGMWxSJruGrbq4TvmgqdRpD9DiD-hYefndQ7f8.

5. Про критичну інфраструктуру: Закон України від 16.11.2021 р. №1882-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#n80>.

6. Методика категоризації об'єктів критичної інфраструктури: затвердж. постановою Кабінету Міністрів України від 9 жовтня 2020 р. №1109 URL: <https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n11>.

7. Організаційно-правові основи забезпечення кібербезпеки: підруч. / М. М. Присяжнюк, А. І. Марущка, Д. С. Мельник та ін.; за заг. ред. М. М. Присяжнюка. К.: Вид-во Ліра-К, 2023. 320 с.

8. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури: затвердж. постановою Кабінету Міністрів України від 19 червня 2019 р. №518. URL: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text>.

9. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні: аналітична доповідь. 2012. 57 с.

Хроленко Я. О.
аспірант ІПРІ НАН України

МЕТОДИ ПРОТИДІЇ ФІШИНГОВИМ АТАКАМ В ІНФОРМАЦІЙНОМУ ПРОСТОРИ

Крадіжка персональних даних сьогодні є гострою проблемою через фішингові лінки. Державна служба спеціального зв'язку та захисту інформації України повідомила, що російські хакери здійснюють дедалі більше кібератак проти звичайних українців, також зростає кількість інформаційно-психологічних операцій у соцмережах та месенджерах. Хакери часто спекулюють на патріотичних темах та виплатах від держави. Наразі існують інструменти, які попереджають користувача про те, що посилання, за яким він намагається перейти, за допомогою комп'ютерного зору потрапить на фальшиві сторінки сайту, а також аналіз сторінки за допомогою штучних нейронних мереж. Також проведено порівняльне дослідження фішингових ресурсів, розглянуто алгоритми отримання даних, основні критерії підозри у фішингу, а також соціальну значимість виявлення фішингу, алгоритми розпізнавання фішингових сайтів: аналіз текстового контенту сторінок, основи розпізнавання образів, нейронних мереж, а також описані основні методи протидії.

Багато послуг тепер доступні через Інтернет. Безпека платежів у цих системах забезпечується різноманітними високотехнологічними рішеннями, такими як сертифікати безпеки, криптографічні протоколи тощо. Однак усі ці рішення виявляються неефективними, коли зловмисники використовують методи соціальної інженерії, які використовують слабкі сторони людського фактору. Одним із найпоширеніших видів подібних атак сьогодні є фішинг. Фішинг (від англ. phishing, password fishing) – вид онлайн-шахрайства, метою якого є отримання доступу до конфіденційних даних користувача шахрайським шляхом. Популярною технікою фішингу є створення фальшивих веб-сайтів, які на вигляд неможливо відрізнити від справжніх. Збитки від злочинів, пов'язаних з фішингом, тільки в 2010 році склали мільярди доларів США. При цьому, згідно зі статистикою, кількість фішингових атак щорічно зростає приблизно в півтора рази. Стрімкий розвиток цього виду злочинності можна зупинити, створивши комплексні системи захисту від фішингових атак. Оскільки арсенал фішерів зростає швидкими темпами, необхідно забезпечити можливість навчання таких систем. На даний момент подібних рішень немає, тому створення комплексної, піддається навчанню, високоефективної системи захисту від фішингових атак є цікавим і актуальним напрямком. Створення такої системи передбачає

попереднє вивчення особливостей фішингових ресурсів і розробку на їх основі методів оцінки ступеня небезпеки інформаційного ресурсу та виявлення потенційно небезпечних ресурсів. Цьому в основному присвячена дана робота [1].

Метою роботи є виконання наступного комплексу завдань: опис основних методів і способів фішингу, аналіз існуючих підходів до вирішення проблеми протидії фішингу, а також опис основних методів автоматизованого антифішингу.

Основна проблема фішингу полягає в тому, що існує кілька видів фішингу, які мають свою специфіку, а програмного забезпечення, яке б повністю захистило людей і компанії, немає.

Ознаками фішингових ресурсів є:

- Схожість графічного вмісту. Основне завдання кіберзлочинців під час фішингової атаки – змусити користувача повірити в справжність фішингового ресурсу. Найпростіший спосіб зробити це – запозичити графічне оформлення з атакованого сайту.
- Схожість змісту тексту. Поняття схожості текстів також є незрозумілим, і, як і в попередньому випадку, можна лише стверджувати з упевненістю про їх повну тотожність.

Однак на практиці, змінюючи текстовий вміст оригінального ресурсу, зловмисники зазвичай використовують стандартний набір перетворень, наприклад [2]:

- вставка наборів випадкових символів;
- довільна вставка та видалення пробілів;
- заміна символів одного кодування на символи іншого кодування, схожі за написанням;
- вставка ключових слів у випадкових позиціях.

Наявність ресурсу у фішингових базах. Інтернет-спільнота підтримує велику кількість баз небезпечних ресурсів. Деякі користувачі додають посилання на такі ресурси, інші підтверджують або спростовують їх безпеку.

Використання функцій форматування URL-адреси. Формат URL-адреси має багато параметрів, деякі з яких рідко використовуються на практиці. Часто зловмисники використовують більш повну форму, додаючи рідко використовувані параметри, щоб ввести в оману користувача і переконати його в достовірності фішингового ресурсу.

Підозрілі облікові дані ресурсу. Реєстраційні дані можуть включати географічне розташування, дату реєстрації домену, ім'я власника сайту або назву організації-власника. Як правило, фішингові сайти активні протягом перших п'яти днів після їх створення.

Наявність ресурсу на одній IP-адресі з раніше ідентифікованими фішинговими ресурсами. Розташування кількох ресурсів на одній IP-адресі є досить поширеною ситуацією, тому доцільно використовувати списки IP-адрес, на яких були виявлені фішингові ресурси.

Використання великої кількості скриптів. Як правило, кількість виконаного коду на сторінці зростає пропорційно її інформаційному наповненню та наданій функціональності.

Запропоновано алгоритми визначення ступеня небезпеки інформаційних ресурсів з урахуванням описаних ознак [2]:

Послідовне використання алгоритмів оцінки ознак. Всі характеристики перевіряються безпосередньо. Оскільки різні алгоритми аналізу даних використовують ознаки різної значущості, необхідно також подати таблицю значущості ознак на вхід охоплюючого алгоритму.

Використання булевої функції. При визначенні ступеня небезпеки інформаційного ресурсу певний набір ознак може бути достатнім для віднесення ресурсу до категорії небезпечних. Наприклад, якщо доменне ім'я сайту міститься у фішингових базах, решту ознак перевіряти не потрібно – такий сайт апіорі небезпечний.

Використання нейронних мереж. Одним із способів відмови від таблиці значущості ознак є використання статистичних методів.

Використання методів лінійної регресії. Для побудови наближеної функції використовуються задані значення небезпек деяких інформаційних ресурсів. Коли функція визначення ступеня небезпеки невідома, не зовсім зрозуміло, як отримати досить велику кількість значень цієї функції при заданих значеннях аргументів. Ця проблема вирішується за допомогою експертних оцінок.

Машинне навчання допомагає автоматизувати виявлення загроз. Особливо це стосується нових загроз, від яких традиційні антивірусні системи та брандмауери не можуть захистити. Машинне навчання може зменшити кількість помилкових спрацьовувань, які становлять серйозну загрозу в традиційному виявленні загроз, на 50-90%.

На відміну від інструментів виявлення на основі сигнатур попереднього покоління, машинне навчання може відстежувати та реєструвати моделі використання мережі серед співробітників організації та своєчасно сповіщати менеджерів про виявлення аномальної поведінки.

Одним із найпоширеніших методів машинного навчання для класифікації фішингу є використання списку ключових функцій для представлення електронної пошти та застосування алгоритму навчання для класифікації електронної пошти як фішингу чи хамів на основі вибраних ознак. Чандрасекаран та ін. [3] запропонував нову методику класифікації

фішингових електронних листів на основі чітких структурних характеристик, таких як структура теми електронного листа та деякі функціональні слова. Вони використовували SVM для перевірки своїх функцій на 400 електронних листах і отримали 95% точність. Однак вони не виконували різних розподілів між навчальними та тестовими даними через малий розмір вибірки. Fette та ін. [4] використали десять різних особливостей, специфічних для оманливих методів для класифікації фішингу, і отримали F1-показник понад 90% за допомогою машинного класифікатора опорних векторів. Однак у своєму моделюванні вони використовували значно більше електронних листів любителів (7000), ніж фішингових (860).

Останні досягнення в глибокому навчанні зробили можливим текстовий аналіз великої кількості фішингових електронних листів різних типів. З цієї причини вважається, що загальні особливості фішингових електронних листів можна витягти та дізнатися глибокою нейронною мережею, такою як модель довготривалої короткочасної пам'яті для виявлення фішингу.

Висновки

Таким чином, штучний інтелект, і зокрема інструменти нейронних мереж, є найкращим вибором проти загрози фішингових атак, дозволяючи швидко створити інтелектуальний захист ще до того, як буде здійснено атаку.

Література

1. Lininger, R., and Vines, D. R. (2005). Phishing: cutting the identity theft line. Print book. Indiana: Wiley Publishing, Inc.
2. Vayansky, Ike & Kumar, Sathish. (2018). Phishing – challenges and solutions. Computer Fraud & Security. 2018. 15-20. 10.1016/S1361-3723(18)30007-1.
3. Madhusudhanan Chandrasekaran, Krishnan Narayanan, and Shambhu Upadhyaya. Phishing e-mail detection based on structural properties. In Proceedings of the NYS Cyber Security Conference, 2006.
4. Ian Fette, Norman Sadeh, and Anthony Tomasic. Learning to detect phishing emails. In Proceedings of the International World Wide Web Conference (WWW), 2007

Каліновський Я. О.

*доктор технічних наук, старший
науковий співробітник, старший
науковий співробітник ІПРІ НАН
України*

Боярінова Ю. Є.

*кандидат технічних наук, старший
науковий співробітник, доцент
кафедри СПСКС ФПМ «КПІ ім. Ігоря
Сікорського»*

Гнатенко В. Д.

магістр

КОДУВАННЯ ІНФОРМАЦІЇ ШТРИХОВИМИ КОДАМИ

Разом з розвитком інформаційних технологій досить великого розповсюдження набули технології кодування інформації. Серед великої кількості видів кодування та відображення даних одним з найрозповсюдженіших є штрихове кодування. Галузі використання штрихового кодування дуже різноманітні: від логістики до ідентифікації людини, від збереження інформації до створення посилання на відомі сайти. Технологія штрихового кодування базується на розпізнаванні інформації, закодованої у штрихах та проміжках визначених розмірів. Існує чимало способів збереження інформації у форматі штрихового кодування, кожен з яких використовується для вирішення певної специфічної задачі.

Через збільшення вагової кодованої інформації основна низка існуючих способів або є надлишковими при їх використанні, або не підходить для рішення задачі з відображенням закодованої інформації в обмеженому просторі з великою щільністю даних. Для рішення проблеми запропоновано спосіб двовимірного штрихового кодування та спосіб зворотного кодування, для подальшого декодування даних.

Запропонований спосіб, задовольняючий усім критеріям, має досить просту специфікацію. Кожен символ закодований за допомогою унікальної комбінації смуг та пробілів, що складаються з чотирьох чорних і трьох білих смужок різної товщини. Ширина смужок знаходиться в діапазоні від 1 до 4 мінімальних одиниць товщини. Сума усіх довжин чорних і білих смужок повинна дорівнювати 13. При необхідності можна змінити кількість смуг, які кодують один символ, що дає змогу в подальшому розширити набір символів, які підтримує кодування.

Даний спосіб спроможний кодувати основні символи таблиці ASCII[1], а саме: починаючи з коду 32(Space) і закінчуючи символом з

кодом 127(DEL). В залежності від кількості символів, висота штрихового коду може знаходитись в діапазоні від 1 до 50 строк, що дає змогу закодувати близько 850 символів. Якщо виникне потреба для збільшення кількості символів, можна прибрати штучну заборону на використання більше 50 строк кодування, тоді алгоритм теоретично може зберегти дані об'ємом до 2700 символів, але для зчитування та декодування штрих-коду потрібно буде більше обчислювальної потужності пристрою, що в результаті збільшить час на розпізнавання та обробку коду. Зазвичай використовується діапазон від 7 до 30 строк. На рис. 1 зображено штриховий код, в якому закодовано 290 символів. Він досить схожий на одновимірні штрих-коди, адже кодує символи за схожим чином, тому що дотримується стандарту GS1[2].

Сам код складається з таких зон:

1. Зона без даних або пуста зона. Використовується на початку та у кінці для більш простого розуміння про знаходження стартового та кінцевого символів;
2. Стартовий символ. Вказує на початок коду для полегшення зчитування;
3. Область додаткових даних до стовпчика. Зберігає дані для коректного зчитування строки;
4. Зона даних. Саме у цій зоні знаходяться закодовані дані;
5. Символ для перевірки коректності зчитування. В ньому зберігається сума усіх товщин чорних смуг в області даних;
6. Кінцевий символ. Вказує на кінець кодування штрихового коду.

Для декодування штрихового коду не потрібен спеціальній сканер, вистачить й звичайної камери смартфона. Для вхідних даних алгоритму достатньо лише фотографії, що дає змогу впровадження реалізації способу кодування на будь-якому сучасному смартфоні.

Саме декодування виконується в декілька етапів:

1. На вхід подається фотографія у будь-якому форматі (png, bmp, jpg тощо);
2. Зображення перебудовується у чорно-білий варіант та перетворюється на числовий масив даних, що були побудовані на основі яскравості кольорів пікселів, де значення 0 відповідає білому кольору, а значення 255 – чорному;
3. Відбувається перший етап сканування, а саме знаходження первинних координат штрихового коду, починаючи з середини зображення;
4. Якщо координати знайти не вдалось – проходимо по всьому зображенню в пошуках координат коду. Під час знаходження координат відбувається перехід до наступного пункту і закінчення пошуку;

5. Якщо координати знайшлися – відбувається перехід до верхньої частини штрихового коду і почергове сканування кожної строки. Після вдалого сканування строки відбувається перевірка інформації на відповідність за допомогою даних, що зберігаються в зонах 3 та 5, зображених на рис. 1. Якщо дані були пошкоджені, то сканування переходить до наступного ряду пікселів;

6. Уся оброблена інформація перевіряється і, якщо жоден з рядків не був пропущений під час сканування, повертається текстовий результат.

Штрихове кодування стало невід’ємною частиною нашого сучасного життя. Чимало речей так чи інакше пов’язані з використанням штрих-кодів і з кожним днем їх стає ще більше.

Представлені способи кодування та декодування штрихового коду дозволяють кодувати інформацію для відображення в умовах малої площі розміщення з великою щільністю даних з метою подальшої можливості швидкого декодування. Дане рішення зменшило швидкість як кодування інформації, так і декодування, в порівнянні зі схожим за будовою PFD417[3]. Декодування PFD417 займає 206мс, а у запропонованого способу – 141мс. Тобто, в 1.4 рази швидше.

Список використаних джерел

1. ISO-IR-006: ASCII Graphic character set [Електронний ресурс] – Режим доступу до ресурсу: <https://www.itscj.ipsj.or.jp/iso-ir/006.pdf>

2. GS1-128 standard [Електронний ресурс] – Режим доступу до ресурсу: <https://www.gs1-128.info/>

3. PDF417 standard [Електронний ресурс] – Режим доступу до ресурсу: <https://www.iso.org/obp/ui/#iso:std:iso-iec:15438:ed-3:v1:en>

Казьмірук С. Д.

*аспірант Державної наукової
установи «Інститут інформації,
безпеки і права Національної академії
правових наук України»*

Леонов Б. Д.

*доктор юридичних наук, професор,
головний науковий співробітник
МНДЦ при РНБО України*

ЗАСТОСУВАННЯ ПОЛІГРАФА ЯК ЗАХІД З ВІДНОВЛЕННЯ ДОВІРИ ДО ДЕРЖАВНИХ ІНСТИТУТІВ

У рамках європейської і євроатлантичної інтеграції України довіра до державних інститутів є запорукою незмінного курсу держави на набуття членства України в Європейському Союзі та Організації Північноатлантичного договору і є одним із ключових моментів забезпечення національної безпеки [1].

З цією метою Україна має сформувати власні спроможності щодо формування ефективної безпекової стійкості у сфері національної безпеки, взявши активну участь у співпраці з партнерами та країнами-членами НАТО у сфері колективної безпеки і оборони.

Указом Президента України від 30 червня 2023 року №359 введено у дію Рішення Ради національної безпеки і оборони України від 23 червня 2023 року «Про прискорення судової реформи та подолання проявів корупції у системі правосуддя», зміст якого, зокрема, передбачає необхідність внесення змін до законів України «Про судоустрій і статус суддів» та «Про Вищу раду правосуддя» щодо запровадження психофізіологічного дослідження із застосуванням поліграфа як умови при доборі кандидатів на посаду судді.

Отже, Рада національної безпеки і оборони України для відновлення довіри до судової гілки влади, прискорення судової реформи та подолання проявів корупції у системі правосуддя вирішила звернутися до суб'єктів права законодавчої ініціативи щодо необхідності розгляду питання: можливості запровадження періодичного психофізіологічного опитування суддів із застосуванням поліграфа; запровадження психофізіологічного опитування із застосуванням поліграфа як умови при доборі кандидатів на посаду судді місцевого суду, конкурсу на зайняття вакантних посад суддів апеляційних судів, вищих спеціалізованих судів та Верховного Суду з метою вироблення оптимальної та ефективної процедури перевірки відповідності кандидатів у судді критеріям доброчесності,

професійної етики або існування інших обставин, які можуть негативно вплинути на суспільну довіру до судової влади у зв'язку з призначенням такого кандидата на посаду судді [1].

Метою дослідження із застосуванням поліграфа є виявлення корупційних ризиків та інших правопорушень вчинених особою які можуть негативно вплинути на суспільну довіру до представників влади у зв'язку з призначенням кандидата на посаду.

Порядок проведення психофізіологічного дослідження із застосуванням поліграфа затверджуватиме Вища рада правосуддя України, при якій доцільно створити «Центр системи виявлення прихованої або недостовірної інформації» для запровадження єдиних державних стандартів проведення психофізіологічного дослідження із застосуванням поліграфа. Зауважимо, що результати психофізіологічного дослідження із застосуванням поліграфа не є підставою для рішення про відмову особі в обійманні посади, а мають рекомендаційний характер. Водночас, відмова кандидата від дослідження при прийомі на роботу є підставою для відмови в розгляді його кандидатури.

У Верховній Раді України зареєстровано законопроекти (реєстр. № 9454 від 03.07.2023) «Про внесення змін до Закону України «Про судоустрій і статус суддів» щодо запровадження додаткових процедур для зміцнення довіри суспільства до судової влади та «Про внесення змін до Закону України «Про судоустрій і статус суддів» щодо запровадження додаткових процедур для зміцнення довіри суспільства до судової влади (реєстр. № 9454-1 від 11.07.2023). Ці законопроекти передбачають застосування поліграфу з метою зміцнення довіри суспільства до судової влади та інститутів правосуддя, а також посилення авторитету суддів в державі.

Акцентуємо увагу, що серед загроз національній безпеці корупційні ризики є одними з найнебезпечніших за своїми наслідками. Глава держави має намір подати законопроект щодо прирівняння корупції до державної зради на воєнний час [2].

Вищезазначене свідчить, що проведення психофізіологічного дослідження із застосуванням поліграфа в контексті зміцнення довіри суспільства до представників держави може стати одним з інструментів перевірки на предмет доброчесності кандидатів на посади осіб, уповноважених на виконання функцій держави.

Підтримуючи зазначені законодавчі ініціативи, вважаємо, що добровільна згода з боку народних депутатів України на особисте проходження психофізіологічного дослідження із застосуванням поліграфа щодо доброчесної поведінки може бути потужним сигналом сприяння про-

тидії корупції для українського суспільства та міжнародних партнерів. Така пропозиція потребує обговорення серед експертів, практикуючих фахівців та науковців.

Застосування поліграфа сприяє вирішенню важливих завдань у сфері національної безпеки: 1) судової експертизи; 2) реалізації прозорої кадрової політики; 3) підвищення ефективності службових розслідувань; 4) добору кандидатів на посаду судді під час спеціальної перевірки, службових розслідувань, а також переведення до іншого суду; 5) запровадження додаткових процедур для подолання проявів корупції, перевірки доброчесності та зміцнення довіри суспільства до всіх осіб, уповноважених на виконання функцій держави.

Аналіз стану застосування поліграфа в Україні свідчить про відсутність єдиної стратегії та системного підходу. Важливим аспектом для національної безпеки держави залишається організація єдиної системи застосування поліграфа на основі міжнародних стандартів ASTM International та American Polygraph Association [3,4].

Перспективами застосування поліграфа як заходу з відновлення довіри до державних інститутів є запровадження інноваційних підходів та технологій, які ефективно застосовуються країнами-членами НАТО у сфері виявлення прихованої та недостовірної інформації та впровадження державних стандартів навчання поліграфологів та проведення психофізіологічного дослідження із застосуванням поліграфа.

Отже, важливо розробити єдині стандарти та правила для застосування поліграфа, з урахуванням позитивного міжнародного досвіду та кращих світових практик у сфері національної безпеки держави. Це сприятиме активізації та переведення у практичну площину процесів європейської і євроатлантичної інтеграції України, а також відновленню довіри до державних інститутів.

Список використаних джерел

1. Рішення Ради національної безпеки і оборони України від 23 червня 2023 року «Про прискорення судової реформи та подолання проявів корупції у системі правосуддя»: введене в дію Указом Президента України від 30 червня 2023 року №359. URL: <https://www.president.gov.ua/documents/3592023-47185>

2. Зеленський хоче прирівняти корупцію до держзради на час війни. URL: <https://www.pravda.com.ua/news/2023/08/27/7417309/>.

3. ASTM International. URL: <https://www.astm.org/>.

4. American Polygraph Association. URL: <https://www.polygraph.org/>.

ПОЛІТИЧНА ПОЗИЦІЯ РОСІЙСЬКОГО МУСУЛЬМАНСЬКОГО ДУХОВЕНСТВА В УКРАЇНСЬКО- РОСІЙСЬКІЙ ВІЙНІ

В Російських засобах масової інформації розвивається наратив братнього військового духу російських мусульман та православних. Наприклад, в Республіці Татарстан телеканал «Мензеля-інформ» міста Мензелінськ повідомив, що військовослужбовці Російської Федерації, які складаються з жителів Татарстану у складі батальйону Алга, вирушають в Україну виконувати бойові завдання в рамках спеціальної військової операції. З напутньою промовою перед військовослужбовцями виступили православний священник та мусульманський муфтії, побажавши солдатам виконати бойові завдання та повернутися живими [1].

Це свідчить про те, що в російсько-українському військовому конфлікті 2022 року спостерігалася гібридизація та єднання російської державної ідеології «Російського Світу» та релігійних інститутів – російського православ'я та ісламу, які підтримують російське керівництво та спеціальну військову операцію.

Під час бойових дій в Україні були помічені російські солдати, які сповідують православ'я та іслам, які, згідно зі своїм віросповіданням, пліч-о-пліч молилися Богу та Аллаху. Так 1 березня 2022 року, мешканцями міста Херсон було опубліковано відео, на якому двоє російських солдатів моляться перед православним храмом. Православний солдат хреститься, тоді як солдат, який сповідує іслам, здійснює молитву (намаз), стоячи на колінах на молитовному килимі [2].

Якщо розглядати позицію мусульманського духовенства Росії загалом, можна констатувати, що воно підтримало спеціальну військову операцію в Україні. Так, 31 березня 2022 року, у місті Владикавказ було проведено конференцію «Духовне служіння та соціальна місія релігійних організацій у контексті формування загальноросійської громадянської ідентичності», на якій лідери мусульманських релігійних організацій Росії зробили заяву про підтримку президента Росії щодо проведення військової спецоперації в Україні. У заяві мусульманських релігійних лідерів було сказано:

«Ми, представники мусульманських організацій Росії, хочемо заявити про свою підтримку керівництва Російської Федерації, повне схвалення концепції її військової доктрини як оборонної. Нібито націоналісти, які представляють український народ, протягом восьми років безперервно порушували Мінські угоди. Керівництво України вісім років убивало мирних жителів та вело підготовку до бліцкригу для повного

знищення населення Донецької та Луганської народних республік, щоб потім наблизити НАТО з його ядерною та біологічною зброєю безпосередньо до кордонів Росії, створивши пряму загрозу національній безпеці всієї нашої країни, всіх наших громадян [3].»

Загалом можна констатувати, що російське мусульманське духовенство, як і Російська Православна Церква, підтримує рішення російської влади про проведення військової спеціальної операції в Україні та пояснює це національними інтересами Російської Федерації, щодо забезпечення національної безпеки.

Для дослідження запитів в інтернеті пов'язаних з мусульманами в Російській Федерації та відношенні їх до спеціальної військової операції було застосовано систему контент-моніторингу Infostream (infostream.ua). За дванадцять місяців 2022 року було знайдено 189 документів з російських веб-ресурсів, у яких згадується словосполучення «Муфтії Росії», «Таджуддін», «Верховний Муфтії» при обов'язковому змісті слів/словосполучень «Спецоперація» або «Спеціальна військова операція».

Нижче наведено графік динаміки (залежності кількості документів за цим запитом по днях року):

Дослідження показало, що максимальна інтенсивність публікацій спостерігалася до 9 серпня 2022 року, а розподіл матеріалів мав приблизно рівномірний характер.

Локальні максимуми кількості публікацій було досягнуто наступними днями:

1	2022.03.02	3	2022.05.20	5	2022.10.26
2	2022.03.26	4	2022.07.09	6	2022.12.17

Література:

1. Мензелінське патріоти будуть служити в батальйоне «Алга». Мензеля Інформ. URL: <https://www.youtube.com/watch?v=GgOEkZiEtiU> (01.05.2023)
2. Военные молятся. 01.03.2022. URL: <https://www.youtube.com/watch?v=GmLBQKT48Kw> (01.05.2023)
3. Всероссийская научно-практическая конференция «Духовное служение и социальная миссия религиозных организаций в контексте формирования общероссийской гражданской идентичности» состоялась во Владикавказе. Национальный антитеррористический комитет. 31.03.2022. URL: <http://nac.gov.ru/konferencii-i-kruglye-stoly/vserossiyskaya-nauchno-prakticheskaya-konferenciya.html> (01.05.2023).

Наукове видання

**НОРМАТИВНО-ПРАВОВА ІНФОРМАЦІЯ
І ПАРЛАМЕНТСЬКИЙ КОНТРОЛЬ**

МАТЕРІАЛИ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

Київ, 21 вересня 2023 року

*Науковий керівник конференції:
Д. В. Ланде*

*Упорядники:
В. М. Фурашев, А. І. Нижник, С. О. Дорогих*

Підписано до друку 08.12.2023.
Формат 60x84/16. Ум-друк. арк. 6,98.
Наклад 100 прим. Зам. № 2312-03.

Видавець ПП «Фенікс»
(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).
Україна, м. Одеса, 65009, вул. Зоопаркова, 25.
e-mail: fenix-izd@ukr.net