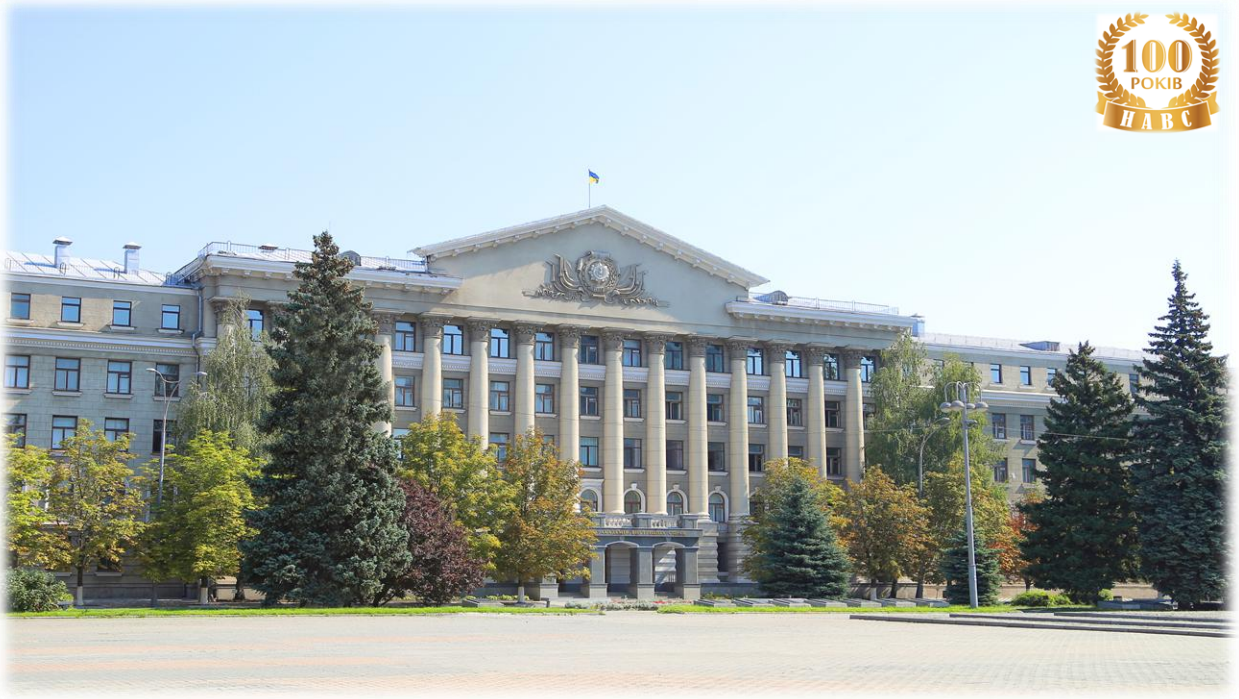
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
Кафедра теорії, історії та філософії права

ІНФОРМАЦІЙНА БЕЗПЕКА СУСПІЛЬСТВА В УМОВАХ ДІЇ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ ТА ПОВОЄННИЙ ПЕРІОД

Збірник матеріалів
Міжвідомчого науково-практичного круглого столу
(Київ, 29 травня 2025 року)



Київ
2025

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
Кафедра теорії, історії та філософії права

ІНФОРМАЦІЙНА БЕЗПЕКА СУСПІЛЬСТВА В УМОВАХ ДІЇ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ ТА ПОВОЄННИЙ ПЕРІОД

Збірник матеріалів
Міжвідомчого науково-практичного круглого столу
(Київ, 29 травня 2025 року)

Київ
2025

УДК 004.056.5(477)

Редакційна колегія:

Тарасенко О.С., проректор Національної академії внутрішніх справ, доктор юридичних наук, професор.

Чернявський С.С., проректор Національної академії внутрішніх справ доктор юридичних наук, професор.

Гусарєв С.Д., провідний науковий співробітник відділу організації наукової діяльності Національної академії внутрішніх справ, доктор юридичних наук, професор.

Пендюра М.М., завідувач кафедри теорії, історії та філософії права навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, доцент.

Кривицький Ю.В., завідувач кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат юридичних наук, доцент.

Кравець В.М., професор кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат юридичних наук, доцент.

Рекомендовано для оприлюднення засіданням кафедри теорії, історії та філософії права Національної академії внутрішніх справ від 17 липня 2025 р. (протокол № 25).

Матеріали подано в авторській редакції. Відповідальність за їхню якість, а також відсутність у них відомостей, що становлять державну таємницю та службову інформацію, несуть автори.

Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повоєнний період : зб. матеріалів (Київ, 29 трав. 2025 р.) / Редкол. : О. С. Тарасенко та ін. Київ : Нац. акад. внутр. справ, 2025. 181 с.

У збірнику розміщено результати наукових пошуків науково-педагогічних, наукових, практичних працівників і здобувачів вищої освіти з проблематики інформаційної безпеки суспільства в умовах дії правового режиму воєнного стану та повоєнний період, а також із широкого кола питань філософських, історико-теоретичних і галузевих юридичних наук через призму творчого доробку вітчизняної вченої Юлії Максименко.

Збірник матеріалів може бути використаний в освітньому процесі, науковій діяльності, є доступним для широкого загалу та сприятиме формуванню високого рівня правової культури та правової свідомості суспільства в цілому.

УДК 004.056.5(477)

© Національна академія внутрішніх справ, 2025

ЗМІСТ

НАУКОВІ ПОВІДОМЛЕННЯ

РЕКОМЕНДАЦІЇ

міжвідомчого науково-практичного круглого столу
«Інформаційна безпека суспільства в умовах дії правового режиму
воєнного стану та повоєнний період»

29 травня 2025 р. новостворені кафедра теорії, історії та філософії права Національної академії внутрішніх справ спільно з кафедрою теорії, історії та філософії права навчально-наукового інституту права та психології академії відповідно Плану науково-дослідної роботи Національної академії внутрішніх справ на 2025 рік організували і провели міжвідомчий науково-практичний круглий стіл на тему: «Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повоєнний період», присвячений пам'яті доцента кафедри теорії держави та права Юлії Євгенівни Максименко (1981–2021 рр.), кандидата юридичних наук, доцента.

Цей науковий захід продовжив добру традицію щорічних наукових заходів, започаткованих кафедрою теорії держави та права у 2010 році, з метою увічнення пам'яті та популяризації наукового доробку відомих вчених, ветеранів кафедри й академії. У роботі міжвідомчого науково-практичного круглого столу взяли участь відомі вчені, наукові та науково-педагогічні працівники, здобувачі вищої освіти закладів вищої освіти, представники наукових установ, центральних органів виконавчої влади, а також юристи-практики.

В освітньо-науковій сфері Юлія Євгенівна Максименко відома як талановита вчена, фахівець у сфері теорії держави та права, безпекознавства. Вона успішно працювала над вивченням різних правових і державних проблем, але найбільший внесок зробила у розробку таких теоретико-правових питань як інформаційні права людини, інформаційна безпека суспільства, забезпечення правового статусу особи в діяльності правоохоронних органів, правової держави, громадянського суспільства та ін.

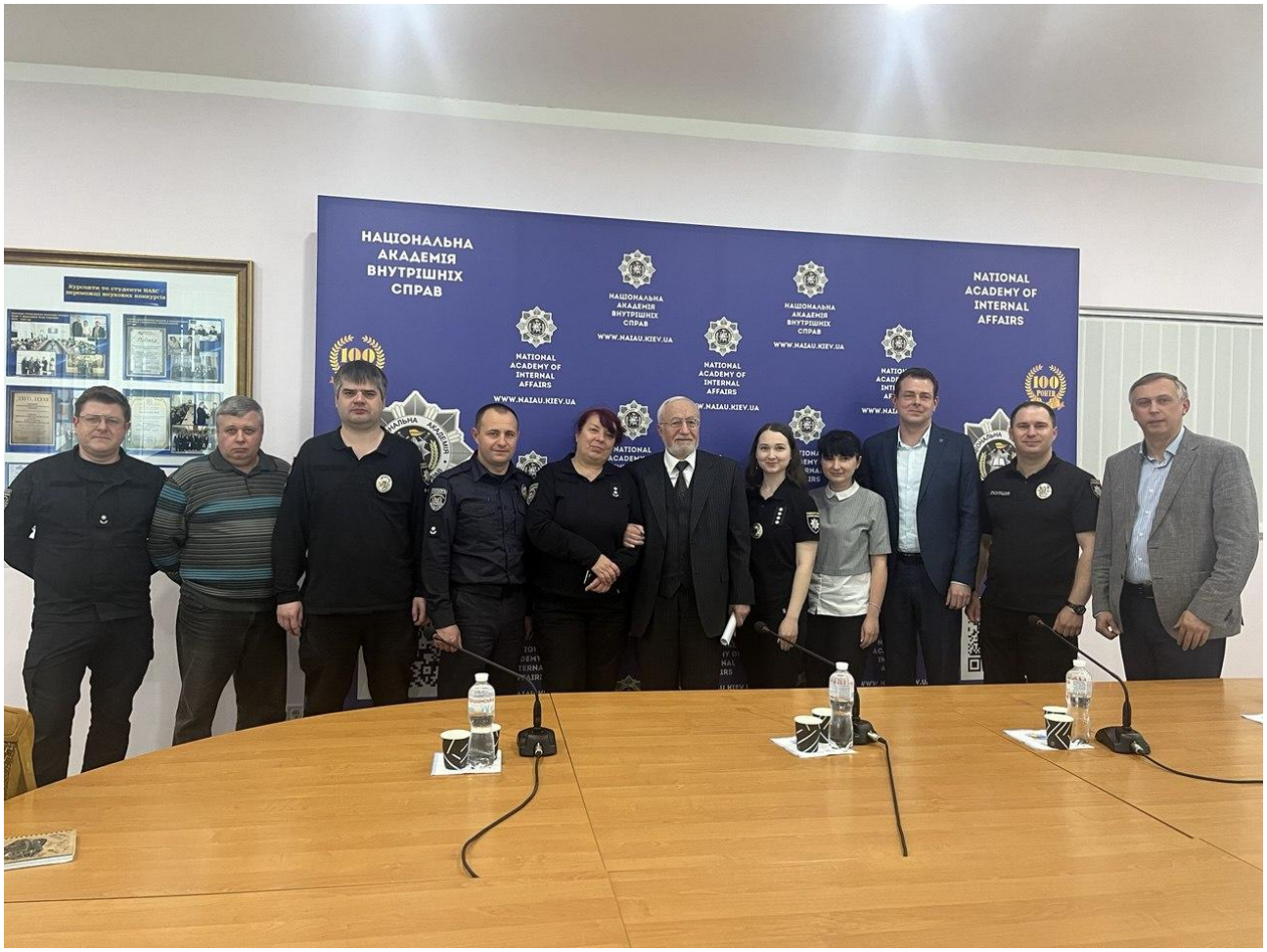
Науковий захід пройшов в теплому, дружньому середовищі в дусі конструктивної дискусії з поміркованою полемікою. Особливу увагу організатори та учасники заходу приділили життєвому шляху і творчому доробку Юлії Євгенівна Максименко. Учасники зібрання обмінялися думками з низки актуальних проблем права та держави, безпекознавства, зокрема принципи конституційно-правового статусу Українського народу, упорядкування законодавства в умовах забезпечення інформаційної безпеки, інформаційна безпека в умовах глобалізації тощо. Серед виступів, які викликали підвищений інтерес, варто виокремити наукові доповіді Михайла Васильовича Костицького та Наталії Вадимівни Кушакової-Костицької на тему: «Правові та етичні проблеми регулювання інтернет в контексті інформаційної безпеки: до постановки питання», Наталії Миколаївни Пархоменко – «Стан наукового потенціалу України як загроза для національної безпеки держави», Олександра Олександровича Тихомирова – «Сучасне розуміння інформаційної безпеки: виміри та рівні забезпечення», а також наукові повідомлення Катерини Сергіївни Білодід на тему: «Соціальні мережі як інструмент інформаційної війни: атаки, фейки та протидія», а також Сергія Євгенійовича Логінова – «Особливості

реалізації інформаційної функції патрульної поліції в умовах воєнного стану».

За результатами міжвідомчого науково-практичного круглого столу «Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повоєнний період» рекомендовано:

– використати окремі положення тез доповідей, що висвітлені під час наукового заходу, при розробці та вдосконаленні навчально-методичних матеріалів для навчальних дисциплін: «Теорія держави та права», «Юридична компаративістика», «Державна політика у сфері національної безпеки»;

– у майбутньому при дотриманні відповідних вимог, передбачених Порядком видачі диплома про вищу освіту з відзнакою в Національній академії внутрішніх справ, враховувати опубліковані тези доповідей у цьому збірнику матеріалів як одну з підстав для отримання диплома з відзнакою.



ПРИВІТАННЯ УЧАСНИКІВ КРУГЛОГО СТОЛУ

Тарасенко Олег Сергійович,
проректор Національної академії внутрішніх справ,
доктор юридичних наук, професор

Шановні колеги!

Щиро вітаю всіх учасників науково-практичного круглого столу!

Відповідно до Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 р. № 685/2021, забезпечення інформаційної безпеки є однією з найважливіших функцій сучасної держави. Уже на початку повномасштабної російсько-української війни наша держава отримала першу важливу перемогу – перемогу в інформаційній війні. Вона стала можливою завдяки кожному громадянину та українському суспільству загалом. Тисячі кіберспеціалістів та інших фахівців у сфері інформаційної безпеки з сектору безпеки і оборони, приватного й державного секторів сформували справжню могутню армію. Заради спільної мети – суверена, незалежна та демократична Україна.

Інформаційна війна розпочалася задовго до широкомасштабного вторгнення РФ. І досі триває поряд із масованими ракетними обстрілами. Її наслідки не такі помітні, на перший погляд, як зруйновані будинки і втрачені життя, покалічені долі… Проте вони не менш руйнівні… Тимчасово окуповані території – це наші втрати і в інформаційній війні. Перші втрати, яких ми зазнали. Адже держава-агресор використала цілий арсенал спеціальних інформаційних операцій, спрямованих на підрив обороноздатності України, розпалювання міжетнічних, міжконфесійних, мовних конфліктів, створення негативного іміджу України в світі, зокрема корупційного. Однак ми робимо висновки, вчимося та стаємо сильнішими у протидії руйнівному інформаційному впливу держави-агресора в умовах розв'язаної нею війни.

Сьогодні серед учасників круглого столу представники суб'єктів сектору безпеки і оборони, інститутів громадянського суспільства, провідних закладів вищої освіти та наукових установ України. Ваш багаторічний досвід і знання – це той наріжний камінь, який дозволяє об'єднати зусилля та виробити дорожню карти для українського суспільства в умовах війни та післявоєнний період, окреслити нові контури інформаційної безпеки у світлі сучасних глобальних трансформацій. Адже кожен громадянин нашої держави вже сьогодні живе у вільній і незалежній країні, де інформаційні права є невід'ємною складовою демократичних прав і свобод, які виборюються ціною життя. У цьому аспекті проведення круглого столу є своєчасним та актуальним, а також гарною нагодою осмислити та визначити дієві механізми протидії загрозам національній безпеці, насамперед в інформаційній сфері, з урахуванням сучасних реалій.

Бажаю всім учасникам наукового заходу плідної співпраці та активного обговорення.

Слава Україні!

Гусарєв Станіслав Дмитрович,
провідний науковий співробітник
відділу організації наукової діяльності
Національної академії внутрішніх справ,
доктор юридичних наук, професор

Шановні колеги, вітаю!

Приєднуюся до вітань учасників міжвідомчого науково-практичного круглого столу!

Сьогодні ми зібралися, щоб не лише обговорити актуальні та важливі питання, виклики й інноваційні рішення у сфері інформаційної та кібербезпеки, але й вшанувати пам'ять Юлії Максименко, яка своєю працею, відданістю та професіоналізмом надихала нас усіх. Її життя було прикладом кропіткою наукової діяльності щодо безпечного інформаційного простору й ми прагнемо продовжити її справу, розвиваючи та зміцнюючи цю важливу сферу.

В умовах повномасштабної військової агресії проти України науковці та науково-педагогічні працівники закладів системи МВС України, зокрема Національної академії внутрішніх справ, продовжують професійно виконують покладені на них обов'язки, а здійснювана ними наукова діяльність дозволяє центральному органу виконавчої влади своєчасно та ефективно реагувати на виклики в умовах збройної агресії. Тематика сьогоднішнього наукового заходу – це відповідь на виклик війни, розв'язаної РФ проти України, агресивної, жорстокої, неспровокованої. Це – віддзеркалення найзлободенніших проблем нашого суспільства, що торкнулися кожного у зв'язку з соціально-політичною ситуацією в державі та необхідності забезпечення національної безпеки, територіальної цілісності нашої країни, збереження життя і здоров'я кожного українця, убезпечення від криміногенних загроз у кризовий період.

Цей науково-практичний круглий стіл – це платформа для обміну знаннями, ідеями та досвідом. Ми розглянемо сучасні загрози, такі як кібератаки, шахрайство з використанням штучного інтелекту, та новітні методи захисту інформації. Впевнений, що ваші доповіді, дискусії та пропозиції стануть вагомим внеском у розвиток інформаційної безпеки в Україні та за її межами.

Сподіваємося, що результати науково-практичного круглого столу, доробок його учасників стануть вагомим теоретичним підґрунтям для розв'язання нагальних завдань у процесі підготовки здобувачів вищої освіти Національної академії внутрішніх справ, їх інформаційно-правового та національно-патріотичного виховання.

Бажаю всім нам плідної роботи, цікавих виступів, нових знайомств і, головне, натхнення для подальших звершень. Нехай цей науковий захід стане ще одним кроком до безпечнішого цифрового майбутнього, яке ми будуємо разом, пам'ятаючи про теоретичний доробок Юлії Максименко.

Слава Україні!

ЖИТТЄВИЙ І ПРОФЕСІЙНИЙ ШЛЯХ МАКСИМЕНКО ЮЛІЇ ЄВГЕНІЇВНИ – ДОСЛІДНИЦІ ТЕОРІЇ ДЕРЖАВИ ТА ПРАВА Й ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

(кандидат юридичних наук за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень (диплом ДК № 046187 від 21 травня 2008 р.); вчене звання доцент кафедри теорії держави та права (атестат доцента 12ДЦ № 043723 від 29 вересня 2015 р.)
(1981–2022 рр.)

Становлення і розвиток національної юридичної науки неможливо уявити без імен яскравих дослідників, які присвятили своє життя служінню праву, освіті та науковим дослідженням. Однією з таких постатей кафедри теорії держави та права Національної академії внутрішніх справ є Максименко Юлія Євгеніївна – кандидат юридичних наук, доцент, фахівець у галузі теорії держави та права, а також дослідниця проблем інформаційної безпеки держави. Її наукова та педагогічна діяльність залишила глибокий слід у розвитку юридичної освіти та наукової думки України.

Юлія Євгеніївна Максименко народилася 19 лютого 1981 р. у селі Бортничі Київської області. Свій професійний шлях вона розпочала в серпні 1998 р. як курсант Національної академії внутрішніх справ України. Після закінчення навчання працювала слідчим у підрозділах органів внутрішніх справ Київської області, зокрема у відділі розслідування злочинів, вчинених організованими групами.

У 2002–2003 рр. навчалася в магістратурі Національної академії внутрішніх справ України, яку закінчила з відзнакою, після чого обіймала посади викладача-методиста Центру дистанційного навчання та розробляла навчальні курси з використанням новітніх освітніх технологій.

З 2006 р. почалася її викладацька кар’єра в Київському національному університеті внутрішніх справ, а згодом у Національній академії внутрішніх справ, де вона пройшла шлях від викладача кафедри міжнародних відносин та національної безпеки до доцента кафедри теорії держави та права.

У 2007 р. Ю.Є. Максименко під науковим керівництвом доцента В.А. Ліпкана захистила кандидатську дисертацію на тему: «Теоретико-правові засади забезпечення інформаційної безпеки України» для здобуття наукового ступеня кандидат юридичних наук за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Це наукове дослідження стало вагомим внеском у формування національної доктрини інформаційної безпеки в умовах становлення незалежної України.

Попри невеликий життєвий і професійний шлях Юлія Євгеніївна є автором понад 100 наукових праць, включаючи підручники, навчальні посібники, статті та методичні розробки. Особливе місце в її доробку займають такі видання як:

- «Інформаційна безпека України в умовах євроінтеграції» (2006 р.);
- «Теоретико-правові засади забезпечення інформаційної безпеки України» (2007 р.);
- «Теорія управління в органах внутрішніх справ» (2007 р., у співавторстві з В.А. Ліпканом);
- підручник «Міжнародне право» (2009 р.) і низка співавторських навчальних посібників з теорії держави та права (2017 р.).

У своїй професійній діяльності вона викладала навчальні дисципліни з «Юридичної деонтології», «Теорії держави та права», «Історії вчень про право і державу», «Юридичної компаративістики», а також спеціальні дисципліни, спрямовані на підготовку наукових кадрів.

Вона активно впроваджувала дистанційні технології навчання, розробила мультимедійні навчальні модулі з інформаційної безпеки та інтегрувала кейс-стаді з реальних розслідувань в освітній процес.

Її наукова діяльність характеризується міждисциплінарним підходом, синтезом теоретико-правового аналізу та практичної орієнтації досліджень. Вона активно досліджувала правові механізми забезпечення національної безпеки, інформаційну політику держави, а також сучасні виклики у сфері кібербезпеки.

Максименко Юлія Євгеніївна була яскравим представником нового покоління українських правознавців, які поєднували наукову глибину, викладацький талант і практичний досвід. Її внесок у розвиток правової думки, інформаційної безпеки, а також у підготовку майбутніх юристів України залишається значущим і актуальним надалі. Її фундаментальні дослідження з теорії держави та права, інформаційної безпеки стали базою для сучасних правових стандартів захисту інформації в Україні. Внесок вченої продовжує визначати стратегію кібербезпеки державних інституцій і готує підґрунтя для подальших досліджень у цій критично важливій сфері.

Її життя – приклад відданості науці, державі та праву. Пам’ять про неї житиме в наукових працях, серед колег, учнів і в серцях тих, хто мав честь із нею працювати.

Завідувач кафедри теорії, історії та філософії права
навчально-наукового інституту права та психології
Національної академії внутрішніх справ **Максим ПЕНДЮРА**

Завідувач кафедри
теорії, історії та філософії права
Національної академії внутрішніх справ **Юрій КРИВИЦЬКИЙ**

НАУКОВІ ДОПОВІДІ

Костицький Михайло Васильович, *професор кафедри теорії, історії та філософії права навчально-наукового інституту права та психології Національної академії внутрішніх справ, академік НАПрН України, почесний академік НАПН України, доктор юридичних наук, професор, заслужений юрист України, головний науковий співробітник Інституту правотворчості та науково-правових експертиз НАН України*

Кушакова-Костицька Наталія Вадимівна, *професор кафедри теорії, історії та філософії права навчально-наукового інституту права та психології Національної академії внутрішніх справ, доктор юридичних наук, професор, заслужений юрист України, провідний науковий співробітник Інституту правотворчості та науково-правових експертиз НАН України*

ПРАВОВІ ТА ЕТИЧНІ ПРОБЛЕМИ РЕГУЛЮВАННЯ ІНТЕРНЕТ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ДО ПОСТАНОВКИ ПИТАННЯ

Ефективне вирішення будь-якої проблеми неможливо без чіткого і правильного її формулювання. Коли йдеться про регулювання інформаційних відносин, зокрема, у мережі Інтернет, складності формулювання кола правових та етичних проблем пов’язані насамперед з темпами технологічного розвитку цієї сфери і значним відставанням відповідного нормативно-правового забезпечення.

Сьогодні, на нашу думку, основні питання, зумовлені інформаційно-психологічною загрозою на індивідуальному і соціальному рівні, та які потребують осмислення як в теоретичному, світоглядному, так і в практичному, правовому ракурсах, наступні:

1) чи є проблема регулювання Інтернет загальноцивілізаційною, перманентною незалежно від часу і притаманною будь-якій державі, зумовленою поширенням (за допомогою інформаційно-комунікативних технологій) світоглядних настанов як засобу маніпуляції свідомістю - головним інструментом влади, її «квінтесенцією»;

2) чи є проблема регулювання Інтернет ідеологічною, пов'язаною із впровадженням концепції цифрового / техногенного суспільства на противагу інформаційному суспільству / суспільству знань? Чи домінуватиме найближчим часом концепція алгоритмічного суспільства, розвиток якого базується на застосуванні технологій штучного інтелекту ?

3) чи є проблема регулювання Інтернет переважно технологічною, пов'язаною із постійними технологічними інноваціями в цій сфері, трансформацією інформаційних технологій в інформаційно-комунікаційні, а на сьогодні в цифрові технології?

Видається, що проблема інформаційно-психологічної безпеки за змістом є перманентною, а змінюються лише технології розповсюдження негативної інформації, що пов'язано з формальною стороною проблеми. Дедалі стає очевидним, що головною світоглядною проблемою сучасного соціуму є криза попередніх ідеологій та його неспроможність створити нові, і як наслідок – намагання людини відшукати нові сенси буття та світоглядні орієнтири в інформаційному просторі, переміщення з фізичної площини прагматичного світу у площину Інтернет-реальності.

За таких умов важливим напрямом вирішення проблеми інформаційної безпеки виступає застосування морально-етичних засобів, зокрема, інформаційної та комп'ютерної етики, які орієнтовані на захист на прав людини в мережі і пов'язані насамперед з інтелектуальною свободою, моральною та юридичною відповідальністю, безпекою користувачів Інтернет, із авторським правом тощо. При цьому поняття інформаційної та комп'ютерної етики дуже близькі й охоплюють ідентичні кола проблем, але відрізняються специфікою поля дослідження. Інформаційна етика є більш широким поняттям, орієнтованим на вироблення і застосування етичних норм в мережі Інтернет зокрема та в галузі інформаційних відносин загалом. Комп'ютерна етика пов'язана насамперед із використанням комп'ютерних технологій та виробленням відповідних правил поведінки як користувачів, так і професіоналів, охоплюючи питання реалізації та захисту їх прав, вироблення засобів і методів попередження та боротьби з інформаційними та комп'ютерними злочинами, етико-правові проблеми охорони інтелектуальної власності та авторського права в Інтернеті.

Загалом аналіз етичних проблем в Інтернеті дозволяє запропонувати таку їх диференціацію:

1) проблеми, пов'язані із доступом до інформаційних ресурсів та визначення його легітимного обмеження в контексті інформаційної безпеки;

2) проблеми, пов'язані із створенням та поширенням контенту в Інтернеті, вільним інформаційним обміном;

3) проблеми, пов'язані із захистом прав і свобод користувачів Інтернету, зокрема, у зв'язку із виникненням нових видів інформаційних прав;

4) проблеми, пов'язані із визначенням та дотриманням морально-етичних та правових обов'язків користувачів Інтернету.

За таких умов найбільш ефективним шляхом вирішення вказаних проблем вбачається не розроблення нормативно-правових та адміністративно-організаційних механізмів переважно заборонного та обмежуючого характеру, а

використання механізмів саморегуляції Інтернет-простору у вигляді етичних кодексів, які діють на рівні самосвідомості, загальної та правової культури індивіда і не передбачають примусових методів впливу на прийняття ним рішень і можливу поведінку в мережі.

Резюмуючи, можна зазначити, що інформатизація всіх сфер суспільного життя, віртуальна екзистенція сучасної людини завдяки мережі Інтернет, медійна / інформаційна перенасиченість на фоні активного поширення дезінформації та дифамації в соціальних мережах, де здатний зорієнтуватись далеко не кожний, призвели до втрати загальноприйнятної ієрархії моральних цінностей. Це в свою чергу призводить до подальшої реалізації технології «вікна Овертона», орієнтованої на зникнення поняття норми як такої (етичної, правової, психічної тощо). Фактично йдеться про переосмислення в сенсі нівелювання ролі моралі в житті особистості та соціуму. Водночас через специфіку і можливості регулювання відносин в інформаційному просторі призначення моралі все більше пов'язується не з приведенням поведінки людини у відповідність формальним нормам, а з необхідністю забезпечення поваги до неї, визнанні самоцінності та гідності кожної особистості, що зрештою повинно стати превалюючим чинником подальших позитивних трансформацій Інтернет-спільноти.

Пархоменко Наталія Миколаївна,
завідувач відділу теорії держави і права Інституту держави і права імені В.М. Корецького НАН України, доктор юридичних наук, професор, член-кореспондент НАН України, член-кореспондент НАПрН України, заслужений юрист України

СТАН НАУКОВОГО ПОТЕНЦІАЛУ УКРАЇНИ ЯК ЗАГРОЗА ДЛЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

Безпека громадян, здатність в разі потреби захистити їх права та свободи, зберегти цілісність та незалежність, забезпечити стабільність правопорядку та панування верховенства права є одним із найцінніших здобутків будь-якого цивілізованого та демократичного суспільства та держави.

Загалом поняття безпеки визначається як діяльність людей, суспільства, держави, світового співтовариства народів щодо виявлення (вивчення), запобігання, послаблення, усунення (ліквідації) і відвернення загрози, здатної згубити їх, позбавити матеріальних і духовних цінностей, завдати невідшкодованих збитків, заблокувати шляхи для прогресивного розвитку [1, с. 47].

З огляду та в умовах зростаючої світової тенденції до виникнення різного роду збройних конфліктів, і особливо російсько-української війни, яка триває вже більше ніж десять років; руйнування або трансформації створених раніше безпекових блоків та союзів, намагання створити нові, пошуку новітніх засобів забезпечення миру в різних регіонах; гібридних воєн, що включають економічне, інформаційне, політичне та воєнне втручання в розвиток держав, нагальною потребою є удосконалення існуючих та створення нових механізмів та засобів захисту національних інтересів, національної безпеки.

Відповідно безпека, в усіх її проявах: суспільна, державна, національна; економічна, політична, інформаційна, екологічна, енергетична та ін., та її забезпечення є однією з найактуальніших проблем сучасної науки та практики.

При цьому сама наука в Україні наразі вимагає посиленої уваги з боку держави як одне з надбань та невід'ємна складова успішності держави, її визнання на міжнародній арені, показник інтелектуального потенціалу нації та народу, інструмент прогресивного розвитку та цивілізованості, чинник та водночас складова національної безпеки держави, особливо в умовах правового режиму воєнного стану.

Втім наразі стійкою є тенденція старіння наукової інфраструктури, скорочення наукових кадрів, обвальне падіння наукоємності ВВП, що свідчить про руйнування наукового потенціалу України та вже стали загрозою для національної безпеки держави [2], що потребує негайного втручання держави. При цьому може виникнути питання, а чому саме зараз в умовах правового режиму воєнного стану, можливо необхідно почекати до завершення війни та більш сприятливих умов для розвитку науки? Можна діяти і так, втім, як ми вже зазначили сучасний стан української науки наразі сам по собі є загрозою національній безпеці держави. Наведемо лише деякі міркування. Зокрема, як і задовго до війни, серед проблем, що характеризують стан сфери науки: хронічне недофінансування; слабкі, а часом однобічні відносини в чотирикутнику: наука, бізнес, держава, громадянське суспільство; недосконаліть механізмів оцінювання наукових установ та відповідності їх бюджетного фінансування; невідповідність матеріально-технічної бази досліджень сучасним вимогам та рівню інформатизації, цифровізації суспільних відносин, використання штучного інтелекту; руйнування наукової інфраструктури; відтік висококваліфікованих кадрів, зокрема молодих науковців; фрагментарність інтеграції України до Європейського дослідницького простору, тощо.

На наше переконання, ефективна діяльність української науки є однією із вагомих складових національної безпеки, та одним з основних завдань держави, особливо в умовах війни як надзвичайного правового режиму, коли йдеться про захист національних інтересів, оборону країни, здобуття перемоги. Вирішення цих завдань потребує різного роду науково-обґрунтованих та виважених заходів та механізмів, винаходів, технологій та прогнозів.

Національна академія наук України, незважаючи на складні обставини воєнного часу, зберегла науковий потенціал, адаптувалась до нових реалій, продовжувала у 2024 р. активний науковий пошук і отримала чимало вагомих результатів у багатьох сучасних напрямах математики, інформатики, механіки і

машинознавства, фізики та астрономії, наук про Землю, матеріалознавства, енергетики та енергетичних технологій, хімії та біології, у галузі ядерних і радіаційних технологій [3, с. 5].

Серед вагомих результатів таких досліджень: інтелектуалізована система керування безпілотними літальними апаратами; матеріали, які можна використовувати для «склеювання» м'яких живих тканин; технологія створення біосумісних імплантів, здатних замінювати пошкоджену кісткову тканину; наукоємні елементи для військових систем слідкування та самонаведення та ін.

Установи суспільного та гуманітарного спрямування досліджували новітні воєнно-політичні фактори впливу на українське суспільство, засади формування національно укоріненої стійкості та безпеки економічного розвитку України. Велику увагу приділено розвінчанню ідеології агресора та пошуку шляхів протидії їй. Для державних органів підготовлено та надано 1820 експертних висновків до нормативно-правових актів і програмних документів, інформаційно-аналітичних матеріалів з різних питань соціально-економічного розвитку країни [3, с. 5].

Отже, наукова діяльність є однією із складових та чинників забезпечення національної безпеки в Україні, інтелектуальним ресурсом прогресивного суспільно-економічного та політичного розвитку, особливо в умовах війни, Зокрема йдеться про її вагому роль в сфері оборони, інформаційної безпеки, прогнозування тощо. Втім наразі гостро потребує додаткової уваги з боку держави, зокрема щодо фінансування, інституційної підтримки та інтеграції в європейський дослідницький простір.

Список використаних джерел

1. Храмов В.О. Безпека. Політологічний енциклопедичний словник/ упорядник В.П. Горбатенко; За ред. Ю.С. Шемшученка, В.Д. Бабкіна, В.П. Горбатенка. К: Генеза, 2004. С. 47.

2. Імплементація євроінтеграційних реформ у сфер науки й технологій. Доповідь Платформи громадянського суспільства Україна – ЄС. Доповідь Платформи громадянського суспільства Україна – ЄС.

3. Звіт про діяльність Національної академії наук України у 2024 році / НАН України. Київ: Академперіодика, 2025. 610 с.

Загуменна Юлія Олександрівна,
професор кафедри теорії та історії держави та права Харківського національного університету внутрішніх справ, доктор юридичних наук, доцент

ПРАВОВІ АСПЕКТИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ЯК ІНСТРУМЕНТУ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ У КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Трансформація характеру сучасних збройних конфліктів дедалі чіткіше демонструє пріоритетну роль інформаційного середовища як стратегічного простору впливу. У цьому контексті штучний інтелект (далі − ШІ) виступає не лише як інструмент технологічного розвитку, а й як потенційно небезпечний механізм, що здатний радикально змінити як засоби, так і масштаби інформаційного протиборства. Особливого значення ця проблема набуває в умовах збройної агресії проти України, де ШІ активно використовується для створення та поширення дезінформаційних продуктів, маніпуляції суспільною думкою, психологічного тиску, порушення цілісності кіберпростору [4, с. 282; 3, с. 2].

Аналіз останніх наукових досліджень та практики застосування ШІ в рамках гібридних воєн свідчить про формування нового кластеру правових загроз, які виникають на перетині інформаційного, кібернетичного та технологічного правопорядку. Зокрема, дослідники наголошують на невизначеності статусу та відповідальності розробників і користувачів автономних систем, відсутності чіткого правового режиму ШІ у межах чинного українського законодавства, а також на ризиках порушення прав людини та основоположних свобод у процесі обробки даних і моделювання поведінки громадян за допомогою алгоритмів [1, с. 249; 2, с. 108; 8, с. 133].

Водночас варто відзначити і значний нормативний вакуум у національному правовому полі, який унеможливлює ефективне регулювання використання ШІ в умовах інформаційної війни. На сьогодні у правовій доктрині України відсутні законодавчо визначені ключові поняття, пов’язані з використанням ШІ в інформаційному просторі, що створює складнощі у кваліфікації відповідних суспільно небезпечних діянь та притягненні до юридичної відповідальності [5, с. 1; 7, с. 35]. На міжнародному рівні ці питання поки що врегульовані фрагментарно, а інституційні ініціативи, такі як AI Act Європейського Союзу, перебувають на стадії імплементації [6, с. 22].

У світлі викладеного особливої актуальності набуває потреба в системному переосмисленні концептуального підходу до правового регулювання штучного інтелекту з урахуванням його потенціалу у сфері військових конфліктів та інформаційної безпеки.

Використання штучного інтелекту у сфері інформаційної війни супроводжується рядом фундаментальних викликів для правового порядку, насамперед з огляду на транснаціональний, автономний та високодинамічний

характер таких технологій. Проблематика правового регулювання полягає не стільки у відсутності загального контролю над технологією, скільки у тому, що традиційні форми правового регулювання не встигають за темпами її розвитку, що призводить до виникнення правових лакун, колізій і невизначеності щодо режиму правової відповідальності.

По-перше, слід акцентувати на відсутності в українському законодавстві чіткого та системного визначення правового статусу систем штучного інтелекту. Зокрема, не визначено, чи є така система об'єктом або суб'єктом права, що викликає труднощі при застосуванні норм цивільного, кримінального та інформаційного права у випадку заподіяння шкоди [1, с. 250; 3, с. 3]. Подібна ситуація створює правову невизначеність як для розробників, так і для користувачів технологій, унеможливлюючи застосування принципів юридичної відповідальності в умовах, коли штучний інтелект функціонує автономно.

По-друге, в нормативному полі відсутня категорія «інформаційна зброя» або «інформаційна атака», здійснена за допомогою ШІ. Це не дозволяє кваліфікувати такі дії як акти агресії або як посягання на національну безпеку, хоча вони можуть мати наслідки, еквівалентні впливу класичних збройних дій [4, с. 284; 5, с. 3].

По-третє, значні труднощі викликає відсутність диференціації між комерційним, військовим та терористичним використанням ШІ. Така правова невизначеність унеможливлює побудову ефективної моделі превентивного контролю та реагування, включаючи відповідні процедури сертифікації, ліцензування та моніторингу застосування штучного інтелекту в чутливих сферах [7, с. 38].

У підсумку актуальною постає необхідність формування цілісної нормативної моделі, що враховувала б особливості автономного функціонування ШІ, його роль в умовах воєнного конфлікту та потенціал у сфері деструктивного інформаційного впливу.

У контексті зростання ролі технологій штучного інтелекту на політичному та правовому рівнях останніми роками окреслилися тенденції до формування національних і наднаціональних регуляторних підходів, спрямованих на забезпечення прозорості, етичності та безпеки використання ШІ. В Україні наразі відсутній спеціальний закон, який би цілеспрямовано регламентував обіг та функціонування систем штучного інтелекту. Окремі аспекти порушуються у документах стратегічного характеру, таких як Концепція розвитку штучного інтелекту в Україні, затверджена наказом МОН № 155 від 2 лютого 2021 року, а також у Концепції забезпечення кібербезпеки України, однак ці документи не мають належного імперативного статусу і здебільшого формулюють рекомендаційні підходи.

Разом із тим Європейський Союз значно випередив національне правове поле, запропонувавши концепцію так званого AI Act − регламенту ЄС про штучний інтелект, ухваленого в 2024 році. Цей акт уперше класифікує системи ШІ за рівнем ризику (від «мінімального» до «неприйнятного») і передбачає спеціальні вимоги до високоризикових додатків, серед яких − використання у сфері критичної інфраструктури, правосуддя, громадського нагляду тощо.

Зокрема, у статтях 5-7 AI Act чітко забороняється використання ШІ для соціального скорингу, маніпулювання поведінкою громадян без їхньої згоди, а також для масового біометричного спостереження в публічному просторі, що прямо стосується інструментів інформаційної війни [6, с. 24].

Для України, яка прагне до правового наближення до acquis communautaire, вивчення досвіду ЄС у регулюванні ШІ є критично необхідним, оскільки дозволяє інтегрувати в національне право стандарти, що передбачають не лише запобігання зловживанням, а й підвищення довіри до технологій у сфері безпеки. Водночас такий підхід має враховувати реалії воєнного стану, що вимагає інституціоналізації спеціального органу контролю за впровадженням і застосуванням ШІ в чутливих сферах − зокрема, через механізми, подібні до діяльності Кіберцентру при РНБО чи СБУ [2, с. 111; 8, с. 135].

Розгортання сучасної інформаційної війни на тлі широкого впровадження технологій штучного інтелекту детермінує нову парадигму правових загроз, які суттєво відрізняються від традиційних викликів у сфері національної безпеки. ШІ, функціонуючи в автономному та адаптивному режимі, здатний стати високоефективним інструментом деструктивного впливу на інформаційний простір держави, зокрема через маніпуляцію суспільною думкою, розповсюдження дезінформації, руйнування довіри до державних інституцій, а також через уразливість до зовнішнього програмного втручання.

Національна правова система України, як і більшість світових юрисдикцій, на сьогодні не має цілісного правового механізму регламентації використання ШІ у воєнних чи гібридних конфліктах. Відсутність законодавчо визначених понять «штучний інтелект», «інформаційна зброя», «автономна система впливу» створює суттєві труднощі в частині кваліфікації правопорушень, притягнення до юридичної відповідальності та унеможливлює ефективне застосування превентивних і захисних заходів.

Оцінка європейського досвіду, зокрема концептуальних положень AI Act, дозволяє сформулювати ключові орієнтири для подальшого оновлення національного законодавства, серед яких особливо важливими є: ризик-орієнтований підхід до регулювання, створення спеціального органу контролю за обігом ШІ-технологій, запровадження нормативного режиму для високоризикових систем, а також кодифікація етичних стандартів та процедур сертифікації.

Таким чином, правове регулювання штучного інтелекту в умовах інформаційної війни має ґрунтуватися на принципах національної безпеки, техноетики, відповідальності та прозорості, при цьому інтегруючи міжнародні стандарти, адаптовані до реалій воєнного часу. Розробка відповідного спеціального законодавчого акту є стратегічно важливим кроком для захисту інформаційного суверенітету України та запобігання масштабному зловживанню технологіями нового покоління у сфері безпеки та оборони.

Список використаних джерел

1. Буряченко О. Сучасні виклики глобальної інформаційної безпеки. *Вісник Львівського університету.* Серія: Міжнародні відносини. 2024. № 55. С. 247–254.

2. Гуржій С.В. Організаційно-технічні та кримінально-правові основи протидії російським ботам в умовах війни. *Науковий вісник Міжнародного гуманітарного університету.* Серія: Юриспруденція. 2023. № 64. С. 108–114.

3. Каранфілова О.В. Складові державно-правового механізму інформаційної безпеки України в умовах воєнного стану. *Наукові записки Південноукраїнського національного педагогічного університету імені К. Д. Ушинського.* 2024. Вип. 1. С. 1–7.

4. Авдєєва Г.К. Системи штучного інтелекту як засоби протидії інформаційній війні в Україні. Національна безпека України: правові та організаційні механізми забезпечення : матеріали наук. конф., Харків, 2023 р. Харків : Ін-т вивчення проблем законності НАН України, 2023. С. 282–287.

5. Павленко Т.А. Технології ШІ у забезпеченні інформаційної безпеки України. Національна безпека України: правові та організаційні механізми забезпечення : матеріали наук. конф., Харків, 2023 р. Харків : Ін-т вивчення проблем законності НАН України, 2023. С. 133–138.

6. Ярошевська Т. Переваги та недоліки використання технологій ШІ в умовах війни та у післявоєнний час. *Вісник Дніпропетровського державного університету внутрішніх справ.* 2024. № 1. С. 22–28.

7. Радзієвська О.Г. Проблеми забезпечення інформаційних прав та безпеки людини в сучасних умовах. Збірник наукових праць кафедри інформаційної та кібернетичної безпеки КПІ. 2023. С. 35–41.

8. Скіцько О., Складанний П., Ширшов Р. Загрози та ризики використання штучного інтелекту в інформаційній війні. Кібербезпека: освіта, наука, техніка. 2023. № 2. С. 1–8.

Колодій Олексій Анатолійович,
доцент кафедри теорії, історії та філософії права Національної академії внутрішніх справ, доктор юридичних наук

ПРИНЦИПИ КОНСТИТУЦІЙНО-ПРАВОВОГО СТАТУСУ УКРАЇНСЬКОГО НАРОДУ

Беззаперечно, що для того щоб об’єктивно дослідити принципи конституційно-правового статусу Українського народу доцільно, насамперед, з’ясувати загальне розуміння принципів.

А тому зазначимо, що у більшості випадків стверджують, що «Принципи права – це такі відправні ідеї існування права, які виражають найважливіші закономірності і підвалини даного типу держави і права, є однопорядковими із сутністю права і становлять його головні риси, відрізняються універсальністю, вищою імперативністю і загальнозначимістю, відповідають об’єктивній необхідності побудови і зміцнення певного суспільного ладу. Принципи права спрямовують і надають синхронності усьому механізму правового регулювання

суспільних відносин, досконаліше інших розкривають місце права у суспільному житті і його розвитку» [1, с. 27].

Що ж стосується принципів конституційно-правового статусу Українського народу, або принципів статусів близьких до нього соціальних інституцій то, насамперед, хотілося б згадати дисертаційне дослідження Сало В.І. який вважає що принципами на підставі яких відбувається взаємодія Європейського Союзу і його членів є «… принципи наділення компетенцією, законності, субсибіарності, пропорційності та лояльної співпраці» [2, с. 17].

Панчишин А.В. у дослідженні «Правовий статус держави: теоретико-правовий аспект» обґрунтовує авторське визначення принципів правового статусу держави як «… вихідних, нормативно закріплених начал організації держави, що визначають напрями її функціонування, відображають сутність правового статусу держави та межі його поширення». Панчишин А.В. основними ознаками принципів правового статусу держави вважає те, що вони: обґрунтовуються вченими-юристами; мають форму ідей і положень, що є фундаментальними; відображають досягнення практичного досвіду держави, об'єктивні закономірності розвитку суспільства; є елементом юридичної політики; є частиною правової ідеології; мають інформаційний вплив; є критерієм ефективності та оцінки статусу держави; є засобом визначення меж правового статусу держави [3 с. 10]. Щоправда чомусь не називає які саме принципи він визнає принципами правового статусу держави.

Заяць Н.В. досліджуючи принципи народного представництва у виборчій системі України стверджує, що «Принципи народного представництва – це найбільш загальні, провідні, нормативно-регулятивні основні начала (ідеї), що відображають демократичну природу виборів як конституційної основи народовладдя й визначають фундамент правового регулювання виборчих прав, гарантій, процедур і технологій, що забезпечують імперативне, внутрішньо збалансоване й нефальсифіковане проведення виборів різних рівнів, демонструючи їх сутність і соціальне призначення. До принципів народного представництва, що пов'язані з конституційним механізмом формування виборних органів публічної влади, слід віднести такі принципи: народного суверенітету, усезагальності, рівності, безпосередності народного представництва, таємності волевиявлення під час формування органів народного представництва, добровільності участі у формуванні представницьких органів, періодичності та обов'язковості проведення виборів, свободи, гласності, істинності, законності та відповідальності механізму формування органів народного представництва» [4, с. 28].

Калиновський Б.В. формулює розуміння принципів місцевої публічної влади в Україні «… як обумовленої природою місцевого самоврядування та місцевої державної виконавчої влади системи основоположних, нормативно-правових, свідомо-вольових правил поведінки, які закріплені чи випливають зі змісту Конституції та законів України і визначають організацію та діяльність місцевих органів публічної влади щодо реалізації їхніх повноважень в інтересах держави та територіальних громад, демонструють сутність і соціальне призначення місцевої публічної влади в Україні» [5, с. 7]. Він вважає, що

найважливішими (основоположними) принципами місцевої публічної влади в Україні є принципи: «… народовладдя (демократизму); верховенства права та законності; соціальної справедливості; гласності; прозорості та відкритості; децентралізації; субсидіарності та пропорційності; поєднання місцевих і державних інтересів; узгодження загальнодержавних, регіональних і місцевих інтересів; адаптації делегованих повноважень до місцевих умов; фінансової, правової, організаційної та матеріальної автономії» [5, с. 26].

Засновуючись на вищезазначених визначеннях можна стверджувати, що сутність конституційно-правового статусу Українського народу, поряд із функціями, найповніше проявляється у його принципах як основоположних засадах щодо здійснення ним влади. Принципи опосередковують собою різноманітні властивості конституційно-правового статусу Українського народу, його ґенезу, ознаки, сутність, соціальне призначення, закономірності реалізації та подальший розвиток. Відповідно до змісту чинних Конституції та законодавства України загальними принципами конституційно-правового статусу Українського народу можна вважати: суверенність Українського народу; єдиновладдя Українського народу; повновладдя Українського народу; безпосереднього волевиявлення Українського народу; поєднання безпосередньої і представницької демократії; пріоритетності безпосередньої влади Українського народу в системі демократії; політичного плюралізму; конституційності й законності; загальності у здійсненні безпосередньої влади Українським народом; рівності у здійсненні безпосередньої влади Українським народом; реальності безпосередньої влади Українського народу; гарантованості безпосередньої влади Українського народу.

Список використаних джерел

1. Колодій А.М. Принципи права України: Монографія. Київ: Юрінком Інтер, 1998. 208 с.

2. Сало В.І. Внутрішні функції держави в умовах членства в Європейському Союзі : автореф. дис. на здобуття наук. ступеня кандидата юрид. наук: спец. 12.00.01 – теорія та історія держави і права; історія політичних і правових учень / Сало Володимир Ігорович. Харків, 2008. 20 с.

3. Панчишин А.В. Правовий статус держави : теоретико-правовий аспект : автореф. дис. на здобуття наук. ступеня кандидата юрид. наук: спец. 12.00.01 – теорія та історія держави і права; історія політичних і правових учень / Панчишин Антон Володимирович. Київ, 2014. 20 с.

4. Заяць Н.В. Народне представництво: сутність, суб’єкти та особливості здійснення в Україні : автореф. дис. на здобуття наук. ступеня доктора юрид. наук: спец. 12.00.02 – конституційне право; муніципальне право / Заяць Наталія Володимирівна. Київ, 2014. 38 с.

5. Калиновський Б.В. Місцева публічна влада в Україні: конституційно-правові засади функціонування та розвитку : автореф. дис. на здобуття наук. ступеня доктора юрид. наук: спец. 12.00.02 – конституційне право; муніципальне право / Калиновський Богдан Валерійович. Київ, 2017. 39 с. (с. 7).

Тихомиров Олександр Олександрович,
доцент кафедри інформаційної безпеки держави Національної академії Служби Безпеки України, доктор юридичних наук, доцент

СУЧАСНЕ РОЗУМІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ВИМІРИ ТА РІВНІ ЗАБЕЗПЕЧЕННЯ

Інформаційна еволюція людства й глибина його інтеграції з інформаційними технологіями вносить корективи в парадигму інформаційної безпеки. Інформаційна безпека поступово набуває значення сутнісної основи нормального життя в глобальному інформаційному суспільстві, стаючи своєрідним елементом його культури, базисом подальшого розвитку, особливим об'єктом для права.

На необхідність суттєвих змін у мисленні, світогляді, культурі людини в інформаційному суспільстві, або ж інформаційних трансформаціях картини світу, і, відповідно, розумінні безпеки, дедалі частіше звертають увагу українські вчені. Зокрема, О.В. Прудникова у своїх роботах пропонує філософський образ «людини інформаційної», культура якої є «найважливішим засобом відтворення світової культурної спільноти, створення світового інформаційного простору» [1], подібно «особистості майбутнього» в футурології Е. Тофлера (хвильова концепція). О.П. Дзьобань та Є.М. Мануйлов наголошують на одній з функцій інформаційної культури – «захист від інформаційного стресу, який багато в чому породжується дисбалансом між зростаючим потоком інформації і здатністю суб'єкта (людини, суспільства) до її обробки», а також відзначають безпосередню залежність культурних і безпекових проблем інформаційного суспільства: «…рівень інформаційної культури суб'єкта прямо пропорційний рівню інформаційної безпеки і, причому, що вище рівень інформаційної культури – то менше загроз останньої (тобто то вище рівень інформаційної безпеки) [2].

Водночас, формування уявлень і, далі, концепцій інформаційної безпеки у значній мірі залежить від осмисленості родового явища «безпека». Безпека є складним соціальним феноменом і може мати безліч пояснень, залежних від того чи іншого контексту, або тієї чи іншої галузі діяльності (науки), приміром:

– психологи визначають її як відчуття, сприйняття і переживання необхідності у захисті життєво важливих потреб і інтересів людини;

– юристи (правники) – як систему встановлених законом правових гарантій захищеності особи і суспільства, забезпечення їх нормальної життєдіяльності, прав і свобод;

– філософи – як стан, тенденції розвитку і умови життєдіяльності соціуму та його структур, за яких забезпечується збереження їх якісної визначеності та оптимальне співвідношення свободи і необхідності;

– політологи – як властивість (якість) системи і результат діяльності ряду систем і органів держави, а також сам процес діяльності, спрямованої на досягнення поставлених завдань щодо забезпечення захищеності особи, суспільства, держави.

Тому в сучасних умовах інформаційного розвитку інформаційна безпека набуває комплексного характеру і стає фундаментом існування глобального інформаційного суспільства. Її розуміння має поєднувати соціальні, технологічні, індивідуальні аспекти, включаючи відображення здатності усвідомлювати і задовольняти потреби в необхідній для життєдіяльності (функціонування) інформації. У межах такої соціотехнологічної (соціотехнічної) парадигми [3], серед змістових складових інформаційної безпеки сьогодні достатньо чітко проглядаються:

1) технологічна, яка визначається технічними, технологічними можливостями суб'єктів в інформаційній сфері та є рушійною силою інформаційних трансформацій;

2) правова, як упорядкованість, організованість суспільних інформаційних відносин, що зокрема охоплює нормування, організацію, управління різноманітними інформаційними процесами;

3) медіа, як комплексне відображення впливів суб'єкта (зокрема людини) на інформацію і інформації на суб'єкта в глобальному інформаційному просторі.

Ці три майже традиційні складові інформаційної безпеки на новій стадії інформатизації суспільного життя, яку називають інтелектуалізацією [4] (як в контексті розвитку ІТ, так і власне самої людини) мають логічно доповнюватися когнітивною складовою. Сучасна інформаційно залежна людина поступово перестає бути суто «споживачем інформації», а стає відповідальним користувачем і автором контенту в глобальному інформаційному просторі. Такі зміни зумовлюють розвиток аналітичних здібностей, які є фактичним виразом когнітивного аспекту інформаційної безпеки, зокрема як формування і задоволення потреби в необхідних для певної діяльності (насамперед, прийняття рішень) обсягах інформації та методах її інтерпретації. Як і в інших випадках цю нову складову інформаційної безпеки необхідно розглядати у зв'язку з життєдіяльністю певного суб'єкта, що зумовлює й відповідні напрями забезпечення.

Таким чином, сьогодні інформаційна безпека це складна характеристика певної соціальної системи чи підсистеми, зокрема людини, що відображає здатність до нормальної життєдіяльності (функціонування) й розвитку в певних умовах інформаційного середовища.

Як вже згадувалося, інформаційна безпека не розглядається безвідносно суб'єкта. У значній мірі вона буде результатами діяльності суб'єкта, про безпеку якого йдеться, та, водночас, тими умовами функціонування, що створюються цією діяльністю, а також здатностями до захисту і забезпечення стабільності, які набуваються і розвиваються в процесі цієї діяльності. Тобто, поєднання зазначених змістових складових інформаційної безпеки є універсальним і може розглядатися в різних масштабах (на різних рівнях) – людини, суспільства, держави, окремої організації.

Деталізація за кожною зі складових інформаційної безпеки можлива на різних рівнях – загальних умов, захисних механізмів, індивідуальних можливостей та спроможностей, наприклад таким чином.

1. Технологічна складова:

1) загальні умови:

– розвиток технологічної бази інформаційного простору;
– впровадження новітніх інформаційних (цифрових) технологій;

2) захисні механізми:

– захист інформації (технічний, програмний, криптографічний);
– забезпечення надійності і достатності систем обробки інформації;

3) індивідуальні можливості й спроможності:

– доступність Інтернету та інформаційних ресурсів;
– забезпеченість сучасними засобами обробки інформації;
– цифрова грамотність.

2. Правова складова:

1) загальні умови:

– законність і правопорядок в інформаційній сфері;
– упорядкованість важливих видів інформаційної діяльності;
– визнання і юридична визначеність інформаційних прав;
– формування правових засад створення і впровадження нових інформаційних технологій;

2) захисні механізми:

– заборони і юридична відповідальність у сфері інформаційних правовідносин;
– порядок захисту певних категорій інформації, зокрема інформації з обмеженим доступом;
– порядок використання спеціальних засобів отримання інформації;
– окремі механізми захисту і відновлення інформаційних прав;

3) індивідуальні можливості і спроможності:

– правова культура і правосвідомість, інформаційно-правова культура;
– здатності адекватного сприйняття правової інформації;
– орієнтованість на захист власних інформаційних прав.

3. Медіа складова:

1) загальні умови:

– доступність, багатоманітність, альтернативність медіа та свобода слова;
– популяризація національного інформаційного продукту;
– збереження національної ідентичності і національної культури;
– позитивний імідж суспільства і держави на міжнародній арені;

2) захисні механізми:

– державне регулювання і контроль у сфері медіа;
– захист від маніпуляцій і дезінформації;
– обмеження щодо змісту інформації;
– заходи інформаційної гігієни;

3) індивідуальні можливості і спроможності:

– сформованість інформаційних потреб та культура інформаційних обмінів;

– здатності критичного ставлення до інформації та її джерел;

– медіаграмотність.

Наведений розподіл і деталізація є умовними і лише певною мірою моделюють компонентний склад інформаційної безпеки в межах комплексної парадигми, що також слугує відображенням системи сучасних напрямів і пріоритетів забезпечення інформаційної безпеки.

Описана вище інтеграція діяльнісного та соціотехнічного підходів у розумінні інформаційної безпеки, по-перше, орієнтує на ідеї взаємодії і взаємозалежності людини та інформаційних процесів сьогодні та в перспективі, а по-друге, дає змогу охопити основні наявні напрями визначення інформаційної безпеки, зокрема як управління загрозами, як системи захисних заходів, як захищеності, як умов функціонування (життєдіяльності) та здатностей суб'єктів в інформаційному середовищі, оскільки всі вони інтерпретуються через ті чи інші змістові компоненти діяльності.

Список використаних джерел

1. Прудніков О.В. Інформаційна культура: концептуальні засади та світоглядний сенс: монографія. Харків: Право. 2015. 352 с.

2. Дзьобань О.П., Мануйлов Є.М. Інформаційна безпека в контексті інформаційної культури. *Інформація і право.* 2017. № 1(20). С. 74−81.

3. Тихомиров О.О. Інформаційна безпека: соціотехнічна парадигма. *Інформаційна безпека людини, суспільства, держави.* 2014. №1. С. 13−20.

4. Бєляков К.І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення : монографія. Київ : КВІЦ, 2008. С. 37–38.

Бразалук Максиміліан Юрійович, *провідний фахівець відділення соціально-гуманітарної роботи та національно-патріотичного виховання відділу соціально-гуманітарної роботи Національної академії внутрішніх справ*

ВПЛИВ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ НА МОРАЛЬНО-ПСИХОЛОГІЧНИЙ СТАН ВІЙСЬКОВОСЛУЖБОВЦІВ ТА ЦИВІЛЬНИХ ОСІБ У КІБЕРПРОСТОРІ

Складні військово-політичні процеси, з якими щодня стикається наша країна та громадяни, породжують велику кількість проблем, як-то: демографічні, економічні, соціальні, криміногенні, правові, культурні, інформаційні тощо. У своїй сукупності вони утворюють цілу низку викликів як для держави, так і для

всього українського народу, який щодня мужньо дає відсіч збройній агресії російській федерації.

З початку повномасштабного вторгнення як українські захисники та захисниці, так і цивільні громадяни піддаються інформаційно-пропагандистському впливу російської федерації. Існує стала тенденція до підвищення технічного рівня реалізації кіберзагроз із боку ворога, вдосконалення та розробки ним нових інструментів кібератак. Як наслідок посилюється розвідувально-підривна діяльність ворога у кіберпросторі з метою поширення кібервпливу на мирне населення України і зокрема на тих, які брали участь в бойових діях і тих, хто став свідком психотравмуючих подій, пов'язаних з бойовими діями. Специфіка психологічного супроводження таких осіб повинна враховувати ступінь інтеграції зазначених осіб у кіберпростір, а також те, що посттравматична реабілітація та соціалізація відбувається зокрема й у вимірі кіберпростору.

Варто зазначити, що інтеграція суспільства у кіберпростір надає для суспільства значні переваги, втім, ця інтеграція напряму пов'язана з використанням інформації та мереж, пов'язаних із цією інформацією, що в свою чергу може спричинити втрату конфіденційності, цілісності та доступності інформації. Тому існує об'єктивна необхідність у надійному захисті мереж та інформаційних систем, пов'язаних із ними [1, с. 88].

Згідно зі Стратегією кібербезпеки України на 2021-2025 роки, російська федерація є одним із основних джерел загроз національній та міжнародній безпеці, яка активно реалізує концепцію інформаційного протиборства. Ця концепція базується на поєднанні деструктивних дій у кіберпросторі разом з інформаційно-психологічними операціями. В свою чергу деструктивна активність створює загрози вчинення актів кібертероризму та кібердиверсій щодо національної інформаційної інфраструктури. Як елемент спеціальних інформаційних операцій ворогом використовуються також кібератаки [2].

Ці дії підпадають під концепцію гібридної війни, яка полягає в створенні державою-агресором внутрішніх протиріч та конфліктів із поєднанням злочинної поведінки та застосуванням конвенційної війни з подальшим їх використанням для досягнення політичних цілей агресії, які зазвичай досягаються за допомогою лише конвенційної війни [3, с. 131]. Інформаційно-психологічний вплив є одним із найважливіших складових гібридної війни.

У Польовому статуті FM 33-1 Міністерства оборони США є дефініція інформаційної операції. Так, інформаційні операції – це попередньо сплановані психологічні дії в мирний і військовий час, спрямовані проти ворожої, дружньої або нейтральної аудиторії шляхом впливу на настанови та поведінку з метою досягнення політичних та військових переваг. Вони включають в себе психологічні дії зі стратегічними цілями, психологічні консолідуючі дії та психологічні дії з безпосередньої підтримки бойових дій [4, с. 122].

За допомогою інформаційно-психологічних операцій нарощується соціально-економічний хаос всередині країни-противника, посилюється психологічний та інформаційний тиск на населення та вище політичне керівництво країни-об'єкта агресії. Оскільки об'єктом інформаційно-

психологічного впливу є свідомість людини, то механізми такого впливу враховують особливості людської свідомості. Так, наприклад, людська свідомість сконцентрована на сприйняття лише найближчих наслідків якоїсь події, не враховуючи її довгострокові перспективи розвитку. Коли певні події спершу здаються позитивними, потім вони призводять до здійснення поставленої деструктивної мети, при цьому мінімізуючи затрати. Для цього противником може використовуватись фальсифікована інформація, дезорієнтуюча інформація, деморалізуюча інформація, дезорганізуюча інформація тощо [5, с. 3,5].

Таким чином, політика держави у сфері забезпечення безпеки в кіберпросторі в умовах воєнного стану повинна враховувати ризики втручання в кіберпростір держави-ворога та напрацьовувати механізми протидії цьому втручанню, оскільки інформаційно-психологічні операції спрямовуються як на військовослужбовців, так і на цивільне населення, зокрема і на тих, хто звільнений з військової служби, отримав бойове поранення або проходить реабілітацію. Обов'язково слід напрацьовувати методичні рекомендації щодо комунікації з цивільним населенням з приводу відокремлення правдивої інформації від дезінформації, тому применшення інтенсивності інформування суспільства про роль ворожих інформаційно-психологічних операцій та кібератак сприятиме подальшому розгортанню розвідувально-підривної діяльності російської федерації у кіберпросторі та поширенню кібервпливу на населення України і погіршенню морально-психологічного стану як військовослужбовців, так і цивільних осіб.

З урахуванням ведення гібридної війни проти нашої держави негативні наслідки можуть проявлятись як у військово-політичній сфері, так і в суспільстві, тому державна політика у сфері кібербезпеки має бути спрямована на надійний захист мереж та інформаційних систем, пов'язаних із ними для протидії, припинення та запобігання впливу інформаційно-психологічних операцій з боку ворога.

Список використаних джерел

1. Толкачов М.Ю. Механізми захисту трафіку в кіберпросторі. Сучасний захист інформації, 4(60), 2024. 85–99: вебсайт. URL: https://doi.org/10.31673/2409-7292.2024.040009.

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

3. Грушко М.В. Міжнародне гуманітарне право: навчально-методичний посібник / за ред. О.В. Бігняка. Одеса : Видавничий дім «Гельветика», 2022. 136 с.

4. Проноза І., Сурова М. Інформаційні (психологічні) операції як інструмент інформаційної війни. С. 121 – 123. Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи *:* IV міжнар.

наук.-практ. конф., 27 верес. 2023 р.: тези доповідей / Міністерство оборони України, НУОУ. К.: НУОУ, 2023. 406 с.

5. Кислий В.Д., Прокопенко Д.С. Інформаційно-психологічний вплив на військовослужбовців. Інформаційна агресія Російської Федерації проти України: Науковий семінар ХНУ ПС ім. І.Кожедуба, 21 жовтня 2020 : вебсайт. URL: https://hups.mil.gov.ua/assets/doc/science/stud-conf/suchasna-vijna-gumanitarnij-aspekt-21-10-2020/8.pdf.

Білозьоров Євген Вікторович,
завідувач відділення організаційно-аналітичного забезпечення навчально-наукового експертно-криміналістичного інституту Національної академії внутрішніх справ, кандидат юридичних наук, доцент

ІНСТИТУЦІЙНИЙ АСПЕКТ МЕХАНІЗМУ ОБОРОННОЇ ФУНКЦІЇ СУЧАСНОЇ ДЕРЖАВИ: ДІЯЛЬНІСНИЙ ВИМІР

Стратегічний вектор України на здобуття повноправного членства в Організації Північноатлантичного договору (НАТО), закріплений у Конституції України, отримав конкретне відображення у Стратегії національної безпеки України [1] та Стратегії воєнної безпеки [2]. З метою поглиблення особливого партнерства з НАТО та поступового входження до його складу, держава визначила пріоритетом досягнення у найкоротші терміни належного рівня взаємосумісності між Збройними Силами України, іншими складовими сектору безпеки й оборони та відповідними структурами країн-членів Альянсу. Особлива увага при цьому приділяється інтенсифікації реформ у межах імплементації річних національних програм під егідою Комісії Україна – НАТО.

Актуальність цих завдань значно посилилася в умовах ескалації військового, економічного, енергетичного та політичного протистояння, спричиненого агресивною політикою російської федерації. Новий етап збройного конфлікту між Україною та росією розпочався 24 лютого 2022 року повномасштабним вторгненням, яке стало логічним продовженням збройної агресії, що триває з 2014 року. В таких умовах Україна обстоює свій цивілізаційний вибір, інтеграцію в європейське співтовариство та домінування прав людини як засадничого принципу демократичного ладу.

Метою цієї наукової розвідки є здійснення методологічної характеристики інституційного елементу механізму реалізації оборонної функції сучасної держави в умовах її протидії зовнішнім і внутрішнім загрозам через призму діяльнісного аспекту.

На основі аналізу наукових джерел, які досліджують окремі аспекти оборонної діяльності держави, доцільно визначити, що термін «оборона» охоплює сукупність політичних, економічних, екологічних, військових, соціальних та правових заходів, спрямованих на забезпечення незалежності, територіальної цілісності, захисту національних інтересів і безпеки громадян України [3, с. 468]. На думку В. Б. Авер'янова, поняття «оборона України» включає систему суспільних відносин, що виникають у процесі забезпечення здатності держави до збройного захисту у разі виникнення загрози чи безпосередньої агресії. Ця діяльність охоплює як застосування Збройних Сил України, так і виконання міжнародних зобов'язань у сфері безпеки [4, с. 366].

Цікавою є також позиція В.В. Сокуренка, відповідно до якої оборона держави є видом державної діяльності, спрямованої на збройний захист її цілісності, недоторканності кордонів та протидії зовнішнім і внутрішнім загрозам. Оборона виконує ключову роль у забезпеченні національного суверенітету та охоплює широкий спектр організаційних, економічних, соціальних, правових і науково-технічних заходів [5, с. 165].

Відповідно до Закону України «Про оборону України», оборона визначається як система заходів політичного, економічного, соціального, військового, наукового, правового та організаційного характеру, спрямованих на підготовку до збройного захисту держави, а також здійснення такого захисту в разі виникнення загроз [6].

Таким чином, реалізація оборонної функції держави передбачає наявність ефективного інституційного забезпечення, що охоплює спеціалізовані органи й установи, уповноважені діяти на професійній основі згідно з чинним законодавством. При цьому важливо підкреслити, що громадяни не усуваються від процесу захисту держави: навпаки, активне залучення населення до оборонної діяльності є одним із ключових напрямів державної політики. Так, відповідно до Закону України «Про основи національного спротиву» [7], національний спротив визначається як комплекс заходів, що організовуються з метою сприяння обороні України через активну участь громадян у забезпеченні військової безпеки, стримуванні та відсічі агресії.

У цьому контексті особливу увагу слід приділити інституційному елементу механізму оборонної функції, до якого належать суб'єкти, наділені правом і обов'язком здійснювати професійну оборонну діяльність у межах законодавчих повноважень. Для уніфікації правового регулювання таких суб'єктів у законодавстві України використовується термін «сектор безпеки і оборони», який, згідно із Законом України «Про національну безпеку України» [8], охоплює систему органів державної влади, Збройних Сил України, інших військових формувань, правоохоронних та розвідувальних органів, а також суб'єктів цивільного захисту, оборонно-промислового комплексу та громадських об'єднань, які залучені до забезпечення безпеки на добровільних засадах.

Згідно з чинним законодавством України структура сектору безпеки і оборони включає в себе компоненти, які розмежовуються відповідно до свого функціонального призначення та юридичної природи. Зокрема, сектор безпеки і оборони України складається із елементів: 1) сили безпеки та оборони; 2) оборонно-промисловий комплекс; 3) громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки. Необхідно звернути увагу й на те, що інституційно складові сектору безпеки та оборони України належать як до державного апарату, так і до інститутів громадянського суспільства [9, с. 79].

Важливе місце в структурі механізму здійснення оборонної функції держави як інституційного (організаційного) елементу належить Національній гвардії України, яка має правовий статус військового формування з правоохоронними функціями, що входить до системи Міністерства внутрішніх справ України. Відповідно до Закону України «Про національну гвардію України» [10], зазначене військове формування призначено для виконання завдань із захисту та охорони життя, прав, свобод і законних інтересів громадян, суспільства і держави від кримінальних та інших протиправних посягань, охорони громадської безпеки і порядку та забезпечення громадської безпеки, а також у взаємодії з правоохоронними органами – із забезпечення державної безпеки і захисту державного кордону, припинення терористичної діяльності, діяльності незаконних воєнізованих або збройних формувань (груп), терористичних організацій, організованих груп та злочинних організацій.

У межах здійснення оборонної функції певна роль належить Державній прикордонній службі України, яка відповідно до ст. 1 Закону України «Про Державну прикордонну службу України» [11] здійснює завдання щодо забезпечення недоторканності державного кордону та охорони суверенних прав України в її прилеглій зоні та виключній (морській) економічній зоні. До того ж, вона може брати участь у боротьбі з організованою злочинністю та здійснювати протидію незаконній міграції на державному кордоні України та в межах контрольованих прикордонних районів.

З огляду на те, що Державна прикордонна служба України входить до єдиної структури сектору безпеки і оборони України, на неї покладається завдання із координації діяльності військових формувань та відповідних правоохоронних органів, пов'язаної із захистом державного кордону України та пропуску до тимчасово окупованої території і з неї, а також діяльності державних органів, що здійснюють різні види контролю при перетинанні державного кордону України та пропуску до тимчасово окупованої території і з неї або беруть участь у забезпеченні режиму державного кордону, прикордонного режиму і режиму в пунктах пропуску через державний кордон України та в контрольних пунктах в'їзду – виїзду [11].

Окрім зазначених інституцій, інші органи, які входять до сектору безпеки і оборони, також здійснюють систему важливих функцій, які відповідають сутності оборонної діяльності держави в сучасних умовах.

Таким чином, можна виокремити, що дослідження інституційного елемента механізму оборонної функції сучасної держави через призму діяльнісного підходу має не тільки теоретичне, а й безпосередньо практичне значення, оскільки спрямоване на формування суб'єктів оборонної діяльності, їх цілей та завдань, механізмів захисту національних інтересів України та є основою для планування і реалізації державної політики у сфері національної безпеки та оборони.

Список використаних джерел

1. Указ Президента України від 14 вересня 2020 р. №392/2020 «Про Стратегію національної безпеки України». URL : https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 26.05.2025).
2. Указ Президента України від 25 березня 2021 р. № 121/2021 «Про Стратегію воєнної безпеки України». URL : https://www.president.gov.ua/documents/1212021-37661 (дата звернення: 26.05.2025).
3. Адміністративне право України : підруч. / В.М. Гаращук та ін. / За ред. Ю.П. Битяка. Київ : ЮрінкомІнтер, 2006. 544 с.
4. Адміністративне право України. Академ. курс : підруч. у 2 т. Т. 2 Особлива частина / ред. кол. В.Б. Авер'янов (голова) та ін. Київ. : Юрид. думка. 2005. 624 с.
5. Сокуренко В. Оборона як ефективний засіб забезпечення безпеки суспільства та держави. *Підприємництво, господарство і право.* 2017. № 2. С. 159-166.
6. Закон України «Про оборону України» від 05 грудня 1991 р. № 1932-XII. URL : https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 26.05.2025).
7. Закон України «Про основи національного спротиву» від 16 липня 2021 р. № 1702-IX. URL : https://zakon.rada.gov.ua/laws/show/1702-20#Text (дата звернення: 26.05.2025).
8. Закон України «Про національну безпеку України» від 21 червня 2018 р. № 2469-VIII. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 26.05.2025).
9. Александров В.М. Сектор безпеки і оборони України в механізмі реалізації оборонної функції держави. *Часопис Київського університету права.* 2020. № 4. С. 78-82.
10. Закон України «Про національну гвардію України» від 13 березня 2014 р. № 876-VII. URL : https://zakon.rada.gov.ua/laws/show/876-18#Text (дата звернення: 26.05.2025).
11. Закон України «Про Державну прикордонну службу України» від 03 квітня 2003 р. № 661-IV. URL : https://zakon.rada.gov.ua/laws/show/661-15#Text (дата звернення: 26.05.2025).

Власенко Валерій Павлович,
доцент кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат юридичних наук, доцент
Дейнеко Анастасія Ігорівна,
курсант навально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ

ПРАВОВІ МЕХАНІЗМИ ПРИТЯГНЕННЯ КРАЇНИ-АГРЕСОРА ДО ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ

З початком широкомасштабної збройної агресії російської федерації (рф) проти України у лютому 2022 року міжнародна спільнота постала перед викликом формування дієвого правового механізму, здатного не лише фіксувати порушення міжнародного права, але й ефективно притягувати державу-агресора до відповідальності.

Механізми міжнародної відповідальності держави за агресію є складними та багаторівневими, що охоплюють політичні інструменти (санкції, дипломатичний тиск, сатисфакція), судові процедури (провадження у міжнародних та національних судах), економічні заходи (реституція, компенсація), а також створення спеціалізованих органів, таких як міжнародні компенсаційні комісії чи фонди. З огляду на масштаби руйнувань та обсяг завданої шкоди, Україні необхідно реалізувати комплексний підхід до формування системи відшкодування, що базуватиметься на міжнародно-правових нормах, прецедентах і вже існуючих механізмах.

Відповідальність держави за міжнародне правопорушення є однією з базових категорій міжнародного публічного права. Її принципи кодифіковані в Статтях про відповідальність держав за міжнародно-протиправні діяння, ухвалених Комісією міжнародного права ООН у 2001 році. Цей документ закріплює обов’язок держави, яка вчинила міжнародне правопорушення, надати повне відшкодування за завдану шкоду [1, с. 244].

Російська агресія супроводжується численними фактами порушення норм міжнародного гуманітарного права та прав людини. Це, зокрема, знищення цивільної інфраструктури, катування, вбивства, примусове переміщення населення, незаконне утримання цивільних осіб, депортація дітей. З огляду на це, відповідальність рф повинна включати не лише політичне засудження, але й конкретні юридичні наслідки: відшкодування, реституцію, сатисфакцію, покарання конкретних осіб тощо.

У цьому контексті важливим є звернення України до Міжнародного Суду ООН з позовом проти РФ, а також підтримка Генеральної Асамблеї ООН, яка у Резолюції A/RES/ES-11/5 закликала створити міжнародний механізм компенсацій для України [2].

Репарації є історично усталеною формою відповідальності агресора за заподіяну шкоду. У сучасному міжнародному праві вони набули вигляду фінансових компенсацій, повернення незаконно вивезеного майна, проведення заходів щодо реабілітації постраждалих. Механізм репарацій застосовувався в різних історичних контекстах – наприклад, до Німеччини після Першої та Другої світових воєн, до Іраку після агресії проти Кувейту у 1990 році. У випадку Іраку діяв спеціальний Компенсаційний фонд ООН, наповнюваний за рахунок доходів від експорту нафти. Цей досвід може бути використаний для України, з урахуванням заморожених російських активів [3, с. 1039-1040].

Однак, як показує практика, реалізація таких механізмів потребує створення міжнародно визнаного органу (трибуналу, фонду), який би не лише реєстрував заяви про шкоду, а й розподіляв компенсації. Одним із інструментів забезпечення компенсацій є конфіскація заморожених активів, що перебувають за кордоном. Після 2022 року низка країн (США, Канада, країни ЄС) заморозили чимало державних активів росії. За даними російського центробанку, 7 країн-учасниць, які запровадили санкції проти, станом на червень 2021 року володіли майже половиною всіх російських валютних резервів у розмірі $585 млрд. Відтоді російські резерви (заморожені) за кордоном зросли до $640 млрд. [4].

Значна частина зусиль України щодо притягнення російської федерації до відповідальності за агресію, військові злочини та порушення прав людини сконцентрована у площині міжнародного судочинства. Передусім ідеться про такі інститути, як Міжнародний Суд ООН, Європейський суд з прав людини (ЄСПЛ) та Міжнародний кримінальний суд (МКС).

ЄСПЛ, незважаючи на вихід рф з Ради Європи, продовжує розгляд скарг України проти росії, об’єднаних у великі міждержавні справи. Основні обвинувачення стосуються порушень права на життя, заборони тортур, права на свободу та безпеку, власність, свободу пересування тощо. Враховуючи те, що на момент вчинення злочинів росія була учасницею Конвенції про захист прав людини і основоположних свобод, юрисдикція ЄСПЛ залишається чинною щодо вчинених правопорушень до 16 вересня 2022 року включно [5, с. 740].

МКС відіграє ключову роль у переслідуванні винних у воєнних злочинах, злочинах проти людяності, геноциді. В березні 2023 року МКС видав ордер на арешт Володимира Путіна та уповноваженої з прав дитини Марії Львової-Бєлової за незаконну депортацію українських дітей. Це рішення стало значущим кроком до персональної відповідальності вищого керівництва країни-агресора [6].

В умовах обмеженості традиційних міжнародних юрисдикцій Україна ініціювала створення спеціального міжнародного трибуналу щодо злочину агресії. Правовою основою такого трибуналу може бути міжнародний договір між державами-партнерами, або відповідна резолюція Генеральної Асамблеї ООН. Зокрема, така ініціатива була підтримана в Європарламенті, а Єврокомісія розглядає можливість долучення до створення відповідного органу [7, с. 57].

Паралельно з судовими механізмами важливе місце посідають позасудові інструменти відповідальності, серед яких:

– створення Міжнародного компенсаційного реєстру збитків, що фіксує факти матеріальної та моральної шкоди, заподіяної внаслідок агресії;

– діяльність громадських організацій (наприклад, EyeWitness to Atrocities чи Truth Hounds та ін.), які документують воєнні злочини за міжнародними стандартами;

– формування коаліцій на базі групи G7, НАТО, ЄС, які допомагають розробити єдиний підхід до конфіскації активів рф і спрямування їх у фонд відбудови України [8].

Таким чином, ефективність захисту інтересів України у війні з росією залежить від поєднання зусиль у сфері як судового переслідування, так і організації міжнародного правового механізму репарацій.

На сучасному етапі міжнародна правова система постала перед безпрецедентним викликом – забезпеченням дієвої відповідальності ядерної держави, постійного члена Ради Безпеки ООН, за збройну агресію. Агресія рф проти України призвела до численних порушень міжнародного гуманітарного права, прав людини та спричинила величезні матеріальні втрати і людські жертви. У цьому контексті важливим є створення комплексного правового механізму, який включає:

– судові провадження в межах Міжнародного Суду ООН, МКС, ЄСПЛ;

– політичні рішення Генеральної Асамблеї ООН щодо формування компенсаційного механізму;

– санкційні заходи та конфіскацію активів країни-агресора для формування фонду відбудови України;

– створення спеціального міжнародного трибуналу щодо злочину агресії;

– фіксація шкоди та документування воєнних злочинів для майбутніх компенсаційних процедур.

Список використаних джерел

1. Грабович Т.А. Статті про відповідальність держав за міжнародно-протиправні діяння (2001): основа сучасного права міжнародної відповідальності. Науковий вісник публічного та приватного права. Випуск 4. 2020. С. 240-245

2. Резолюція Генеральної Асамблеї ООН A/RES/ES-11/5 «Сприяння механізмам репарацій Україні» від 14.11.2022. URL: https://docs.un.org/en/A/RES/ES-11/5

3. Рашевська К.Є. Моделі та механізми виплати репарацій: міжнародний досвід та ідеї для України. Baltic Journal of Economic Studies. 2022 С.1032-1041

4. Наталія С., Павло Д., Катерина Р. Конфіскація російських активів: юридичні, правозахисні та політичні обмеження. Transparency International Ukraine. URL: https://ti-ukraine.org/research/konfiskatsiya-rosijskyh-aktyviv-yurydychni-pravozahysni-ta-politychni-obmezhennya/?fbclid=IwZXh0bgNhZW0CMTAAAR0IDr4BsQC5HLrzKsDWLkQXl8vAisTpb_Vkg4cQxlLTFxHq4cIKC-93lYo_aem_Ad5DZ0SKve674Zmr8s3klos6ng7XNVxKsHeQS8qlErEAKa--of5Ue2C38yOw9QyHzzteC0zxrAJoOHarvzoYOjCV

5. Тітко Е.В., Білоусова К.В. Особливості захисту прав людини в практиці ЄСПЛ проти РФ в умовах збройного конфлікту. *Юридичний науковий електронний журнал.* 2023. № 4. С. 739-742. URL : http://www.lsej.org.ua/4_2023/179.pdf

6. Міжнародний кримінальний суд (МКС) в Гаазі видав ордери на арешт президента Росії Володимира Путіна та уповноважену при президенті з прав дитини Марії Львової-Бєлової. Стаття від 17 бер. 2023 р. Прес-служба Апарату Верховної Ради України. Опубліковано 17 березня 2025. URL : https://www.rada.gov.ua/news/news_kom/259864.html

7. Андрій Єрмак і Роберта Мецола закликали підтримати створення міжнародного трибуналу для політичного керівництва Росії. Офіційне інтернет-представництво Президента України. 2022. URL: https://www.president.gov.ua/news/andrij-yermak-i-roberta-mecola-zaklikali-pidtrimati-stvorenn-77529

8. Комітет з прав людини інформує про платформи фіксації та розслідування злочинів РФ проти цивільного населення України. Інформаційне управління. 2022. URL: https://www.rada.gov.ua/print/222106.html

Власенко Валерій Павлович,
доцент кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат юридичних наук, доцент
Хуторян Марія Віталіївна,
курсант навально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ

ЗАХИСТ КУЛЬТУРНОЇ СПАДЩИНИ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ: НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО ТА МІЖНАРОДНІ ЗОБОВ'ЯЗАННЯ

Культурна спадщина – це важлива складова ідентичності народу, духовного самовираження та соціальної згуртованості. Тобто в такому розумінні культурна спадщина є ментальною складовою народу. Якщо культурну спадщину розуміти як сукупність успадкованих людством від попередніх поколінь об'єктів культурної спадщини, то в такій інтерпретації до уваги береться матеріальна складова культури народу. В такому сенсі та в сучасних безпекових умовах захист української культурної спадщини є викликом для міжнародного права, національного законодавства та гуманітарної політики [1].

Нормативне визначення поняття «об'єкт культурної спадщини» законодавцем тлумачиться як визначне місце, споруда (витвір), комплекс (ансамбль), їхні частини, пов'язані з ними рухомі предмети, а також території чи

водні об’єкти (об’єкти підводної культурної та археологічної спадщини), інші природні, природно-антропогенні або створені людиною об’єкти незалежно від стану збереженості, що донесли до нашого часу цінність з археологічного, естетичного, етнологічного, історичного, архітектурного, мистецького, наукового чи художнього погляду і зберегли свою автентичність [2]. Відповідно до Гаазької Конвенції 1954 року про захист культурних цінностей у випадку збройного конфлікту, до речі Україна є стороною цієї Конвенції, Високі Договірні Сторони зобов’язуються підготувати ще в мирний час охорону культурних цінностей, розташованих на їх території, від можливих наслідків збройного конфлікту, вживаючи заходів, які вони вважають необхідними.

Питання захисту культурних цінностей відображаються і в наступних міжнародно-правових актах, таких як:

- Протоколи до Конвенції (перший протокол (1954) забороняє вивезення культурних цінностей з окупованих територій, другий протокол (1999) вводить категорію «покращений захист», встановлює кримінальну відповідальність за істотні порушення);

- Конвенція про охорону всесвітньої культурної і природної спадщини 1972 року зобов’язує держави – сторони цієї Конвенції забезпечувати якомога ефективнішу охорону і збереження та якомога активнішу популяризацію культурної і природної спадщини, розміщеної на її території, шляхом політики надання такій спадщині певних функцій у громадському житті, створення однієї чи кілька служб з охорони, збереження й популяризації культурної й природної спадщини, розвитку наукового й технічного опрацювання методів роботи, які дають змогу державі усувати небезпеку, що загрожує її культурній та природній спадщині тощо. Наприклад, у лютому 2022 року Україна звернулася до ЮНЕСКО із закликом надати захист для 7 об’єктів, які перебувають під загрозою знищення, зокрема Софійський собор у Києві, історичний центр Львова**,** центр Одеси;

- Римський статут Міжнародного кримінального суду, який визначає знищення культурних об’єктів як воєнний злочин (працівниками Офісу Генерального прокурора станом на початок 2024 року зафіксовано та передано до Міжнародного кримінального суду понад 900 фактів знищення або пошкодження об’єктів культурної спадщини, зокрема знищення Художнього музею ім. Бродського у Маріуполі, пошкодження Палацу Потоцьких у Херсоні, руйнування старовинних церков на Чернігівщині та Харківщині) [3; 4].

В умовах війни значна кількість злочинів рф направлена проти музеїв та музейних колекцій, які є концентрованим уособленням культурної спадщини України. При цьому, втрат зазнають як музеї державної форми власності, так і комунальної та приватної. Задокументовано відповідні факти привласнення та розграбування щонайменше у 12 музеях, серед яких: Маріупольський краєзнавчий музей, Художній музей імені А.І. Куїнджі у м. Маріуполі, Донецький обласний краєзнавчий музей, Мелітопольський міський краєзнавчий музей, Картинна галерея імені Альбіна Гавдзинського та ін. [4].

Безпосередньо в Україні захист культурних цінностей в разі збройної агресії регулюється, у першу чергу, міжнародними договорами ратифікованими

Україною, які у відповідності до ст. 9 Конституції України, є частиною українського законодавства [5].

Відповідно до ст. 27 Закону України «Про охорону культурної спадщини» у разі, коли пам'ятці загрожує небезпека пошкодження, руйнування чи знищення, власник або уповноважений ним орган, особа, яка набула права володіння, користування чи управління, зобов'язані привести цю пам'ятку до належного стану (змінити вид або спосіб її використання, провести роботи з її консервації, реставрації, реабілітації, музеєфікації, ремонту та пристосування) [2; 6].

Закон України від 15.04.2014 № 1207-VII «Про забезпечення прав і свобод громадян та правовий режим на тимчасово окупованій території України» визначає, що відповідальність за охорону культурної спадщини на тимчасово окупованій території покладено на рф як на державу, що здійснює окупацію, відповідно до норм і принципів міжнародного права, а питання повернення культурних цінностей врегульоване Законом України від 21.09.1999 № 1068-XIV «Про вивезення, ввезення та повернення культурних цінностей».

Система охорони культурної спадщини в Україні визначена також у постановах Кабінету Міністрів України від 22.05.2019 № 452 «Про затвердження Порядку визначення категорій пам'яток», від 30.10.2013 № 841 «Про затвердження Порядку проведення евакуації у разі загрози виникнення або виникнення надзвичайних ситуацій»; наказах Міністерства Культури України від 11.03.2013 № 158 «Про затвердження Порядку обліку об'єктів культурної спадщини» та від 10.07.2017 № 579 «Про затвердження Методики планування заходів з евакуації» [1; 7].

Відповідальність за умисне незаконне знищення, руйнування або пошкодження пам'яток-об'єктів культурної спадщини, а також порушення вимог охорони об'єктів спадщини (несанкціоновані роботи, недбале зберігання тощо) регулюються Кримінальним кодексом України (ст. 298) та Кодексом України про адміністративні правопорушення (ст. 92, 188^{33}).

Разом з тим, вважаємо за доцільне, звернути увагу на питання щодо розроблення спеціальної норми, яка б передбачала відповідальність за незаконне використання знаку охорони культурних цінностей, використання культурних цінностей, які знаходяться під спеціальним захистом [7].

Зважаючи на масштаб завданої шкоди культурній спадщині, Україна мобілізувала державні, громадські та міжнародні ресурси для її збереження. У 2022 р. створено Реєстр пошкоджених об'єктів, що містить опис, фото, геолокацію – як доказову базу для судів та основу для відновлення. Забезпечено функціонування інформаційно-комунікаційної системи «Державний реєстр нерухомих пам`яток України» e-pamiatka.gov.ua», забезпечено роботу в ній обласних уповноважених органів охорони культурної спадщини та спеціалістів міністерства. У 2023 році Міністерство культури та стратегічних комунікацій розробило проект цифровізації, укриттів для музеїв, правового супроводу спадщини під час війни. Завдяки співпраці з Google, ЮНЕСКО та SUCHO розпочато цифрову архівацію спадщини: 3D-моделювання, фотофіксація, створення віртуальних копій [1].

Отже, культурні цінності України як матеріальні об’єкти є свідченням історичного становлення українського народу, української нації, є частиною світової культурної спадщини, а отже безумовно підлягають збереженню і захисту від знищення чи пошкодження.

Список використаних джерел

1. Вікторія Губарева. Цифрова відбудова: як сучасні технології допоможуть зберегти архітектурну спадщину? 2023. URL : https://rubryka.com/article/3d-skanuvannya-arhitektury/

2. Про охорону культурної спадщини : Закон України від 8 черв. 2000 р. № 1805-III

URL: https://kodeksy.com.ua/pro_ohoronu_kul_turnoyi_spadwini/27.htm

3. Базов О.В. Міжнародно-правові засади відповідальності за міжнародні злочини проти культурної спадщини в умовах збройних конфліктів. Юридична україна. 2020. С. 67–72. URL: https://yur-ukraine.com/wp-content/uploads/2021/04/pdf-6.pdf.

4. Короткий Т., Савченко Я., Хендель Н. Виклики та загрози для культурної спадщини України в умовах агресії рф проти України. Український часопис міжнародного права. 2022. С. 54–65. URL: https://doi.org/10.36952/uail.2022.4.54-65.

5. Конституція України. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

6. Правові аспекти культурної спадщини та захисту історичних пам’яток. «Консультант» Юридичний маркетплейс. Дата публікації 29.05.2024. URL: https://consultant.net.ua/consultant-article/4755.

7. Іліка М. Правове регулювання захисту культурних цінностей в Україні в умовах воєнного стану. Юридичний факультет ЧНУ ім. Юрія Федьковича. URL: https://law.chnu.edu.ua/pravove-rehuliuvannia-zakhystu-kulturnykh-tsinnostei-v-ukraini-v-umovakh-voiennoho-stanu/

Дорощук Ніна Олександрівна,
професор кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат історичних наук, доцент

ЗНАЧЕННЯ ВИКЛАДАННЯ ІСТОРИКО-ПРАВОВИХ ДИСЦИПЛІН У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ ДЛЯ ЗМІЦНЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПРОТИДІЇ РАШИСТСЬКИМ ІПСО

Повномасштабна збройна агресія російської федерації проти України призвела до суттєвої трансформації усього спектру суспільних відносин у нашій державі і, зокрема, в освітньому просторі. Війна стала черговим викликом для

системи освіти, адже обумовила потребу у змінах організаційних форм навчання, переосмисленні акцентів у змісті навчального матеріалу, виборі методів викладання. Тож особливої ваги у сучасних умовах набули гуманітарні, передусім, історико-правові, дисципліни, адже вони відіграють ключову роль у формуванні патріотизму, усвідомленні національної ідентичності, розвитку правової свідомості здобувачів вищої освіти.

Агресія з боку російської федерації сьогодні здійснюється у різних формах: як збройній, так і ідеологічній. Тож інформаційна війна, поширення ІПСО великою мірою впливають на наповненість інформаційного простору України. Це створює додаткові перешкоди формуванню правової свідомості та правової культури здобувачів вищої освіти [1, с. 100]. Історико-правова підготовка закладає основи критичного мислення, створює ідеологічну базу для протидії дезінформації та посилення згуртованості суспільства.

Історико-правові дисципліни займають вагоме місце в системі освітньо-професійного навчання здобувачів вищої освіти у закладах вищої освіти зі специфічними умовами навчання, які здійснюють підготовку поліцейських, що закріплено Стандартом вищої освіти першого (бакалаврського) рівня галузі знань 08 Право, спеціальності 081 Право, затвердженого наказом Міністерства освіти і науки України від 20.07.2022 р. № 644 та Стандартом вищої освіти першого (бакалаврського) рівня галузі знань 26 Цивільна безпека, спеціальності 262 Правоохоронна діяльність, затвердженого наказом Міністерства освіти і науки України від 28.05.2024 р. № 769 та розробленими, відповідно до законів України та названих стандартів, Освітньо-професійною програмою за першим (бакалаврським) рівнем вищої освіти підготовки фахівців освітнього ступеня бакалавра в галузі знань 08 «Право» за спеціальністю 081 «Право» кваліфікація: бакалавр права, та Освітньо-професійною програмою за першим (бакалаврським) рівнем вищої освіти підготовки фахівців освітнього ступеня бакалавра в галузі знань 26 «Цивільна безпека» за спеціальністю 262 «Правоохоронна діяльність» кваліфікація: бакалавр правоохоронної діяльності.

До дисциплін історико-правового циклу, які викладаються у національній академії внутрішніх справ належать: Історія держави та права України та Історія держави та права зарубіжних країн, які вивчаються здобувачами вищої освіти за спеціальністю 081 «Право», та Історія держави та права, яка вивчається здобувачами вищої освіти за спеціальністю 262 «Правоохоронна діяльність». Названі дисципліни формують у здобувачів вищої освіти розуміння закономірностей розвитку держави та права, сприяють виробленню правильних оцінок державно-правових явищ, вихованню політичної та правової культури, поваги до прав і свобод громадян, розвитку патріотичних та морально-етичних переконань, формуванню науково-юридичного світогляду та мислення, необхідних для вивчення та застосування права. Ці знання є фундаментальними для розуміння сучасної юридичної доктрини, законодавства та практики правозастосування.

Водночас, у сучасних реаліях, вони виступають інструментом ідеологічного супротиву та запорукою здатності протидіяти ворожим ІПСО. Тож в умовах воєнного стану, коли питання державного суверенітету, тяглості української

правової ідентичності, національної безпеки, дотримання прав і свобод людини набувають особливої гостроти, значення вивчення історико-правових дисциплін важко переоцінити.

Сучасні рашистські інформаційні атаки мають системний характер, у їх основі лежать спотворені оцінки історичних подій, які використовуються як засіб легітимізації агресії, підриву історичних коренів українського державотворення, нівелювання цінностей українських державно-правових інститутів [2]. Упродовж століть українцям нав'язувалися російські імперські наративи. Наприклад, оцінюючи зміст Переяславської угоди (1654 р.), російські ідеологи стверджують що то був акт добровільного входження українських земель до складу московської держави на засадах автономії і таким чином відбулося «возз'єднання двох братніх народів». Українські вчені, на основі ґрунтовного дослідження «Березневих статей» (1654 р.), доводять, що це були відносини протекторату, метою яких для Б. Хмельницького була спільна боротьба проти Речі Посполитої. Ліквідація Гетьманщини в українській науці трактується як результат імперської колонізаторської політики, метою якої була уніфікація суспільно-політичних відносин, а відтак – асиміляція українців. У російських дослідженнях ця подія подається як раціональна адміністративна реформа, метою якої було «удосконалення системи управління у регіоні». Для українців і сталін, і путін є ніким іншим як кривавими диктаторами, для росіян – «видатними державними діячами, мудрими управлінцями, жорстокими до ворогів, але та жорстокість є абсолютно необхідною для захисту інтересів свого народу». Аналіз процесів становлення радянської влади в Україні у 1917-1921 рр. та анексії Криму, Донецької та Луганської областей (2014 р.) засвідчують спадковість і незмінність як цілей, так і стратегії й тактики імперської політики рашистської держави.

Отже, вивчення історії україно-російських відносин, численних прикладів збройного протистояння, різного роду проявів шовіністичної рашистської політики дозволяє виробити розуміння багатоваріантності історичних інтерпретацій подій, а відтак формує розуміння причин та мотивів діяльності як окремих політиків так і зовнішньої та внутрішньої політики держави загалом. Опанування цими компетентностями сприяє розвитку стійкості майбутніх правоохоронців до маніпулятивного впливу, посилює уміння розрізняти фейки, забезпечує здатність протистояти дезінформації.

Важливим аспектом історико-правової підготовки є також аналіз досвіду провідних країн світу у подоланні кризових явищ та загроз державному суверенітету. Для прикладу, вивчення напрацювань Ізраїлю у «війні судного дня» (1973 р.), коли, в умовах неочікуваної агресії та зниженої готовності армії, ізраїльським політикам та військовим вдалося знайти правильні рішення для перемоги над агресором є надзвичайно актуальним для українського сьогодення. Дослідження «Нового курсу» президента США Ф. Рузвельта, завдяки якому вдалося подолати «велику депресію», безумовно стане у нагоді у період повоєнної відбудови України.

Отже у сучасних умовах повномасштабної російсько-української війни викладання історико-правових дисциплін у закладах вищої освіти має важливе

теоретичне і практичне значення. Історико-правові дисципліни є фундаментальними у професійній підготовці майбутніх правників, оскільки закладають основи розуміння закономірностей державно-правового розвитку. Водночас їх вивчення сприяє не лише формуванню базових знань, але і навиків критичного мислення, наукового аналізу історичних джерел, що є ключовим у розпізнаванні дезінформації, виробленню усвідомлених оцінок державно-правових явищ. Опанування історико-правовими знаннями закладає міцні підвалини національно орієнтованої правової свідомості, що дозволяє протистояти ворожим інформаційним впливам.

Список використаних джерел

1. Константінов С.Ф. Юридична освіта та підготовка правників в умовах воєнного стану. *Нове українське право*. 2023. № 2. С. 98–103.
2. Капранов Д.В. Історична пам'ять і дезінформація: механізми протидії в умовах гібридної війни. *Інформаційне право України*. 2023. № 1. С. 51–58.

Дручек Олена Василівна,
професор кафедри правового забезпечення та правоохоронної діяльності факультету забезпечення державної безпеки Київського інституту Національної гвардії України, кандидат юридичних наук, доцент
Москалюк Олена Михайлівна,
старший спеціаліст-криміналіст з особливих доручень управління криміналістичного забезпечення головного слідчого управління Національної поліції України, кандидат юридичних наук

ІНФОРМАЦІЙНА БЕЗПЕКА У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ: ПРОБЛЕМИ ПОНЯТТЯ ТА ЗМІСТУ

За сучасних умов інформація є найціннішим ресурсом, що глобальним чином впливає на потенціал розвитку держави, суспільства та людської цивілізації у цілому. Водночас, інформація є суспільним і технологічним феноменом, швидкі і почасти неконтрольовані зміни котрого призводять до зміни його якості, а, отже – до трансформації змісту. Відтак, сучасне суспільство перебуває під постійною загрозою отримання недостовірної, спотвореної інформації, маніпулювання нею, інформаційного шпигунства, комп'ютерної злочинності тощо.

Значне зростання ролі інформації в умовах ведення повномасштабної війни, розв'язаною росією проти України, а також стрімкий розвиток використання

надсучасних інформаційних технологій, включно із ШІ, суттєво впливають як на функціонування сектору безпеки та оборони у цілому, так і на функціонування Національної поліції України, зокрема. Адже непрофесійний підхід до інформатизації може не тільки перешкодити отриманню очікуваних результатів у конкретному сегменті функціонування зазначених суб'єктів, а й перетворитися на джерело серйозних загроз існуванню держави у цілому.

Аналізуючи національне законодавство у сфері інформаційної безпеки, приходимо до висновку, що у його межах наразі не визначено вимоги, заходи та способи забезпечення та гарантування інформаційної безпеки у діяльності правоохоронних органів України, зокрема, Національної поліції.

Незважаючи на те, що у розділі 4 Закону України «Про Національну поліцію» [1] визначено основні положення інформаційно-аналітичного забезпечення поліції, ні у цьому, ні у будь-якому іншому правовому акті не розкрито зміст поняття «інформаційна безпека у діяльності Національної поліції України».

Проблемні питання інформаційної безпеки діяльності правоохоронних органів розробляли О. Негодченко [2], Є Нікулін [3], Н. Моргун [4], А. Пересада [5], А. Суббот [6] та інші дослідники.

Вважаємо, що в основу вирішення проблеми визначення поняття інформаційної безпеки у діяльності Національній поліції України (НПУ) має бути покладено підхід, відповідно до якого зазначене поняття розглядається як елемент системи національної безпеки та складова інформаційної безпеки – стану захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом» [7].

Концептуальне розуміння інформаційної безпеки ґрунтується, передовсім, на його розумінні зазначеного поняття як сукупності певних проявів, що обумовлюють безпеку інформаційного простору, а саме: процесу забезпечення захищеності інформації; діяльність уповноважених суб'єктів державної влади щодо захисту інформаційного простору; стану захищеності інформації; сукупність суспільних відносин у сфері захисту інформації та напрямок державної політики [8, с. 25–30]. Виходячи із зазначеного, інформаційна безпека в умовах інформаційного суспільства розглядається як суспільно-правовий та технічний феномен, що об'єктивується в організаційній, технічній та правовій сфері, та потребує окремого напряму правового регулювання.

Важливим для формування поняття інформаційної безпеки у діяльності НПУ вважаємо виділення ключових ознак загального поняття «інформаційна безпека», які обґрунтовують Н. Моргун, О. Шевчук, С. Марчевський, а саме: а)

наявність відомостей про які-небудь події та чиюсь діяльність; б) належність таких відомостей до інтересів окремих суб'єктів; в) забезпечення уповноваженими суб'єктами захисту інформаційного простору від внутрішніх та зовнішніх загроз; г) наявність певних правовідносин, однією із сторін яких виступає держава; ґ) наявність інформаційного простору (інформаційних ресурсів, інформаційної інфраструктури; засобів інформаційної взаємодії) [4, с. 412].

Виявлені зв'язки між складовими поняття інформаційної безпеки обумовлюють можливість їх застосування до аналізу поняття «інформаційна безпека у діяльності НПУ». Так, Є.Ю. Нікулін під зазначеним поняттям розуміє такий стан внутрішніх та зовнішніх правовідносин, при якому, по-перше, забезпечується та гарантується правомірність використання уповноваженими особами органів Національної поліції інформації в межах відомчого, міжвідомчого, загальнодержавного та міжнародного інформаційного простору; по-друге, здійснюються заходи, спрямовані на своєчасне виявлення, запобігання і нейтралізацію реальних і потенційних загроз інформаційній безпеці поліції та протидію несанкціонованим діям щодо інформації у ввіреному інформаційному просторі» [3, с. 20]. Натомість, Н. Моргун, О. Шевчук, С. Марчевський розглядають інформаційну безпеку у діяльності НПУ у якості складової національної безпеки України, що виявляється у правовідносинах уповноважених суб'єктів поліції між собою та з іншими суб'єктами (людиною, суспільством, державою, юридичними особами), які спрямовані на забезпечення захисту інформаційного простору від будь-яких загроз [4, с. 213-414].

Зміст функції забезпечення інформаційної безпеки НПУ, на нашу думку, пов'язаний із функцією охорони та захисту інформації у суспільних відносинах, які мають місце у суспільстві, що обумовлює необхідність застосування поліцейськими спеціальних знань із технічних галузей, підгалузей, окремих інституцій як технічних, так і суспільних наук.

Під системою інформаційного забезпечення органів поліції Г.М. Шорохова розуміє сукупність взаємопов'язаних і взаємодіючих організаційних елементів і технічних засобів, які здійснюють інформаційне забезпечення НПУ[9, с. 266].

Забезпечення захисту інформаційного простору від будь-яких загроз відбувається органами (підрозділами) поліції під час виконання ними завдань з надання поліцейських послуг у сферах: охорони прав і свобод людини, а також інтересів суспільства і держави; забезпечення публічної безпеки і порядку; протидії злочинності; надання в межах, визначених Законом України «Про Національну поліцію», послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги.

У ст. 25 Закону України «Про Національну поліцію» [1] визначено повноваження поліції у сфері інформаційно-аналітичного забезпечення. Зокрема, визначено, що поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень у таких напрямах: 1) формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; 2) користується базами (банками) даних Міністерства

внутрішніх справ України та інших органів державної влади; 3)здійснює інформаційно-пошукову та інформаційно-аналітичну роботу; 4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями; 5) надає до Єдиного державного реєстру призовників, військовозобов'язаних та резервістів. Поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень.

Однією із умов підвищення ефективності системи інформаційної безпеки функціонування НПУ у період воєнного стану в Україні є пошук принципово нових способів організації роботи з інформаційними ресурсами, стандартизація яких спрямована на створення та гармонізацію єдиного інформаційного простору сектору безпеки та оборони та, зокрема, правоохоронних органів.

Узагальнення позицій спеціалістів із проблем формування систем протистояння інформаційній небезпеці [10, 11, 12] дозволяє окреслити систему необхідних заходів, які можуть бути застосовані для захисту інформаційної безпеки діяльності НПУ у період воєнного стану, та здійснюватися комплексно, на основі нових наукових розробок і програмних продуктів. На нашу думку, комплекс таких заходів має реалізовуватися за двома основними напрямами: 1) захист інформаційних систем, що використовуються у діяльності НПУ у процесі виконання поставлених перед нею задач; 2) захист працівників поліції від шкідливого інформаційно-психологічного впливу.

Так, у межах першого із зазначених напрямів доцільним вважаємо: а) здійснення захисту об'єктів, що перебувають у розпорядженні органів НПУ, та розташованої в них комп'ютерної техніки від пошкодження або іншого навмисного виведення з ладу; б) захист інформаційних систем НПУ від кібератак, зокрема, шляхом установки відповідних систем захисту, що забезпечують повний захист периметра від вторгнень; в) захист інформації, яка становить державну, військову або службову таємницю, від несанкціонованого витоку; г) радіоелектронний захист; ґ)розробку засобів електронної розвідки; д) використання соціальних мереж для формування відповідної інформаційної політики та протистояння дезінформації противника; д) захист систем зв'язку. У межах другого із зазначених напрямів доцільним вважаємо: а) запобігання психологічного впливу на психіку працівників НПУ; б) використання всіх доступних видів психологічної роботи із поліцейськими, з подальшим їх поширенням на різні категорії населення; в) здійснення цілеспрямованих заходів інформаційно-психологічної підтримки.

Вважаємо, що зазначені заходи своїм результатом матимуть створення стійкого захисту від інформаційного впливу та готовності працівника поліції до відсікання інформації, яка має на меті дестабілізацію морально-психологічного стану та забезпечення перемоги ворога у інформаційній війні.

З огляду на зазначене, вважаємо за необхідне розробити закон «Про інформаційну безпеку правоохоронних органів України», чим закласти

нормативну базу відповідного напряму державного управління. У зазначеному контексті слушним буде виокремлення інформаційної безпеки правоохоронних органів як різновиду інформаційної безпеки, а також подальша реалізації завдання – це вироблення необхідних нормативно-правових документів, координації процесів належного використання інформації у діяльності правоохоронних органів.

Список використаних джерел

1. Про Національну поліцію: Закон України від 2 лип. 2015 р. № 580-VIII. URL:https://zakon.rada.gov.ua/laws/show/580-19#Text// (дата звернення: 29.04.2025).
2. Негодченко В.О. Інформаційна безпека в органах Національної поліції України: адміністративно-правове забезпечення. *Право і суспільство.* № 6. 2020. С. 167– 174. DOI: https://doi.org/10.32842/2078- 3736/2020.6.1.24. (дата звернення: 29.04.2025).
3. Нікулін Є.Ю. Адміністративно-правове забезпечення інформаційної безпеки Національної поліції України: дис. … канд. юрид. наук. : 12.00.07. Київ. 2021. 133 с. URL: https://uacademic.info/ua/document/0422U100087#google_vignette. (дата звернення: 29.04.2025).
4. Моргун Н.С., Шевчук О.О., Марчевський С.В. Щодо визначення поняття інформаційної безпеки у діяльності Національній поліції України. *Аналітично-порівняльне правознавство.* 2024. № 8. С. 409-415. URL: https://app-journal.in.ua/wp-content/uploads/2024/08/69.pdf. (дата звернення: 29.04.2025).
5. Пересада О.М. Роль Національної поліції України в забезпеченні інформаційної безпеки держави: теоретико-методологічні аспекти. *Правовий часопис Донбасу.* № 4 (69). 2019. С. 183–189. DOI: https:// doi.org/10.32366/2523-4269-2019-69-4- 183-189.
6. Суббот А. Інформаційна безпека діяльності працівників правоохоронних органів. *Віче.* 2014. № 22. С. 19-22. URL: http://nbuv.gov.ua/UJRN/viche_2014_22_6.
7. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text. (дата звернення: 29.04.2025).
8. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. Київ : КНТ, 2006. 280 с.
9. Шорохова Г.М. Інформаційне забезпечення діяльності територіальних органів поліції України. *Юридичний науковий електронний журнал.* 2018. № 6. С. 264–267. URL: http://www.lsej.org.ua/6_2018/73.pdf. (дата звернення: 29.04.2025).
10. Кавун С.В., Носов В.В., Манжай О.В. Інформаційна безпека. Навчальний посібник. Ч. 2. Харків: Вид. ХНЕУ, 2018. 196 с.
11. Петровський О. Проблемні питання формування єдиного інформаційного простору правоохоронних органів. *Підприємництво, господарство і право.* 2017. № 8. С. 145–148.

12. Смотрич Д., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету.* Серія ПРАВО. 2023. Випуск 77: частина 2. С.121-127. DOI https://doi.org/10.24144/2307-3322.2023.77.2.20.

Іванчук Наталія Віталіївна,
старший викладач кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат юридичних наук

КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ДЕРЖАВНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасне життя неможливо уявити без глибокого проникнення інформатизації в усі його сфери. Інформаційна розвиненість поступово стає однією з важливих складових, що визначають образ «сучасної людини», створюючи необхідну основу для її повноцінного існування. С кожним роком інформація набуває все більшого загальносуспільного значення, що надає особливу актуальність гуманітарним дослідженням явищ, нерозривно пов’язаних з нею.

Інформатизація сучасного суспільства передбачає проникнення інформаційних технологій практично в усі сфери суспільного життя, що надає домінуючого значення діяльності держави, пов’язаній із забезпеченням вільного обміну інформацією, інтеграцією у світове інформаційне суспільство, забезпеченням інформаційної безпеки та інші.

Однак, в умовах глобалізації інформаційного обміну і широкого впровадження інформаційних технологій в усіх сферах життєдіяльності суспільства України існує проблема захисту інформації, що обробляється в інформаційних, інформаційно-телекомунікаційних та автоматизованих системах від викликів і загроз у кібернетичному та віртуальному просторі, а також від кримінальних протиправних дій правопорушників. Тим більше, що у сучасному за інформатизованому суспільстві інформація стала не просто засобом комунікації, а й об’єктом діяльності людей, тому сьогодні її сутність вивчається багатьма галузями знань.

Забезпечення інформаційної безпеки України є однією з найважливіших функцій держави. Держава, маючи найбільші можливості впливу на суспільні відносини, потенційно є найнебезпечнішим елементом, але водночас і основним стимулятором та організатором покращення умов функціонування суспільства. Тому, основою забезпечення високого рівня інформаційної безпеки повинна стати ефективна управлінська діяльність, яку доцільно розглядати в двох аспектах: як управління технічними системами та як вплив на соціальні процеси з метою досягнення поставлених цілей. У світлі розбудови глобального інформаційного суспільства другий аспект набуває особливого значення.

Сучасна теорія соціального управління інтерпретує управлінську діяльність як підтримання цілісності будь-якої складної соціальної системи та забезпечення її оптимального функціонування і розвитку. Для врахування взаємозв'язку інформаційної безпеки і громадянського суспільства слушним буде її осмислення крізь призму теорії соціальних систем. Іншими словами, відображенням поєднання управлінського аспекту може стати осмислення інформаційної безпеки як стану інформаційної Це покладає на державу особливу відповідальність і висуває найвищі вимоги до якості та ефективності її діяльності в інформаційній сфері, зокрема і до правового забезпечення інформаційних відносин.

Дослідження функції держави, її сутності та змісту безпосередньо залежать від мети, поставленої перед державою, завдань, які є найбільш актуальні для неї на певному історичному етапі розвитку суспільства. Мета діяльності держави – це виражена воля суспільства, що спрямована на досягнення бажаних результатів, зумовлених рівнем розвитку суспільства. Вона уособлює собою прагнення досягти змін якісного і кількісного характеру відповідно до об'єктивних закономірностей розвитку суспільства, його можливостей та потреб. Вища мета держави це загальний стратегічний напрям її діяльності. На відміну від основних функцій, які є напрямами діяльності у певних сферах, вона представляє собою єдиний загальнодержавний напрям діяльності на певному етапі розвитку суспільства і держави. Функції, завдання держави, як правило, підкоряються єдиній меті. Саме мета держави є визначальною і впливає на зміст функцій і завдань держави, породжує необхідну реалізацію відповідних функцій.

Відповідно до ст. 17 Конституції України забезпечення інформаційної безпеки, поряд із захистом суверенітету і територіальної цілісності, визнається однією з найважливіших функцій держави і справою всього Українського народу. Виходячи з цього, забезпечення інформаційної безпеки доцільно розглядати як цілеспрямовану діяльність, домінуючим, але не єдиним елементом об'єктно-суб'єктного складу якої є держава. Така інтерпретація враховує синергетичні тенденції розвитку сучасного суспільства та субсидіарні особливості його взаємодії з державою і в повній мірі відповідає положенням теорії держави і права, згідно з якими функції держави розуміються як напрями, сторони або види державної діяльності.

Якщо говорити про інформаційні заходи оборони держави, то це сукупність скоординованих дій, які готуються та здійснюються суб'єктами забезпечення національної безпеки і оборони України в мирний час, в особливий період, в умовах воєнного або надзвичайного стану щодо прогнозування та виявлення інформаційних загроз у воєнній сфері, запобігання, стримування та відсічі збройній агресії проти України, протидії інформаційним загрозам з боку держави-агресора, а також здійснення інших необхідних дій в інформаційному протиборстві.

Сьогодні інформаційна сфера є інтегруючою основою життєдіяльності суспільства, а забезпечення інформаційної безпеки визнається однією з концептуальних засад його подальшого розвитку. За таких умов особливого значення набуває формування виваженої державної інформаційної політики на

основі системних наукових досліджень явищ інформаційної сфери, провідне місце серед яких займає інформаційна безпека.

Інформаційна безпека України – це складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів.

Забезпечення такої безпеки є пріоритетною функцією держави, спрямованість якої визначається інформаційним розвитком. Належний рівень сталого розвитку інформаційної безпеки зумовлюється сукупністю правових умов, спрямованих на оптимальне функціонування та розвиток суб'єктів інформаційного простору в частині законності та доцільності. Остання має розглядатися як особливий предмет інформаційних відносин, важливий засіб та, водночас, об'єкт державно-правового забезпечення інформаційної безпеки.

Враховуючи такий концептуальний підхід, інформаційна безпека як результат комплексної державної діяльності і як стан оптимального функціонування і розвитку суб'єктів в інформаційній сфері потребує комплексної оцінки через систему показників інформаційної безпеки (критерії та показники, що відображають технологічну сторону безпеки й рівень інформаційного розвитку суспільства, а також наявні та потенційні можливості до забезпечення безпеки) – найбільш значущих параметрів, що надають загальне уявлення щодо інформаційної системи держави, її стійкості, ефективності, здатності до розвитку тощо.

Список використаних джерел

1. Оніщенко Н.М. Правова система: проблеми теорії. Київ : Ін-т держави і права ім. В. М. Корецького НАН України, 2002. 349 с.
2. Довгань О.Д., Ткачук Т.Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право*. 2019. № 1 (28). С. 86–99.
3. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України : дис. докт. юрид. наук : 12.00.07. Ужгород, 2019. 487 с.
4. Інформаційна безпека України: глосарій / заг. ред. Р. А. Калюжний. Київ : Текст, 2004. 136 с.
5. Француз А.Й., Кудін С.В., Федорчук О.В. Сутність інформаційної безпеки України. *Право.ua.* 2022. № 4. С. 5–10.

Кравець Віталій Михайлович,
професор кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат юридичних наук, доцент

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ГЛОБАЛІЗАЦІЇ

Сучасну епоху називають ерою інформації або інформаційним суспільством, де інформація стала одним з ключових ресурсів розвитку держави та суспільства. Впровадження інформаційних технологій у всі сфери суспільного життя істотно підвищило залежність безпеки держави, суспільства та кожної конкретної людини від надійності функціонування інформаційної інфраструктури, достовірності інформації, що використовується, її захищеності від несанкціонованої модифікації, а також протиправного доступу до неї. Потреби сучасної людини суттєво змінилися і розширилися, зріс попит на інформаційну безпеку для особистісної реалізації в умовах сучасних глобалізаційних викликів.

У нинішніх реаліях саме розвиток інформаційних технологій, рівень інформаційної безпеки та міжнародна інформаційна безпека визначатимуть місце держави на міжнародній арені. Найближчим часом залежність усіх сфер діяльності суспільства та держави від інформаційних систем буде тільки зростати і потребувати підвищення якості технологій [1, с. 61].

Україна, як і більшість країн світу, стикається з різноманітними викликами в цій сфері – від кібератак та шпигунства до поширення недостовірної інформації та втручання у внутрішні справи [2, с. 9]. Щоб вистояти в таких умовах перед дезінформацією та маніпуляціями, які вміло застосовують, насамперед, російські ЗМІ, і яка розповсюджується за допомогою соцмереж та інших комунікаційних каналів, кожній державі необхідна консолідація, довіра до влади, а з боку держави – широкомасштабна інформаційна політика швидкого реагування із застосуванням сучасних технологій. При цьому, громадяни повинні правильно фільтрувати інформацію, критично мислити, аналізувати, звертати увагу на джерела інформації, власників медіа, оскільки в міру збільшення усвідомлення маніпуляція зменшується.

Відповідно до Конституції України захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [3].

У Стратегії інформаційної безпеки дається визначення поняттю «інформаційна безпека України» як складової частини національної безпеки України, стану захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєвоважливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об’єктивної інформації, існування ефективної системи захисту і протидії нанесенню шкоди через

поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [4].

Таким чином, інформаційну безпеку треба розуміти як стан, при якому за допомогою національних та міжнародних ресурсів забезпечується захист від інформаційного впливу на свідомість особи та суспільства, унеможливлюється інформаційний вплив на прийняття рішень державними інститутами, а також недоторканість приватних і державних цифрових баз даних, можливість їх швидкого відновлення у випадку протиправного посягання і забезпечення покарання зловмисників [5, с. 244].

Щодо принципів інформаційної безпеки, варто зазначити, що законодавство України на сьогоднішній не містить їх переліку [6, с. 53]. Проте, відповідно до ст. 3 проекту Закону України «Про засади інформаційної безпеки України», основними принципами забезпечення інформаційної безпеки України є [7]:

– верховенство права;

– пріоритетність захисту прав і свобод людини і громадянина в інформаційній сфері;

– своєчасність і адекватність заходів захисту життєвоважливих національних інтересів України від реальних і потенційних загроз інформаційній безпеці;

– свобода збирання, зберігання, використання та поширення інформації; достовірність, повнота та неупередженість інформації;

– захищеність особи від втручання в її особисте та сімейне життя;

– обмеження доступу до інформації виключно на підставі закону;

– гармонізація особистих, суспільних і державних інтересів, відповідальність всього Українського народу за забезпечення інформаційної безпеки;

– розмежування повноважень, взаємодія та відповідальність державних і недержавних суб’єктів забезпечення інформаційної безпеки;

– пріоритетність розвитку національних інформаційних технологій, ресурсів, продукції та послуг;

– можливість задіяння в інтересах забезпечення інформаційної безпеки України систем і механізмів міжнародної та колективної безпеки;

– гармонізація інформаційного законодавства з нормами міжнародного права і правовими актами Європейського Союзу.

Досвід світової спільноти вказує на те, що ефективне вирішення питань захисту інформації, яка обертається у інформаційно-телекомунікаційних системах, та забезпечення надійного захисту цих систем від злочинних посягань, включаючи атаки з-за кордону, можливе тільки за умови створення комплексних систем захисту. Ці системи мають інтегрувати правові, організаційні, інженерні та технічні заходи разом із програмними засобами захисту.

Центральну роль у системі управління інформаційною безпекою в Україні відіграє Державна служба спеціального зв’язку та захисту інформації, яка

координує заходи з криптографічного та технічного захисту інформаційних ресурсів, забезпечуючи надійний зв'язок між органами державної влади та інтегрований захист інформаційних систем [8].

Ефективне державне управління інформаційною безпекою вимагає координації та співпраці між різними органами державної влади, правоохоронними органами, громадськими організаціями та приватним сектором, що дозволить обмінюватися інформацією, координувати заходи з реагування на загрози та вдосконалювати практики інформаційної безпеки. Держава повинна встановлювати та забезпечувати стандарти безпеки інформаційних систем, просувати культуру кібербезпеки, здійснювати моніторинг кіберзагроз і реагувати на них, а також сприяти розвитку кадрового потенціалу у сфері кібербезпеки.

Вивчення міжнародного досвіду дозволяє прийти до висновку, що Україні варто адаптувати найефективніші практики та інструменти забезпечення інформаційної безпеки, враховуючи свої унікальні характеристики та виклики. Серед ключових напрямів, на які варто звернути увагу для забезпечення надійної інформаційної безпеки держави в сучасних умовах, – інтеграція світових стандартів, створення внутрішньої нормативно-правової бази, посилення взаємодії державних і приватних структур, підвищення інформаційної грамотності населення [6, с. 56].

Погоджуємося з думкою Терзі О.О., що інформаційну безпеку можна гарантувати лише завдяки міжнародній співпраці, оскільки комунікаційні мережі мають глобальний характер. У зв'язку з цим, необхідно посилити відносини України з іншими державами та міжурядовими організаціями щодо забезпечення правової безпеки інформації.

Список використаних джерел

1. Фокіна-Мезенцева К. Інформаційна безпека у глобальному суспільстві. *Вісник КНТЕУ.* 2021. № 5. С. 61–71.
2. Шевчук М.О. Система управління інформаційною безпекою в контексті сучасних викликів. *Науковий вісник Херсонського державного університету.* Серія Юридичні науки. Випуск 1. 2024. С. 9–13.
3. Конституція України від 28.06.1996. URL: https://zakon. rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/ conv#Text.
4. Стратегія інформаційної безпеки. URL: https:// zakon.rada.gov.ua/laws/show/685/2021#n14.
5. Кононенко В.П., Здоровко С.С., Корольова А.Є. Інформаційна безпека як стан. *Науковий вісник Ужгородського Національного Університету,* 2023. Серія Право. Випуск 76: частина 2. С. 244–250.
6. Терзі О. О. Принципи забезпечення інформаційної безпеки держави: досвід України та зарубіжних країн. *Право та державне управління.* 2024. № 3. С. 51–57.
7. Проект Закону України «Про засади інформаційної безпеки України», внесений народними депутатами України: І. М. Стойком (реєстр. № 390),

О. І. Кузьмуком (реєстр. № 041), Ю. М. Сиротюком (реєстр. № 214) URL: https://ips.ligazakon. net/document/JG3TH00A?an=31

8. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23 лютого 2006 р. № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

Кривицький Юрій Віталійович,
завідувач кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат юридичних наук, доцент

ВСТУП ДО МЕТОДОЛОГІЇ ДОСЛІДЖЕННЯ ПРАВОВОЇ РЕФОРМИ

Усе має бути зроблено настільки просто, наскільки це можливо, але не більше[1]

Розвиток вітчизняного правознавства зумовлений інтеграційними і глобалізаційними процесами, що відбуваються в Європі та світі, його переходом від методологічного монізму до світоглядно-методологічного плюралізму. Це у свою чергу викликає необхідність концептуального перегляду традиційних уявлень про праводержавні закономірності, а також поглибленого осмислення ролі юридичної науки в новітньому суспільстві. Ґрунтовне пізнання правових і державних явищ, визначення принципових орієнтирів подальшого поступу правознавства є найважливішим напрямом наукових досліджень, основою ефективності яких має бути методологія правознавства. Саме тому формування методологічної системи є першочерговим завданням сучасної юриспруденції. Особливо важливі ці питання для української правової науки [1, с. 5].

Загальновизнано, що методологічні дослідження – необхідна умова розвитку науки. На зламах історії, в умовах кризових викликів остання завжди повертається до методологічних питань [2, с. 11–12]. Вони істотно актуалізуються в періоди суспільних реформ, докорінних трансформацій системи цінностей, світоглядних основ та орієнтирів соціуму. Адекватність опрацювання економічних, культурних, політичних і соціальних перетворень, результативність досліджень нових правових реалій повинні базуватися на сучасній системі теоретичних уявлень, сформованих у результаті перегляду філософських засад і методів наукового пізнання права [3, с. 10].

Оновлення юридичної методології, окрім антропологізації, глобалізації й деформалізації, детерміноване процесами глокалізації, локалізації, правової глобалізації, кризою низки міжнародних правових принципів, норм, інститутів, руйнуванням правових засад міжнародної безпеки, суттєвим підвищенням

[1] Ейнштейн (нім. Einstein) Альберт (1879–1955 рр.) – німецький та американський фізик, громадський діяч-гуманіст.

геополітичної напруги, які призводять до зростання ролі й значення ідеологічних постулатів правового розвитку, актуалізації праворозуміння, юридичної доктрини, трансформації уявлень про напрям і спрямованість розвитку правової системи крізь призму співвідношення принципів міжнародної безпеки та національного суверенітету, універсальних і конкретно-історичних правових принципів, норм, стандартів, інститутів у правовій системі, утвердження принципів і стандартів верховенства права, прав людини, демократії, істотного зростання у правовій системі ролі інститутів громадянського суспільства, новелізації методологічних підходів, прийомів і методів, формування в юридичній науці загальних засад геогенезису [4, с. 53–54].

Ступінь достовірності пізнавальної діяльності визначається як відповідність її результатів «реальному стану речей», що залежить від обрання і використання правильного шляху та найбільш адекватних засобів наукового дослідження. Саме тому питання методологічного забезпечення є першочерговим для теоретичного осмислення в будь-якій предметній сфері. Лише за умови озброєності сучасною методологією вітчизняна юридична наука зможе виконати поставлені перед нею завдання з розробки та доктринального обґрунтування правової реформи та механізму її реалізації з урахуванням міжнародних та європейських правових стандартів насамперед у сфері охорони та захисту прав і свобод людини, функціонування демократичних інститутів.

Передовий світовий і національний досвід правового розвитку переконує, що жодна правова реформа неможлива без серйозного методологічного й теоретичного фундаменту, належного наукового та гносеологічного супроводу. Поєднання стратегії і тактики правової реформи з юридичною наукою є шляхом сприяння подоланню деструктивних процесів у соціумі. Розробка методології науки загалом і правознавчої зокрема – це досить суттєвий напрям діяльності вчених, особливо важливий для здійснення правового реформування в новітніх умовах. Своєчасність питання зумовлена об’єктивною потребою переосмислення вихідних засад методології правових реформ, необхідністю під час розбудови правової держави використання аксіологічного потенціалу права в якості основи його суспільної значущості та практичної дієвості. Адже, відповідаючи на питання, що пізнається у праві, ми завжди робимо вибір певної природи права, а оскільки ми не маємо гарантії щодо правильності зробленого вибору, то неминуче постає гносеологічне питання щодо самого характеру вибору, питання про те, як робиться вибір узагалі [5, с. 33].

У цьому контексті М.С. Кельман зазначає, що успіх правових досліджень у багатьох випадках зумовлюється використанням науково обґрунтованої методології. Опрацювання правових реформ останніх років, в тому числі у сфері сучасного правознавства, переконує, що здійснювані в цьому напрямі дослідження проводяться без використання необхідних методологічних прийомів і засобів, які повинні забезпечувати об’єктивні результати. За цих умов принципове значення мають теоретично та прагматично аргументовані, побудовані на виважених методологічних підходах концепції та програми правового розвитку суспільства, зокрема правової реформи. Для ефективності сучасного вітчизняного правознавства важливим є створення цілісної

методологічної системи, яка повинна складатися з основних концептуальних підходів, найбільш затребуваних методів і засобів пізнання як загальних, так і юридичних, а також методики правових досліджень [3, с. 441].

Усебічність наукового осмислення досвіду, проблем і перспектив правової реформи залежить від низки чинників, серед яких визначальним є з'ясування адекватних засобів і технології дослідження: методологічних підходів, принципів, методів, процедур тощо. Теоретико-методологічний запит з узагальнення, розширення та обґрунтування наукових знань про природу правової реформи зумовлює необхідність згрупування та опрацювання зібраного матеріалу, визначення стратегії наукового пізнання. Відправним пунктом дослідження є положення, що наукові знання набуваються лише за умови, якщо вивчення предмета (тобто певного аспекту, виміру, зрізу, рівня, сторони правової реформи) здійснюється відповідно до вимог теорії пізнання. Ключовим елементом цієї теорії є методологія, котра визначає істинність (правильність) і переконливість одержаних результатів та висновків наукового пошуку. За твердженням А. Ейнштейна, теорія пізнання без контакту з наукою стає порожньою схемою. Наука без теорії пізнання, якщо вона взагалі можлива без неї, – примітивна та безладна [6, с. 36]. Необхідність розробки методологічної бази дослідження істотних властивостей правової реформи зумовлена постійною потребою комплексного розкриття теоретичного образу цього правового явища та перспектив її подальшої реалізації в майбутньому.

Як слушно відмічає М.І. Козюбра, проблеми методології є неминучими для будь-якої науки. Плідність наукового пізнання, ступінь і глибина його проникнення в сутність досліджуваних явищ, а зрештою – приріст наукових знань вирішальною мірою залежать від методологічного інструментарію. Його своєчасне оновлення – неодмінна передумова не лише підвищення ефективності досліджень, а й нормотворчої та нормозастосовної практики [7, с. 22].

Отже, завершуючи методологічний екскурс у розрізі предмета наукового пошуку, варто зауважити, що методологія юридичної науки (правознавства, юриспруденції), методологія загальнотеоретичного правознавства (теорії держави і/та права, загальної теорії держави і/та права), методологія окремого наукового правового знання (наприклад, теорії правової реформи), методологія конкретного юридичного дослідження (приміром, сутності правової реформи), методологія права – це не тотожні поняття. Очевидним є й те, що будь-яка методологія як система методів має бути онотологічно й гносеологічно обґрунтованою: інша онтологія – інша й методологія.

Список використаних джерел

1. Кельман М. С., Котуха О. С., Коваль І. М. Методологія як форма мислення і складова культури дослідника : навч. посіб. / За заг. ред. М. С. Кельмана. Львів : Растр-7, 2017. 220 с.

2. Гальчинський А. С. Глобальні трансформації: концептуальні альтернативи. Методологічні аспекти : наук. вид. Київ : Либідь, 2006. 312 с.

3. Кельман М. С. Юридична наука: проблеми методології : монографія. Тернопіль : Терно-граф, 2011. 492 с.

4. Удовика Л. Г. Трансформація правової системи в умовах глобалізації: антропологічний вимір : монографія. Харків : Право, 2011. 552 с.

5. Козловський А. А. Гносеологічні принципи права. *Проблеми філософії права.* 2005. Т. III. № 1–2. С. 32–44.

6. Ющик О. І. Правова реформа: загальне поняття, проблеми здійснення в Україні : монографія. Київ : Ін-т законодавства Верховної Ради України, 1997. 192 с.

7. Козюбра М. Методологія правознавства і методологія права: співвідношення понять та їх особливості. *Право України.* 2014. № 1. С. 22–32.

Кумеда Тетяна Андріївна,
професор кафедри теорії, історії та філософії права навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат мистецтвознавства, доцент

КРИТИЧНЕ МИСЛЕННЯ ЯК ЗАПОРУКА МЕДІАСТІЙКОСТІ ПІД ЧАС ВІЙНИ

У сучасному світі інформація стала не лише джерелом знань, а й засобом впливу, маніпуляції та навіть зброєю. Інформаційна війна є невід'ємним компонентом гібридних конфліктів, які націлені не тільки на захоплення територій, знищення інфраструктури чи деморалізацію війська, але й на маніпулювання масовою свідомістю, зміну наративів, розкол суспільства. Як зауважує дослідниця Т. Каленюк, інформаційна агресія має чітко окреслену психологічну мету: «зруйнувати спільну реальність і нав'язати спотворене уявлення про події» [1, с. 102]. Інформаційна війна – це комплекс дій, спрямованих на зміну інформаційного середовища противника з метою досягнення стратегічних або тактичних переваг. Зазвичай вона розглядається як складова частина гібридної війни, яка включає пропаганду, дезінформацію, інформаційно-психологічні операції та кібератаки.

Під час повномасштабної війни в Україні проблема медіастійкості набула особливої гостроти, адже будь-яка пропаганда базується на ірріціональному, інтуїтивному сприйнятті світу та націлена на емоційний інтелект людини. Війна породжує сильні емоційні реакції, які можуть впливати на здатність мислити раціонально, і саме контроль над емоціями дозволяє краще справлятися з навантаженням війни. Замість того щоб дозволити емоціям керувати думками, людина може навчитися контролювати їх вплив і приймати раціональні рішення. У таких умовах завданням кожної людини є не просто вижити, а створити умови для повноцінного життя і максимально зберегти себе.

У цьому контексті критичне мислення виступає ключовою передумовою формування медіастійкості громадян, без якої неможливе повноцінне функціонування суспільства в умовах інформаційних атак, воно є своєрідним

ментальним імунітетом – інтелектуальним бар'єром, що не дозволяє механічно приймати будь-яку інформацію за істину. Критичне мислення – основа когнітивного розвитку, воно заохочує людину мислити неупереджено, аналітично, логічно, по-новому використовувати отримані знання. «Критичне мислення в інформаційній війні виконує роль аналогічну бронежилету на передовій: воно не гарантує цілковитої безпеки, але значно підвищує шанси на виживання – ментальне, ідеологічне, цивілізаційне» [2, с. 59]. Його відмітними рисами є рефлексивність, повільність, уважність, здатність до запитань, розрізнення стереотипів, маніпуляцій, компромісів, воно опирається на усвідомлення того, що відбувається.

Критичне мислення – це складна інтелектуальна діяльність, яка передбачає аналіз, оцінку, інтерпретацію, обґрунтованість, пошук логічних помилок та когнітивних викривлень, рефлексію та аргументацію. П. Елдер і Р. Пол визначають його як «самостійне мислення, яке ґрунтується на логіці, доказах та здатності до самокорекції» [3, p. 54]. Слід відзначити, що воно має не лише пізнавальне, але й етичне значення: воно формує культуру мислення, відповідальність за інформаційні дії та протидіє масовим маніпуляціям.

Окрім індивідуального виміру, критичне мислення набуває суспільного значення. Як підкреслює Н. Ротман, воно є основою інформаційної гігієни, без якої неможлива стабільність демократичного суспільства: «Стійкість до пропаганди починається не з заборон, а з навички запитувати: "Хто це сказав? Чому саме зараз? Які факти підтверджують це твердження?"» [4, с. 22].

У сучасній Україні критичне мислення стало не лише ознакою освіченості, а й проявом громадянської зрілості. На відміну від механічного поширення новин у соціальних мережах, критичне осмислення контенту — це акт відповідальності. Наприклад, у 2022 році після вибуху в Краматорську поширилася хвиля фейкових повідомлень про «сотні загиблих» та «зраду з боку командування». Завдяки реакції медіаспільноти, фактчекінгових ресурсів та активного аналізу користувачів ці маніпуляції були спростовані менш ніж за добу. Це свідчить про зростання ролі критичного мислення у громадян, здатних не лише споживати, а й аналізувати інформаційний потік.

Медіастійкість це не просто навичка, це інструмент самозахисту в умовах медіафлуктацій і фейкової інтервенції. Це комплекс знань, навичок та установок, необхідних для ефективної участі в інформаційному суспільстві. Медіастійкість включає вміння ідентифікувати джерела інформації, оцінювати їхню достовірність, розрізняти факти та інтерпретації, аналізувати емоційний та маніпулятивний зміст. В українському контексті цей термін адаптується з акцентом на протидію дезінформації, зокрема в умовах гібридної війни. В умовах війни медіастійкість сприяє глибшому та свідомішому аналізу подій, дозволяючи критично осмислювати власні думки, контролювати емоційні реакції та адаптувати свої переконання і стратегії до мінливих обставин. Це не лише підвищує ефективність прийняття рішень, але й сприяє збереженню раціонального підходу в умовах невизначеності та емоційного тиску, характерних для війни.

Таким чином, критичне мислення є основоположною когнітивною компетентністю, що дозволяє сформувати стійкість до інформаційних загроз. У поєднанні з медіастійкістю воно забезпечує безпечну, активну та відповідальну участь громадян у суспільному житті. Воно дозволяє людині аналізувати, оцінювати та перевіряти інформацію перед тим, як її приймати або ділитися нею, допомагає розпізнавати надійні джерела інформації від ненадійних, оцінити інформацію з різних джерел, перевірити її достовірність та визначити можливі наслідки. У військових операціях це може включати аналіз розвідувальних даних, оцінку потенційних загроз та розробку стратегій дій. На війні необхідно швидко аналізувати нові інформаційні потоки та приймати відповідні рішення.

Критичне мислення допомагає розробляти альтернативні плани дій та оцінювати їхні наслідки, виявляти власні когнітивні упередження та враховувати їх при оцінці інформації, що у свою чергу знижує ризик стати жертвою маніпуляцій через дезінформацію. У воєнний час дуже легко піддатися емоціям, страху та груповому мисленню, а критичне мислення надає здатність зберігати незалежність думки, розглядати аргументи з обох сторін конфлікту і приймати рішення, які ґрунтуються на логіці та розсудливості, а не на паніці або стереотипах. Крім того, критичне мислення під час війни також включає врахування етичних аспектів рішень - допомагає визначити, які дії є морально виправданими з точки зору людських цінностей, навіть у найскладніших обставинах.

Список використаних джерел

1. Каленюк Т. Інформаційна війна як форма когнітивної агресії: сучасні підходи до аналізу. *Політичні студії.* № 3 (19). 2022. С. 101–108.

2. Андрухов О. Інформаційна безпека в умовах гібридної війни: роль мислення та освіти. *Соціальні комунікації.* № 1. 2023. С. 55–61.

3. Paul R., Elder L. Critical Thinking: Tools for Taking Charge of Your Learning and Your Life. Rowman & Littlefield, 2022. 642 p.

4. Ротман Н. Критичне мислення як стратегічна відповідь на дезінформацію. *Медіаграмотність в Україні*. №2. 2022. С. 18–23.

Лапка Володимир-Андрій Петрович,
судовий експерт відділу автотехнічних досліджень лабораторії автотехнічних досліджень та криміналістичного дослідження транспортних засобів Київського НДЕКЦ МВС

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ СУДОВОГО ЕКСПЕРТА

У контексті стрімкої цифровізації суспільства та зростання кількості кіберзлочинів, судова експертиза зазнає суттєвих трансформацій. Традиційні

методи збору, обробки й аналізу доказової інформації вже не можуть забезпечити належну ефективність та точність у правозастосовній практиці. Сьогодні зростає потреба в обробці складних цифрових доказів, таких як електронні документи, відеозаписи, дані з мобільних пристроїв чи соціальних мереж. Водночас, використання інформаційних технологій (*далі* – ІТ) дозволяє автоматизувати рутинні процеси, скорочувати час проведення експертиз і забезпечувати стандартизацію методів аналізу. Це особливо важливо в умовах зростання кількості судових справ, що потребують експертного висновку, та підвищення вимог до якості й достовірності таких висновків.

Аналіз законодавства вказує на відсутність єдиного підходу до розуміння терміна «інформаційні технології». Так, у ДСТУ 5034:2008 під ІТ розуміється «сукупність методів, процесів і програмно-технічних засобів, об'єднаних у технологічний процес, що забезпечує добирання, зберігання, накопичування, оброблення, пошук, виведення, копіювання, передавання та розповсюджування інформації» (п.4.1.22) [1, с. 5]. У ДСТУ 2481-94 дане поняття розкривається через виконання функцій збирання, зберігання, оброблення, передавання та використання знань [2]. На законодавчому рівні фактично вперше даний термін було визначено у ст. 1 Закону України «Про Національну програму інформатизації» від 04.02.1998 року, де під ІТ розумілась «цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування» [3]. Даний Закон втратив чинність на підставі Закону України «Про Національну програму інформатизації» [4] де законодавець уже оперує поняттям «інформаційно-комунікаційні технології» під якими пропонується розуміти результат інтелектуальної діяльності, сукупність систематизованих наукових знань, технічних, організаційних та інших рішень про перелік та послідовність виконання операцій для збирання, обробки, накопичення та використання інформаційної продукції, надання інформаційних послуг(п.15 ч.1 ст.1).

Підсумовуючи вищевикладене, можна сказати, що Існуючі нормативні акти та стандарти в основному при тлумаченні ІТ зосереджуються на його функціональних аспектах (збирання, зберігання, обробка, передавання інформації), технічних засобах реалізації процесів або ж інтелектуальній складовій та організаційних рішеннях. В свою чергу. заміна у сучасному законодавстві поняття «інформаційні технології» на ширше «інформаційно-комунікаційні технології» (далі – ІКТ) свідчить про еволюцію підходів до регламентації цифрового середовища, інтеграцію комунікаційного компоненту та необхідність адаптації нормативного поля до динаміки розвитку цифрових технологій. Отже, формування єдиного визначення ІТ/ІКТ є актуальним завданням для подальшого вдосконалення законодавства у сфері інформаційного права.

Аналіз наукових джерел підтверджує відсутність єдиного, уніфікованого підходу до визначення поняття «інформаційні технології» у науковому дискурсі. Сучасні дослідники та автори навчальних посібників пропонують різні підходи

до тлумачення цього терміна, акцентуючи увагу на окремих аспектах – функціональному, технологічному, процесуальному або прикладному. Зокрема, одні автори підкреслюють роль ІТ як інструменту ефективної роботи з інформацією [5, с. 485; 6, с. 34], інші – як сукупності процесів, спрямованих на трансформацію первинної інформації в нову якість, або як складну систему методів і засобів, що забезпечують повний цикл роботи з інформацією, включаючи її захист і потенційне використання з різною метою [7, с.14; 8, с. 141; 9, с. 3]. Така розмаїтість підходів свідчить про багатогранність феномена інформаційних технологій і потребу в подальшому теоретичному узагальненні для формування комплексного, системного визначення, яке б відповідало сучасним науковим і практичним реаліям розвитку цифрового суспільства.

Незважаючи на відсутність уніфікованого наукового та законодавчого тлумачення поняття «інформаційні технології» необхідно констатувати, що з їх появою з'явилися нові можливості для підвищення ефективності, точності та швидкості виконання різноманітної діяльності, в тому числі і діяльності судових експертів.

Судова експертиза в Україні регулюється Законом України «Про судову експертизу» [10] та іншими нормативно-правовими актами. Вона охоплює різні види досліджень, зокрема криміналістичні, економічні, технічні, медичні тощо. ІТ у цьому контексті виступають як інструмент для автоматизації процесів, аналізу даних і забезпечення прозорості експертних висновків.

Впровадження інформаційних технологій у судово-експертну діяльність є ключовим чинником підвищення ефективності, об'єктивності та достовірності експертних досліджень. Особливої актуальності це питання набуло із початком повномасштабного вторгнення рф, значною активізацією використання цифрових засобів для ведення інформаційних війн, кібератак на критичну інфраструктуру, поширення дезінформації та інших злочинів, які мають цифровий слід. В цих умовах судовий експерт опиняється перед необхідністю не лише фіксувати та аналізувати електронні докази, а й оперативно реагувати на новітні виклики, пов'язані з використанням складних технічних засобів, шкідливого програмного забезпечення, технологій штучного інтелекту тощо.

Сьогодні інформаційні технології дозволяють автоматизувати процеси збору, обробки та аналізу даних, що сприяє зменшенню впливу людського фактора та підвищенню точності експертних висновків. Зокрема, використання спеціалізованого програмного забезпечення для обробки цифрових доказів, застосування методів комп'ютерної криміналістики та інтеграції штучного інтелекту у процес аналізу складних даних. Ці інновації дозволяють судовому експерта ефективно працювати з великими обсягами інформації, виявляти приховані закономірності та забезпечувати більш обґрунтовані висновки.

В загальному можна виділити наступні основні напрями застосування ІТ у судовій експертизі:

- *автоматизація процесів*: використання спеціалізованого програмного забезпечення для збору, обробки та аналізу великих обсягів даних. Це сприяє зменшенню впливу людського фактора та підвищенню точності експертних висновків. Так, для проведення деяких видів лінгвістичних експертиз, для

встановлення авторства, виявлення плагіату або автоматично згенерованих текстів виникає необхідність обробки та аналізу значного масиву даних. Відповідно, використання різноманітних інформаційних технологій значно спрощують даний процес.

- *цифрові докази*: аналіз інформації з електронних носіїв (комп'ютерів, смартфонів, хмарних сховищ). Зокрема, за допомогою спеціального програмного забезпечення судовий експерт може: відновлювати видалені файли; досліджувати структуру файлових систем; аналізувати журнал подій ОС; відслідковувати мережеву активність та ін.

Необхідно погодитись з О.Г. Козицькою яка наголошує на тому, що сьогодні цифрові докази вимагають новітніх підходів до їх збирання, зберігання, використання та дослідження. Особливого значення цифрова інформація набуває під час розслідування воєнних злочинів і використання технологій розвідки на підставі відкритих джерел (Open Source Intelligence, OSINT), які містять поради щодо фіксації цифрових доказів (цифрової інформації). Прикладом можуть слугувати й положення «Протоколу Берклі», які містять поради щодо фіксації цифрових доказів (цифрової інформації). При цьому «інформація у відкритому доступі може надавати підказки, підтримувати результати розвідки та служити прямим доказом у судах» [11, с. 65-66; 12].

- *електронні бази даних*: створення централізованих реєстрів для зберігання та швидкого доступу до експертної інформації. Зокрема, необхідно погодитись з , який наводить приклади успішного використання автоматизованих інформаційно-пошукових систем (далі – АІПС) у судово-експертних установах України: АІПС «ТАІС» і «Рикошет» – у балістичній експертизі; АІПС «Взуття» – у трасологічній експертизі; АІПС «Марка» для проведення експертиз лакофарбових матеріалів і покриттів; АІПС «Проволока» – в експертизі металів і сплавів та ін. и [13, с. 180 ; 14, с. 104]. Також у своїй діяльності судові експерти звертаються до різноманітних баз даних: електронні бази нормативно-правових актів; методик проведення експертиз; внутрішні інформаційні системи обліку та супроводу експертиз та ін.

- *візуалізація та моделювання*: використання 3D-моделей, віртуальної реальності для реконструкції подій. Так, 3D-моделювання та реконструкція подій широко застосовуються у трасології, автотехнічній експертизі, будівельно-технічних дослідженнях. Сучасні програми дозволяють моделювати місця події, траєкторії руху транспортних засобів чи інших об'єктів тощо. Зокрема, необхідно погодитись з Н. Мисковець, який наголошує на тому, що підвищеню якості виконання земельно технічних експертиз стало використання системи автоматизованого проектування (САПР) таких як (ArcGiS, QGiS, Digitals, GiS6 Pro, AutoCad) та закоординованих (виконаних в певній системі координат) картографічних матеріалів [15, с. 146].

Наголошуючи на позитивних моментах запровадження ІТ в діяльності судового експерта, необхідно також зазначити, що це вимагає і відповідної підготовки від останніх. Судові експерти не тільки повинні володіти сучасними ІТ інструментами, але й забезпечувати належний рівень кібербезпеки та захисту персональних даних.

Підсумовуючи вищевикладене, можна сказати, що сьогодні інформаційні технології є важливим інструментом діяльності судового експерта. За їх допомогою підвищується оперативність та об'єктивність експертних висновків. Однак, зважаючи на існуючі виклики, ефективність їх застосування залежить від вирішення ряду питань: законодавчого врегулювання питань роботи з цифровими доказами; створення уніфікованих методик для роботи з цифровими доказами; належне фінансування експертних установ та забезпечення їх сучасним обладнанням і програмним забезпеченням; створення належних умов забезпечення ефективного захисту цифрових доказів та ін.

Список використаних джерел

1. ДСТУ 5034:2008 «Науково-інформаційна діяльність. Терміни та визначення понять». Київ. Держспоживстандарт України. 2009. URL: https://metrology.com.ua/wpcontent/uploads/2015/04/images_ntd_dstu_5034_2008.zip)
2. ДСТУ 2481-94 Системи оброблення інформації. Інтелектуальні інформаційні технології. Терміни та визначення. Київ. Держстандарт України. 1994. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=79130
3. Про Національну програму інформатизації: Закон України від 04.02.1998 № 74/98-ВР. (втратив чинність від 01.03.2023, підстава – 2807-IX). URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text
4. Про Національну програму інформатизації: Закон України від 01.12.2022 № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text
5. Дубовик О.В. Інформаційні технології та їх роль в діяльності судових інстанцій. Електронне наукове видання «Аналітично-порівняльне правознавство». С. 485-492. URL: https://app-journal.in.ua/wp-content/uploads/2024/10/78.pdf
6. Томашевський О.М., Цегелик Г.Г., Вітер М.Б., Дудук В.І. Інформаційні технології та моделювання бізнес-процесів. Навч. посіб. К.: «Видавництво «Центр учбової літератури», 2012. 296 с.
7. Інформаційні технології : навчальний посібник / О.І. Зачек, В.В. Сеник, Т.В. Магеровська та ін.; за ред. О.І. Зачека. Львів : Львівський державний університет внутрішніх справ, 2022. 432 с.
8. Макоєдова В.О. Аналіз принципів побудови та підходів до визначення поняття «інформаційна технологія». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»,* 2022. № 2(18). С. 138–149
9. Kukhareva P.V., Weir C., Del Fiol G., Aarons G.A., Taft T.Y., Schlechter C.R., Reese T.J., Curran R.L., Nanjo C., Borbolla D., Staes C.J., Morgan K.L., Kramer H.S., Stipelman C.H., Shakib J.H., Flynn M.C., Kawamoto K. Evaluation in Life Cycle of Information Technology (ELICIT) framework: Supporting the innovation life cycle from business case assessment to summative evaluation. Journal of Biomedical Informatics, 2022. № 127. URL: https://doi.org/10.1016/j.jbi.2022.104014
10. Про судову експертизу: Закон України від 25.02.1994 № 4038-XII. URL: https://zakon.rada.gov.ua/laws/show/4038-12?find=1&text=%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%

B0%D1%86%D1%96%D0%B9%D0%BD%D0%B5#w1_1

11. Шепітько В.Ю., Авдєєва Г.К., Шевчук В.М., Капустіна М. В., Яремчук В.О., Негребецький В.В., Соколенко М.О., Пугач А.О. Інноваційні методи та цифрові технології в криміналістиці та судовій експертизі / Питання боротьби зі злочинністю : зб. наук. пр. / редкол.: В.С. Батиргареєва (голов. ред.) та ін. Харків: Право, 2024. Вип. 48. 202с. С. 65-66. URL: http://pbz.nlu.edu.ua/issue/view/18894

12. Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних : практичний посібник з ефективного використання відкритих цифрових даних у розслідуванні порушень міжнародного кримінального права, прав людини та міжнародного гуманітарного права. ООН. Права людини. Канцелярія Верховного комісара URL: https:// www.law.berkeley.edu/wp-content/uploads/2022/03/BerkeleyProtocol-Ukrainian.pdf

13. Петрова І., Кіпушева Т., Духненко Д.С. Автоматизація проведення судових експертиз як складова комплексного розвитку експертного забезпечення правосуддя // Scientific Foundations of State and Law: collective monograph / Karpova N., Piestsov R., Makarova O., Konchakovska V., Karnaukh A. – etc. – International Science Group. – Boston : Primedia eLaunch, 2022. 316 p. 174- 183. URL: https://isg-konf.com/wp-content/uploads/2022/06/Monograph/Doi/Legal/ISG.2022.MONO.LEGAL.2.7.2.pdf

14. Журавель В. А., Коновалова В. О., Шепітько В. Ю. Практикум з криміналістики : навч. посіб. Київ, 2013. 128 с.

15. Мисловець Н. Застосування методик та методичних рекомендацій при проведенні земельно технічних експертиз: від традиційних методів до цифрової трансформації. / Вплив інновацій на розвиток судової експертизи: від традиційних методів до цифрової трансформації: Матеріали Всеукраїнської науково-практичної конференції (м. Львів, 26 квітня 2024 року) / Укладачі: Зелінська М.Б., Хомич Н.П., Грицишин П.М., Чабанюк О.М. Л.: ЛНДІСЕ МЮ України, 2024. 219 с. С. 144-149. URL: http://ndekc.lviv.ua/pdf/19062024.pdf

Лапка Оксана Ярославівна,
доцент кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат юридичних наук, доцент
Назаренко Ольга Анатоліївна,
старший викладач кафедри теорії, історії та філософії права навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ

В умовах стрімкої цифровізації суспільства та зростання загроз у кіберпросторі проблема забезпечення інформаційної безпеки набуває виняткової актуальності. Сьогодні фішинг, шкідливе програмне забезпечення, атаки типу відмова в обслуговуванні (DDoS), атаки нульового дня та розширені стійкі загрози (APT) створюють серйозні виклики для держав. Традиційні методи захисту, такі як антивірусні програми чи системи виявлення вторгнень, стають менш ефективними через швидке вдосконалення технік кібератак. У цьому контексті штучний інтелект (далі – ШІ) відкриває нові можливості для виявлення, аналізу та нейтралізації кіберзагроз. Однак використання ШІ у сфері інформаційної безпеки супроводжується й низкою викликів, що потребують ґрунтовного аналізу.

Інформаційне середовище сьогодні охоплює не лише класичні комп'ютерні мережі, а й Інтернет речей, хмарні сервіси, мобільні пристрої, що ускладнює управління ризиками. Основні виклики включають: зростання кількості та складності кібератак; використання соціальної інженерії; поява нових типів шкідливого програмного забезпечення; вразливість критичної інфраструктури [1, с. 118]. У таких умовах потреба в інтеграції ШІ в системи кібербезпеки є об'єктивною та невідкладною.

Серед ключових переваг застосування штучного інтелекту в інформаційній безпеці варто виокремити його здатність швидко аналізувати великі обсяги даних, виявляти закономірності, аномалії та потенційні загрози [2; 3, с. 381].

Штучний інтелект – це сукупність технологій, що дозволяють інформаційним системам імітувати людський інтелект, зокрема в аспектах навчання, аналізу, прогнозування й ухвалення рішень [4, с. 24]. У сфері інформаційної безпеки ШІ застосовується для:

–для автоматичного аналізу великої кількості даних, що надходять з різних джерел,

–для виявлення неправдивої інформації,

–для розпізнавання змінених (підроблених) зображень шляхом порівняння їх з оригінальними,

–для встановлення принципів, схем і способів поширення дезінформації,

–для блокування виявленої дезінформації [5, с. 64].

–аналізу поведінки користувачів з метою виявлення відхилень (User and Entity Behavior Analytics, UEBA);

–виявлення вторгнень (IDS/IPS) на основі машинного навчання;

–прогнозування кіберзагроз шляхом обробки великих обсягів даних;

–реалізацію адаптивного захисту, що автоматично змінює політики безпеки залежно від контексту загрози [6].

Швидке зростання ринку ШІ у сфері кібербезпеки підтверджують дані MarketsandMarkets: очікується, що з 2019 до 2026 року його обсяг зростатиме на 23,3% щороку – з 8,8 до 38,2 млрд доларів США [3], с. 384 Компанія Gartner прогнозує, що до 2025 року понад 80% організацій впровадять ШІ у свої системи інформаційного захисту [7]. Це зумовлено зростаючою вразливістю цифрового середовища та обмеженістю традиційних механізмів захисту.

Україна активно долучається до процесів цифрової трансформації та розвитку технологій ШІ. Прийнята Стратегія кібербезпеки України передбачає створення стабільного та безпечного кіберпростору як гарантії прав і свобод громадян [8]. Водночас Концепція розвитку штучного інтелекту [9] визначає ключові напрямки розвитку цієї технології задля підвищення конкурентоспроможності держави та ефективності публічного управління. Ратифікація Угоди між Україною та Європейським Союзом про участь у програмі ЄС «Цифрова Європа» [10] відкриває Україні доступ до інструментів розвитку цифрової економіки, зокрема штучного інтелекту.

Поряд з позитивними моментами необхідно наголосити і на певних ризиках використанні ШІ:

- непрозорість алгоритмів (чорна скринька);
- можливість використання ШІ для атак (deepfake, генерація шкідливого коду);
- ризик дискримінації через упередженість даних [11; 12, с. 207];
- витік даних (ШІ-системи можуть використовуватися для крадіжки даних або зловживання ними, йдеться про особисту чи фінансову інформацію, а також комерційну таємницю);
- упередженість (ШІ-системи можуть бути упередженими, що може призвести до дискримінації або несправедливого ставлення до певних груп людей) [13, с. 92].

Ці виклики потребують створення ефективної нормативно-правової бази, яка забезпечить прозорість і підзвітність систем ШІ, збереження прав людини в цифровому середовищі та контроль за автоматизованими рішеннями.

Підсумовуючи вищевикладене, можна сказати, що штучний інтелект має значний потенціал у сфері інформаційної безпеки. Його застосування дозволяє підвищити рівень автоматизації, ефективності та адаптивності захисних систем. Водночас, для повноцінного та безпечного впровадження технологій ШІ необхідно забезпечити: формування чіткої нормативно-правової основи; дотримання етичних принципів; створення механізмів зовнішнього моніторингу; забезпечення прозорості роботи алгоритмів. Відповідно, розвиток штучного

інтелекту в Україні має здійснюватися на засадах безпеки, відповідальності та міжнародної співпраці, що дозволить не лише ефективно протидіяти сучасним загрозам, а й сприяти сталому розвитку цифрового суспільства.

Список використаних джерел

1. Слюсар В.І. Загрози інформаційній безпеці в умовах гібридної війни. *Захист інформації*. 2022. № 1. С. 117–123.
2. Котенко Д., Хлапонін Ю. Штучний інтелект у системах виявлення і запобігання кібератакам: перспективи та виклики. *Підводні технології: промислова та цивільна інженерія*. 2024. №1(14), С. 48–55.
3. Лунгол О.М. Огляд методів та стратегій кібербезпеки засобами штучного інтелекту. *Кібербезпека: освіта, наука, техніка*. 2024. № 1 (25). С. 379-389. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/632/523
4. Мальцев В.А. Штучний інтелект у цифровій трансформації: базові підходи і виклики. *Інформаційні технології і безпека*. 2021. № 2. С. 21–28.
5. Воропаєва Т.С., Авер'янова Н.М. Штучний інтелект в системі інформаційної безпеки України в умовах російсько-української війни. / Collection of scientific papers «SCIENTIA»: Scientific forum: theory and practice of research. August 23, 2024. Valencia, Kingdom of Spain. P. 62-67.
6. Хома І.О. Інтелектуальні системи кіберзахисту: сучасний стан і перспективи розвитку. *Кібербезпека: освіта, наука, техніка*. 2023. № 4(16). С. 45–52.
7. Gartner. Top Security and Risk Trends in 2023 URL: https://www.gartner.com/en/articles/top-security-and-risk-trends-in-2023
8. Про Стратегію кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text
9. Концепція розвитку штучного інтелекту: Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text
10. Угода між Україною та Європейським Союзом про участь України у програмі Європейського Союзу "Цифрова Європа" (2021 - 2027): Угода. Міжнародний документ від 05.09.2022. URL: https://zakon.rada.gov.ua/laws/show/984_005-22#Text
11. Кириленко Л.А. Етичні та правові аспекти використання штучного інтелекту в системах захисту інформації. *Правова держава*. 2021. Вип. 32. С. 91–98.
12. Бабич О.В. Правові та етичні аспекти впровадження штучного інтелекту. *Інформаційне право України*. 2023. № 3. С. 200–210.
13. Примиська С.О., Кримська А.О., Супрун О.М. Стратегії забезпечення безпеки даних у системах штучного інтелекту. *Таврійський науковий вісник*. 2024. № 2. С. 88-99.

Лапка Оксана Ярославівна,
доцент кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат юридичних наук, доцент
Прилуцька Крістіна Вікторівна,
курсант навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

Інформаційна безпека є критично важливим аспектом сучасного суспільства, особливо в умовах воєнного стану, коли загрози кібератак, дезінформації та шпигунства набувають стратегічного значення. В Україні, де воєнний стан діє з 24 лютого 2022 року, забезпечення інформаційної безпеки стало одним із пріоритетів національної безпеки.

Доктрина інформаційної безпеки України визначає інформаційну безпеку як важливу самостійну сферу забезпечення національної безпеки [1]. Указом Президента України № 685/2021 від 15.10.2021 р. було схвалено Стратегію інформаційної безпеки [2]. Її метою є регулювання інформаційної безпеки на нормативно-правому рівні, посилення можливостей щодо забезпечення інформаційної безпеки України, інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, охорони суверенітету та цілісності України, демократії, прав та свобод людини і громадянина. Таким чином закладалися основи національної та інформаційної безпеки в інформаційній сфері [3, с. 51].

Інформаційна безпека – це стан, за якого в умовах дії реальних і потенційних загроз забезпечується самозбереження, сталий та прогресивний розвиток інформаційної сфери, в тому числі захищеність інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, інформаційних процесів та їх суб’єктів, а також досягнення відповідних національних цілей та реалізація національних інтересів в інформаційній сфері [4, с. 77-78; 5, с. 411].

Необхідно погодитись з У. Андрусів, який наголошує на тому, що під час воєнного стану інформація стає не лише ресурсом, а й засобом ведення війни. Посиленими є кібер- та інформаційна активність ворога, збільшуються масовані інформаційні атаки, широко використовуються соціальні мережі, перш за все для дестабілізації громадської думки та ін. За таких умов інформаційна безпека охоплює не лише технічні аспекти, а й стратегічну комунікацію, контрпропаганду, контроль над інформаційними потоками [6, с. 33].

Відповідно до ДСТУ ISO/IEC 29146:2023 «Інформаційні технології. Методи безпеки. Структура керування доступом» [7], методи захисту інформаційних систем включають організаційні, технічні та фізичні заходи, спрямовані на управління ризиками інформаційної безпеки.

У контексті воєнного стану особливу увагу приділяється методам, які дозволяють ефективно реагувати на динамічні загрози. Зокрема серед них доречно виділити:

❖ Правові методи – базуються на законодавстві України, зокрема, Законах України: «Про захист інформації в інформаційно-телекомунікаційних системах» [8], «Про державну таємницю» [9] та «Про захист персональних даних» [10], Закон України «Про основні засади забезпечення кібербезпеки України» [11]. Ці акти формують законодавчу основу, яка визначає правила обігу інформації, права суб'єктів, обов'язки операторів та порядок реагування на кіберінциденти.

❖ Організаційні методи – передбачають створення структур і процедур, спрямованих на управління інформаційною безпекою. Вони включають розробку політик безпеки, навчання та аудит інформаційних систем. У воєнний час до таких методів належать:

- *розробка політики безпеки*. В Україні створюються комплексні системи захисту інформації, які відповідають вимогам законодавства та міжнародним стандартам.
- *навчання та інструктажі*. Проведення тренінгів для працівників щодо кібергігієни, зокрема уникнення фішингових атак, є критично важливим в умовах воєнного стану.
- *аудит і контроль*. Регулярний аудит інформаційних систем дозволяє виявляти порушення та вдосконалювати заходи безпеки [12, с. 56].

❖ Технічні методи – охоплює застосування засобів технічного захисту інформації. Вони включають використання апаратних і програмних засобів для захисту інформації. До таких методів відносять:

- *антивірусний захист*. Використання сучасних антивірусних програм дозволяє виявляти та нейтралізувати шкідливе програмне забезпечення.
- *криптографічний захист* (шифрування даних, електронний цифровий підпис). Зокрема, шифрування є ключовим методом захисту інформації під час її передачі та зберігання. Особливо важливим даний метод є для захисту комунікацій між військовими підрозділами, державними органами.
- *резервне копіювання та відновлення даних*;
- *системи контролю доступу й логування* для обмеження прав доступу та фіксації дій користувачів;
- *багатофакторна аутентифікація* для посиленої перевірки особистості [13].

Розвиток технологій на основі штучного інтелекту і машинного навчання також відкриває нові можливості у виявленні та реагуванні на загрози [14].

❖ Інформаційні методи – спрямовані на протидію дезінформації та інформаційним впливам, які є частиною гібридної війни. До них належать:

- *моніторинг інформаційного простору*. Виявлення дезінформаційних кампаній та їх нейтралізація.
- *проведення інформаційних кампаній*. Зокрема, актуальним є проведення роз'яснення громадянам правил кібергігієни та процедур реагування на кіберзагрози.

❖ Соціальні та психолого-комунікаційні методи. Зокрема, соціальні методи ґрунтуються на розумінні поведінки користувачів у цифровому середовищі [15]. Для забезпечення інформаційної безпеки важливим є врахування людського чинника. Основними заходами є:

- формування навичок цифрової гігієни;
- психологічна діагностика та профілактика внутрішніх загроз.

Ефективне забезпечення ІБ вимагає комплексного підходу, що передбачає взаємодію між усіма методами. Слушною з цього питання є і позиція, яка наголошує на тому, що в умовах воєнного стану інформаційна безпека України має базуватися на синхронізованих діях різних структур держави та громадянського суспільства [3, с. 55]. Доречним, на наш погляд, є використання штучного інтелекту для загроз та автоматизації захисту. Також важливим є обмін досвідом та технологіями з державами-партнерами, міжнародними організаціями.

Підсумовуючи вищевикладене, можна сказати, що забезпечення інформаційної безпеки в умовах воєнного стану є комплексним завданням, яке вимагає поєднання технічних, організаційних, правових та інформаційних методів. Сучасні методи інформаційної безпеки мають адаптуватися до нових викликів, таких як кіберзагрози, гібридні впливи, зростання ролі соціальних мереж. Ключем до успіху є постійне оновлення знань, інтеграція технологій та активна участь усіх суб’єктів інформаційного середовища.

Список використаних джерел

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року № 47/2017 URL: https://zakon.rada.gov.ua/laws/show/47/2017#n2
2. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7
3. Мазуренко Л.І. Інформаційна безпека в умовах російсько-української війни: виклики та загрози. *Вісник Харківського національного університету імені В. Н. Каразіна*, Серія «Питання політології», 2022. Випуск 42. С. 50-57.
4. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України : дис… д-ра. юрид. наук : 12.00.07. Ужгород. 2019. 487 с.
5. Моргун Н.С., Шевчук О.О., Марчевський С.В. Щодо визначення поняття інформаційної безпеки у діяльності Національній поліції України. *Електронне наукове видання «Аналітично-порівняльне правознавство».* С. 409-415. URL: https://app-journal.in.ua/wp-content/uploads/2024/08/69.pdf
6. Андрусів У. Інформаційна безпека в умовах війни: нові виклики і відповіді. *Інформаційне право України*. 2023. № 1. С. 31–35.
7. Про прийняття національних стандартів, зміни до національного стандарту та скасування національних стандартів: Наказ ДП"УкрНДНЦ" від 17.08.2023 № 210. URL: https://zakon.rada.gov.ua/rada/show/v0210774-23#Text

8. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
9. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
10. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
11. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
12. Бачинська О. А. Організаційні аспекти забезпечення інформаційної безпеки в Україні. *Держава та регіони. Серія: Право*. 2022. № 1. С. 55–59.
13. Інформаційна безпека: що це таке, види та засоби захисту. https://voll.kiev.ua/uk/blog/informacijna-bezpeka-sho-ce-take-vidi-ta-zasobi-zahistu
14. Yakimenko I., Yermakov V. AI and ML in Cybersecurity: Opportunities and Risks. *Cybersecurity Journal*. 2023. Vol. 9№. 2. P. 33–39.
15. Садовська І. Психологічні аспекти інформаційної безпеки. *Психологія і суспільство*. 2021. № 2. С. 78–84.
16. Мазуренко Л.І. Інформаційна безпека в умовах російсько-української війни: виклики та загрози. *Вісник Харківського національного університету імені В. Н. Каразіна,* Серія «Питання політології», 2022, випуск 42. С. 50-57.

Лапка Оксана Ярославівна,
доцент кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат юридичних наук, доцент
Трофимчук Дарія Юріївна,
курсант навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ

ОБМЕЖЕННЯ СВОБОДИ СЛОВА ТА ІНФОРМАЦІЙНИХ ПРАВ ГРОМАДЯН ПІД ЧАС ВОЄННОГО СТАНУ

Свобода слова та право на інформацію є фундаментальними складовими демократичного суспільства, закріпленими як у національному законодавстві, так і в міжнародно-правових актах. Однак, в умовах війни, держава може обґрунтовано застосовувати обмеження на ці права задля захисту національної безпеки, суспільного порядку та обороноздатності. Такі обмеження мають тимчасовий характер і повинні відповідати принципам пропорційності, необхідності та законності.

Право на свободу вираження поглядів гарантується статтею 34 Конституції України [1], а також статтею 10 Конвенції про захист прав людини і

основоположних свобод [2]. Воно включає право вільно отримувати, поширювати та зберігати інформацію. Разом з тим, дані акти передбачають і можливість обмеження цього права. Так, у ч. 3 ст. 34 Основного Закону встановлено, що в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя, здійснення права на свободу слова може бути обмежене законом [1]. Можливість тимчасового обмеження конституційних прав, зокрема свободи слова та інформаційної діяльності, передбачено і у Законі України «Про правовий режим воєнного стану» [3].

Запровадження 24.02.2022 року в Україні воєнного стану, відповідно до п. 3 Указу Президента України №64/2022 [4] встановлює тимчасові обмеження окремих конституційних прав і свободи людини і громадянина. Зокрема, прямо вказується на можливість обмеження прав, передбачених статтею 34 Конституції України [1]. Такі обмеження виправдовуються необхідністю захисту національної безпеки та громадського порядку.

В теорії права на інформацію виділяються два основні аспекти:

– свобода доступу до інформації – право кожного громадянина отримувати інформацію, яка необхідна для усвідомленої участі в суспільному житті, ухваленні рішень та контролю за владою;

– обмеження права на інформацію – необхідність встановлення розумних обмежень на доступ до інформації в інтересах захисту національної безпеки, державної таємниці, приватності або інших правомірних інтересів [5; 6, с. 84].

Під час воєнного стану держава може запроваджувати обмеження на діяльність ЗМІ, зокрема через регулювання роботи телерадіоорганізацій, видавництв та інших інформаційних установ. Наприклад, стаття 8 Закону України «Про правовий режим воєнного стану» [3] дозволяє вводити цензуру, обмежувати поширення певної інформації або забороняти діяльність медіа, якщо їхня діяльність загрожує національній безпеці. Такі заходи можуть включати заборону на поширення інформації, що може сприяти паніці, дезінформації чи підриву обороноздатності країни.

У практиці воєнного стану в Україні з 2022 року спостерігалися випадки тимчасового обмеження доступу до певних інформаційних ресурсів, які вважалися такими, що можуть використовуватися для поширення пропаганди або дезінформації. Наприклад, було заборонено трансляцію низки російських телеканалів та обмежено доступ до певних інтернет-ресурсів.

Закон України «Про доступ до публічної інформації» від 13 січня 2011 року [7] встановлює презумпцію відкритості інформації, однак у період воєнного стану доступ до певних даних може бути обмежено. Зокрема, розпорядники інформації можуть відмовляти в наданні інформації, якщо її розголошення може завдати шкоди національній безпеці або територіальній цілісності. Такі відмови мають бути обґрунтованими, а причинно-наслідковий зв'язок між розголошенням інформації та можливою шкодою чітко доведеним.

Свобода вираження поглядів, закріплена в статті 34 Конституції України [1], може обмежуватися через заборону на проведення масових заходів, мітингів чи демонстрацій, що також є частиною інформаційних прав громадян. Указ Президента № 64/2022 [4] передбачає можливість таких обмежень, якщо вони необхідні для забезпечення громадського порядку та безпеки. Наприклад, у період воєнного стану в Україні заборонено проведення масових акцій, що може розглядатися як обмеження права на публічне вираження думки.

Необхідно погодитись з А.С. Чистяковою та Д.В. Костенко, які наголошують на тому, що обмеження повинні бути чітко обґрунтовані, пропорційними та передбаченими законом, аби уникнути необґрунтованого порушення прав громадян [6, с. 84]. На цьому наголошується і у Європейській конвенції з прав людини, де встановлено вимогу, щоб обмеження прав були пропорційними, законними та необхідними в демократичному суспільстві. У контексті воєнного стану це означає, що обмеження свободи слова та інформаційних прав мають бути чітко обґрунтованими, обмеженими в часі та спрямованими виключно на досягнення легітимної мети, такої як захист національної безпеки. Верховний Суд України наголошує, що такі обмеження повинні бути виваженими та не порушувати основоположних прав людини [8].

Незважаючи на воєнний стан, громадяни зберігають право на судовий захист своїх прав і свобод (стаття 55 Конституції України [1]). Це включає можливість оскарження незаконних обмежень свободи слова чи доступу до інформації. Наприклад, громадяни можуть звертатися до національних судів або Європейського суду з прав людини, якщо вважають, що їхні права були порушені без належного обґрунтування.

Обмеження свободи слова та інформаційних прав можуть створювати виклики для громадянського суспільства, зокрема через обмеження діяльності громадських організацій, ЗМІ та активістів. Такі обмеження можуть призводити до зниження рівня прозорості влади та ускладнення громадського контролю за її діями. Водночас, як зазначає правозахисник Володимир Чемерис, обмеження громадянських свобод у воєнний час можуть сприйматися як необхідна ціна за безпеку, але потребують чіткого правового регулювання та контролю [9].

Для мінімізації таких ризиків держава має забезпечувати

- *прозорість обмежень* – усі обмеження свободи слова та інформаційних прав повинні супроводжуватися чітким обґрунтуванням і публікацією відповідних нормативних актів.
- *тимчасовість заходів* – обмеження мають бути чітко обмеженими в часі та скасовуватися після усунення загрози.
- *судовий контроль* – необхідно забезпечити ефективний механізм судового оскарження незаконних обмежень.
- *інформування громадян* – органи влади повинні активно інформувати громадян про їхні права та можливості захисту, зокрема через офіційні веб-ресурси та соціальні мережі.

Підсумовуючи вищевикладене, можна сказати, що обмеження свободи слова та інформаційних прав громадян під час воєнного стану в Україні є правомірним інструментом. Однак, такі обмеження повинні відповідати

принципам пропорційності, законності та необхідності, а також міжнародним стандартам прав людини.

Список використаних джерел

1. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
2. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини): Конвенція. Рада Європи. Міжнародний документ від 04.11.1950. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text.
3. Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text.
4. Про введення воєнного стану в Україні: Указ Президента України від 24.02.2022. № 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text
5. Любовець Г. Контент негативу. Як захистити себе та країну в умовах тотального інформаційного протистояння : монографія / Григорій Любовець, Валерій Король. Київ : Видавничий дім «Києво-Могилянська академія», 2021. 266 с.
6. Чистякова А.С., Костенко Д.В. Трансформація права на інформацію в умовах воєнного часу. *Legal Bulletin.* 2024. № 4 (14). С. 81-90. URL: https://lbku.krok.edu.ua/index.php/legal-bulletin/article/view/501/443.
7. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.
8. Обмеження конституційних прав людини у воєнний час мають бути виваженими, законними і легітимними. *Верховний Суд України.* 2022. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1286958/
9. Чемерис В. Воєнний стан і права людини: взаємозв'язок. Інститут «Республіка». 2018. URL: https://inrespublica.org.ua/voiennyi-stan-i-prava-liudyny-vzaiemozv-iazok/

Лупало Олександр Анатолійович,
професор кафедри адміністративно-правових дисциплін навчально-наукового інституту права та психології НАВС, кандидат юридичних наук, доцент

СИНЕРГЕТИЧНИЙ ПІДХІД У СИСТЕМІ НАКЛАДАННЯ АДМІНІСТРАТИВНИХ СТЯГНЕНЬ: МІЖНАРОДНИЙ ДОСВІД ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ В УКРАЇНІ

Сучасні виклики у сфері запобігання адміністративним правопорушенням потребують переосмислення ролі адміністративного права – не лише як системи фіксації й покарання, а як механізму ефективного впливу на правосвідомість

громадян. Згідно зі статтею 23 Кодексу України про адміністративні правопорушення, адміністративне стягнення є «мірою відповідальності, що застосовується з метою виховання особи, яка вчинила правопорушення, у дусі додержання законів України, поваги до правил співжиття, а також запобігання вчиненню нових правопорушень як самим порушником, так і іншими особами» [1, с. 13]. Втім, постає питання: чи справді чинний Кодекс передбачає ефективний набір інструментів, здатних реалізувати ці завдання – виховати особу, запобігти повторному правопорушенню, сформувати у неї повагу до правопорядку? Очевидно, що механізми, які домінують у національній правозастосовній практиці, є переважно каральними, формальними і не враховують індивідуальні особливості правопорушника. Іншими словами, застосування адміністративних стягнень, які визначені в КУпАП, не дозволяють досягти повною мірою поставлених ним же завдань.

Натомість у правових системах багатьох європейських держав відбувається зміщення акцентів із покарання на відновлення та зміну поведінки, де адміністративне стягнення розглядається не лише як реакція на правопорушення, а як комплексний інструмент ресоціалізації, просвітництва та профілактики. В цьому контексті дедалі більшої актуальності набуває впровадження синергетичного підходу, який дозволяє поєднувати адміністративні, соціальні, освітні та поведінкові заходи впливу для досягнення максимально сталого правового результату.

За визначенням, поданим у "Філософському енциклопедичному словнику":

Синергетика (від грец. συνεργία - «співпраця, узгодженість дій») – це напрям міждисциплінарного наукового знання, що виник на межі фізики, хімії, біології, кібернетики, який вивчає загальні закономірності самоорганізації структур у відкритих системах [2, с. 606]. Синергетика широко застосовується не лише у фізичних і біологічних науках, а також у соціології, політології, менеджменті та правознавстві. У сфері права цей підхід використовується для посилення ефективності складних соціально-правових систем, де взаємодія норм, інституцій та поведінкових практик створює нову якість правового регулювання.

У правовому полі цей принцип означає, що поєднання адміністративних стягнень з іншими заходами впливу (адміністративних санкцій, освітніх, соціальних заходів, інформаційної підтримки) може дати значно кращий результат, ніж проста ізольована адміністративна санкція [3]. І, сучасні правоохоронні органи закордонних країн вже ефективно застосовують їх в своїй діяльності.

Так, у 2016 році в окрузі Лаудон, штат Вірджинія, п’ятеро підлітків віком 16–17 років були визнані винними у вандалізмі – нанесенні расистських графіті на історичну будівлю школи для афроамериканців. Прокурорка Алехандра Руеда запропонувала альтернативне покарання: замість традиційного ув’язнення підлітки мали прочитати 12 книг із запропонованого списку з 35 творів, що висвітлюють теми расизму, дискримінації та соціальної справедливості (зокрема, «Убити пересмішника» Гарпер Лі, «Колір пурпуровий» Еліс Вокер). Кожен мав написати есе після прочитання кожної книги, відвідати Меморіальний музей Голокосту та виставку про інтернування японських

американців, а також написати підсумкове есе про отримані уроки. Результати показали, що жоден з підлітків не вчинив повторного правопорушення, а їхні есе свідчили про глибоке усвідомлення шкоди, завданої їхніми діями [4]. У правовому полі цей принцип означає, що поєднання кількох видів впливу (санкцій, освітніх, соціальних заходів, інформаційної підтримки) може дати значно кращий результат, ніж проста ізольована санкція.

Водночас, пошук оптимальних адміністративно-правових заходів впливу на правопорушника є багатофакторним і комплексним процесом, що вимагає обов'язкового врахування вікових, освітніх, світоглядних характеристик особи, її соціального досвіду та виховного середовища. У 2021 році Бен Джон, 21-річний студент з Лестера, був засуджений за зберігання майже 70 000 документів з неонацистською та праворадикальною пропагандою. Суддя Тімоті Спенсер призначив йому умовне покарання з умовою читання класичної англійської літератури, включаючи твори Джейн Остін, Чарльза Діккенса, Вільяма Шекспіра та Томаса Гарді. Бен мав повертатися до суду кожні чотири місяці для перевірки знань з прочитаного. Однак після того, як він порушив умови вироку, Апеляційний суд скасував умовне покарання і призначив реальне ув'язнення.[5]

У Франції обов'язкові курси безпеки дорожнього руху можуть бути призначені як додатковий або альтернативний захід у разі порушення правил дорожнього руху. Таке зобов'язання має право накладати як адміністративний орган, так і суд. Проходження курсу обов'язкове у визнаному навчальному центрі, програма якого включає інтерактивну участь у модулях, симуляції ситуацій, рольові вправи та письмове тестування. Фінансування навчання покладається на правопорушника, що також виконує стимулюючу функцію.

Результатом проходження курсу є не лише формальна оцінка знань, а й індивідуальна оцінка рівня свідомості ризику – здатності особи усвідомлювати наслідки своєї поведінки на дорозі. У разі ухилення від проходження курсу передбачено додаткові санкції, включаючи адміністративну заборону на керування транспортним засобом [6]

Ці приклади засвідчують, що тенденція до пошуку комплексних, поєднаних підходів до правопорушників стає все більш поширеною у демократичних юрисдикціях. Рішення, в яких санкція поєднується з інтелектуальним, моральним або соціальним впливом, сприяють більш глибокому усвідомленню особою наслідків своїх дій. Проте такий підхід потребує чітких меж застосування, оцінки мотиваційних причин правопорушника, рівня ризику та контролю з боку відповідних органів. Саме в цьому контексті синергетичний підхід набуває не лише педагогічної, а й правової цінності як форма цілеспрямованої ресоціалізації.

Таким чином, застосування до правопорушників лише каральних заходів поступово втрачає ефективність. У сучасних умовах дедалі актуальнішим стає формування комплексної моделі відповідальності за вчинене правопорушення, що зосереджується не лише на факті вчинення правопорушення, а й на зміні поведінкових установок правопорушника.

Підвищення ефективності адміністративного впливу на правопорушника можливе шляхом інтеграції різних механізмів впливу – юридичних,

психологічних, соціальних та інформаційних, - які в комплексі забезпечують не лише покарання за вчинене правопорушення, а й сприяють стійкій зміні поведінкових установок особи в подальшому. Водночас обов'язковою умовою досягнення цієї мети є індивідуалізація впливу шляхом врахування особливостей правопорушника та характеру вчиненого діяння. Зокрема, необхідно брати до уваги тип правопорушення, вік особи, її соціальний статус, рівень освіти, мотиваційні чинники, що сприяли вчиненню правопорушення, а також інші важливі особистісні характеристики. Впровадження синергетичного підходу у сферу застосування адміністративних стягнень відкриває нові можливості для підвищення ефективності правового впливу на правопорушників. Зокрема, такий підхід дозволяє:

1. формувати багаторівневу систему адміністративної відповідальності, яка поєднує не лише елементи покарання, а й заходи превентивного, виховного та ресоціалізаційного характеру. Це сприяє не просто реагуванню на факт правопорушення, а й цілеспрямованому коригуванню поведінкових моделей особи;
2. інтегрувати адміністративне покарання із соціальними, освітніми та психологічними заходами впливу, що дозволяє створити цілісну систему впливу, орієнтовану на глибинні зміни правосвідомості правопорушника та його мотиваційних установок;
3. забезпечити залучення громадськості, органів місцевого самоврядування, освітніх установ, громадських організацій, цифрових сервісів і аналітичних платформ до процесу реалізації адміністративних рішень, що сприяє підвищенню прозорості, підзвітності та ефективності заходів адміністративного впливу;
4. індивідуалізувати адміністративний вплив, тобто адаптувати заходи до конкретних особистісних характеристик правопорушника, таких як вік, рівень освіти, соціальний статус, життєві обставини, мотиваційні фактори, а також ступінь ризику рецидиву та потенціал успішної ресоціалізації.

Загалом застосування синергетичного підходу дозволяє побудувати адміністративно-правову модель, що спирається на комплексний, багатофакторний і системний вплив на правопорушника, орієнтований не лише на відновлення правопорядку, а й на формування стійких правосвідомих поведінкових орієнтацій у суспільстві.

Потрібно погодитися, що чинний КУпАП не забезпечує в повній мірі досягнення визначених ним же завдань у сфері провадження в справах про адміністративні правопорушення. Так, відповідно до статті 245 Кодексу, завданнями провадження є: «своєчасне, всебічне, повне і об'єктивне з'ясування обставин кожної справи, вирішення її в точній відповідності з законом, забезпечення виконання винесеної постанови, а також виявлення причин та умов, що сприяють вчиненню адміністративних правопорушень, запобігання правопорушенням, виховання громадян у дусі додержання законів, зміцнення законності» [1].

Однак на практиці перелік адміністративних стягнень, передбачених чинним законодавством, обмежений і не дозволяє повною мірою досягти цих

цілей. Зокрема, він не враховує індивідуальні особливості правопорушника, характер вчиненого діяння та соціальний контекст його вчинення. Це створює підстави необхідності для запровадження більш гнучкої, адаптивної та виховної системи адміністративно-організаційного впливу.

Таким чином, доцільно впроваджувати ширший спектр альтернативних заходів, які можуть реально забезпечити виконання завдань провадження – зокрема, виявлення причин та умов, що сприяють правопорушенням, їх запобігання, а також виховання громадян у дусі поваги до закону й правопорядку.

Такі заходи мають значний потенціал для формування правосвідомості, особливо серед молоді та першоразових порушників.

Законодавство України вже допускає деякі альтернативи (позбавлення права керування транспортними засобами, позбавлення права обіймати певні посади або займатися певною діяльністю тощо), однак залишається жорстко формалізованим. На наш погляд, включення до Кодексу України про адміністративні правопорушення нової статті, яка передбачала б можливість застосування додаткових заходів впливу у поєднанні з адміністративними стягненнями, або доповнення чинного переліку санкцій відповідними обов'язковими елементами, є доцільним та обґрунтованим. Такий підхід дозволить підвищити індивідуалізацію адміністративної відповідальності, посилити її виховний та профілактичний потенціал, знизити рецидив та підвищити правову культуру населення, а також наблизити вітчизняну практику до європейських стандартів правового реагування.

Підставою для таких змін може бути нова редакція КУпАП або прийняття спеціального закону про адміністративну відповідальність у сфері профілактики правопорушень.

Висновки. Здійснений аналіз свідчить, що адміністративні стягнення в їх нинішньому вигляді в Україні виконують переважно каральну функцію, в той час як КУпАП прямо вказує на необхідність виховання правопорушника та запобігання новим правопорушенням. Традиційні заходи, як-от штраф чи адміністративний арешт, є формальними та малоефективними у досягненні цієї мети, особливо серед неповнолітніх, осіб із низьким рівнем правової культури чи повторних порушників.

Міжнародна практика підтверджує, що синергетичний підхід, який поєднує правові, освітні, психологічні та соціальні інструменти впливу, сприяє більш стійкому правосвідомому поведінковому ефекту. Приклади з США, Великої Британії та Франції свідчать, що ефективним є саме багаторівневий, індивідуалізований вплив, що враховує особистісні особливості порушника, характер проступку і суспільну шкоду.

У зв'язку з цим доцільно:

розширити перелік адміністративних стягнень, закріпивши їх виховну функцію на законодавчому рівні; внести зміни до КУпАП доповнивши його статтею 24-2, яка буде передбачати можливість застосування альтернативних виховних заходів. Пропонуємо низку альтернативних заходів, що можуть супроводжувати адміністративні санкції:

– проходження профілактичних (повторних) курсів (з ПДР, фінансової грамотності, поводження з тваринами тощо);

– виконання соціально корисних робіт (допомога безхатькам, участь в освітніх акціях);

– публічне вибачення або написання есе / рефлексій щодо допущеного правопорушення;

– залучення до громадських слухань чи тематичних тренінгів;

– профілактичні інтерв'ю або консультації з соціальними працівниками;

– умовно-добровільна участь у медіаційних програмах для мінімізації конфліктних ситуацій.

– впровадити експериментальні моделі на місцевому рівні (наприклад, в ОТГ) щодо комбінованого реагування;

У цілому, синергетичний підхід до адміністративних санкцій дозволяє змістити акцент із репресивного впливу на превентивно-виховний, наблизивши українську систему адміністративної відповідальності до кращих практик правових держав Європи.

Список використаних джерел

1. Кодекс України про адміністративні правопорушення: чинне законодавство зі змінами та допов. станом на 01 січ. 2025 р. – К. : Центр учбової літератури, 2025. – 156 с.

2. Філософський енциклопедичний словник / За ред. В.І. Шинкарука. — К. : Абрикос, 2002. — 736 с.

3. Майік І. Application of synergetic approach in comparative jurisprudence while studying legal system [Електронний ресурс] // Legea şi Viaţa. – 2013. – №12. – С. 136–137. – Режим доступу: https://ibn.idsi.md/sites/default/files/imag_file/Application%20of%20synergetic%20approach%20in%20comparative%20jurisprudence%20while%20studynig%20legal%20system.pdf Назва з екрана. – Дата звернення: 25.04.2025.

4. Broom, D. A US judge sentenced teenage vandals to read books. This is what happened [Електронний ресурс] // World Economic Forum. – 2019. – Режим доступу: https://www.weforum.org/stories/2019/04/this-is-what-happened-when-a-us-judge-sentenced-teenage-vandals-to-read-books/

5. Davies, C. UK judge orders rightwing extremist to read classic literature or face prison [Електронний ресурс] // The Guardian. – 2021. – Режим доступу: https://www.theguardian.com/politics/2021/sep/01/judge-orders-rightwing-extremist-to-read-classic-literature-or-face-prison. Дата звернення: 25.04.2025

6. Driving safely and securely on French roads [Електронний ресурс] // French Interministerial Road Safety Committee (CISR). – 2023. – Режим доступу: https://www.onisr.securite-routiere.gouv.fr/sites/default/files/2023-10/2023%2007%2016%20CISR%20Press%20kit%20in%20ENG.pdf. – Назва з екрана. – Дата звернення: 25.04.2025.

Львова Олена Леонідівна,
старший науковий співробітник відділу теорії держави і права Інституту держави і права імені В.М. Корецького НАН України, кандидат юридичних наук, старший науковий співробітник

ПРОБЛЕМИ УТВЕРДЖЕННЯ НАЦІОНАЛЬНО-ПРАВОВОЇ ІДЕНТИЧНОСТІ В УМОВАХ ВІЙНИ

У Преамбулі Конституції України 1996 р. проголошено, що Верховна Рада України від імені Українського народу приймає цю Конституцію, «виражаючи суверенну волю народу, спираючись на багатовікову історію українського державотворення, усвідомлюючи відповідальність перед Богом, власною совістю, попередніми, нинішнім та прийдешніми поколіннями». Зазначене посилює фокус на національній ідентичності, що, за словами М. Козловець, сприяє усвідомленню нацією своєї сутності, тотожності й цінності [1, с. 439].

Щодо змісту поняття «національно-правова ідентичність», то в науковій літературі наголошується, що це той стан самовизначення нації як повноцінного суб'єкта права, який базується на правовій традиції, державотворчій дійсності та цивілізаційній перспективі [2, с. 163].

Нація, яка усвідомлює власну ідентичність як непересічність, неповторність, оригінальність у державно-політичному вимірі, здатна сформувати правову систему, що теж буде характеризуватися такими властивостями. Усвідомлення правової ідентичності передбачає відкрите, обґрунтоване запозичення досвіду світової спільноти щодо питань правотворення, втілення прогресивних ідей у правове поле держави на основі єдності, паритету у взаємовідносинах, а не домінування запозичених ціннісно-правових ідеалів, що може призвести до втрати національної самобутності української правової системи [3]. З огляду на зазначене слід згадати, що за час війни в Україні у сфері правотворчості відбуваються руйнівні для нашої нації речі, як-то – намагання легалізувати одностатеві стосунки, скасування Закону України «Про захист суспільної моралі» і т. п.

М. Шульга наголошує, що кожна національна ідентичність визначається власними цінностями, в свою чергу руйнування цих цінностей порушує політичний процес і, як наслідок, сам процес демократії. Ствердження власної ідентичності та захист національних цінностей є необхідною умовою існування демократичної держави. Лише усвідомлення своєї національної ідентичності створює можливості для діалогу з іншими ідентичностями. Сучасна криза демократичного суспільства – це криза демократичних цінностей. Дослідники спостерігають парадокс: з одного боку – руйнування каскаду загальних цінностей на користь індивідуалізма, просування множинної ідентичності, що в свою чергу суперечить формуванню будь-якого загального інтересу; з іншого боку – світова тенденція глобалізації, створення міжнародних інституцій (ЄС) що примусово нав'язують наднаціональні цінності, які можуть суперечити з

цінностям національним [4, с. 14]. Тож нині спостерігається слабкість ціннісно-ідеологічного фундаменту, на якому б будувалася правова політика держави. Втім серед конституційних засад утвердження національної ідентичності, окрім згаданої вище Преамбули Конституції України, є принцип верховенства права, визначений ст. 8 Конституції, суть якого спирається на розуміння права, яке інтегрує в себе, окрім законодавства, «…й інші соціальні регулятори, зокрема норми моралі, традиції, звичаї тощо» [5].

Тобто, мораль, звичаї і традиції як соціальні норми, що ідентифікують українську націю, можуть опинитися поза національним законодавчим полем, що є вельми небезпечним, особливо з огляду на те, що російський агресор багато років намагається знищити не лише українську культуру, а й цілеспрямовано здійснює геноцид нашої нації, про що свідчать жахливі наслідки війни.

Утім на захист національної ідентичності став прийнятий 13 грудня 2022 року Закон України «Про основні засади державної політики у сфері утвердження української національної та громадянської ідентичності» [6] (далі по тексту – Закон), ст. 3 якого встановлює правову основу державної політики у сфері утвердження української національної та громадянської ідентичності, якою, зокрема, є Конституція України. Зокрема, п. 2 ст. 4 Закону визначає основні завдання державної політики у сфері утвердження української національної та громадянської ідентичності, серед яких: формування у громадян України, у тому числі дітей та молоді, активної громадянської позиції на основі поваги до прав людини, духовних цінностей українського народу, національної самобутності.

У відповідності до змісту конституційного принципу верховенства права, ціннісними орієнтирами утвердження української національної та громадянської ідентичності, згідно п. 3 ст. 6 Закону, визнаються: соборність – єдність, неподільність усіх територій України, духовна єдність українців; самобутність українського народу, яка визначається його історією, культурою, традиціями та українською мовою; гідність – відстоювання своїх духовно-моральних і державницьких позицій, усвідомлення власної ваги та громадянського обов’язку у міжнародному співтоваристві.

Дані цінності визначають зміст і суть національної ідентичності, яка має віддзеркалюватися у правовій площині, у характері нормативно-правових актів, які приймаються. На жаль, сучасні глобалізаційні тенденції у напрямі адаптації українського законодавства до законодавства інших країн часто нівелюють українську самобутність, особливо з огляду на поширювані останнім часом гасла потреби боротьби із стереотипами і навіть встановлення покарання за так звану дискримінацію. Як підкреслює А. Романова, «значна кількість людей керуються внутрішніми переконаннями про добро і зло, а не страхом перед можливими санкціями. Це свідчить про високий рівень розвитку правової та суспільної свідомості як певного «критерію» балансу і гармонії між нормами позитивного і природного права. У воєнний час значно зростає роль природного права в суспільстві, адже саме завдяки високому рівню духовно-морального розвитку людина здатна у кризові періоди суспільного розвитку не втратити ціннісні вектори правомірної поведінки, а суспільство – не маргіналізуватися» [3].

Тож доречно процитувати пп. 17 п. 7 ст. 1 Закону, який визначає українську національну ідентичність як «стійке усвідомлення особою належності до української нації як самобутньої спільноти, об'єднаної назвою, символами, географічним та етносоціальним походженням, історичною пам'яттю, комплексом духовно-культурних цінностей, зокрема українською мовою і народними традиціями» [5].

Отже, утвердження національно-правової ідентичності українського народу наразі перебуває під загрозою з огляду на такі виклики: 1) військову агресію, яка направлена на знищення української нації як такої з її історією, культурою, традицією, духовністю; 2) жвавий процес беззастережного дублювання непритаманних українському суспільству деяких європейських моделей життя та сім'ї, що призводить до порушення прав окремої людини з її уявленням про добро та зло, про власну ідентичність, належність, до руйнації української самобутності, її ціннісно-правового фундаменту, що стає загрозою національній безпеці України.

Список використаних джерел

1. Козловець М.А. Феномен національної ідентичності: виклики глобалізації: монографія. Житомир : Вид-во ЖДУ ім. І. Франка, 2009. 558 с.
2. Ковальчук В. Національно-правова ідентичність та її роль в умовах конституційної трансформації в Україні. *Вісник Національного університету «Львівська політехніка»*. Серія: «Юридичні науки». № 4 (32). 2021. С. 159-166.
3. Романова А.С. Національна ідентичність у праві в кризовий період розвитку суспільства. Фаховий електронний науково-практичний журнал *Проблеми сучасних трансформацій*. Серія: Право, публічне управління та адміністрування. 2022. № 3. URL: https://reicst.com.ua/pmtl/article/view/issue_3_2022_title/issue_3_2022_title
4. Шульга М.В. Криза демократичних цінностей у процесі формування національної ідентичності. *Проблема ідентичності в XXI столітті*. Зб. наук. праць студентів, аспірантів на викладачів. 15 жовтня 2020 р. Київ, 2020. 94 с.
5. Рішення Конституційного Суду України N 15-рп/2004 від 2 листопада 2004 року у справі за конституційним поданням Верховного Суду України щодо відповідності Конституції України (конституційності) положень статті 69 Кримінального кодексу України справа про призначення судом більш м'якого покарання). *Офіційний веб-портал Верховної Ради України «Законотворчість».* URL: http://zakon3.rada.gov.ua/laws/show/v015p710-04.
6. Про основні засади державної політики у сфері утвердження української національної та громадянської ідентичності: Закон України 2834-IX від 13.12.2022. *Офіційний веб-портал Верховної Ради України «Законотворчість».* URL: https://zakon.rada.gov.ua/laws/show/2834-20#Text

Михайленко Роман Володимирович,
доцент кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат філософських наук, доцент

ДЕЗІНФОРМАЦІЯ ТА ІНФОРМАЦІЙНА БЕЗПЕКА

Військова агресія рф проти України відкрила новий спектр проблем. Зокрема, це стосується і феномену інформації. Зараз інформаційний фронт набув великої активності. Д. Смотрич, Л. Браілко слушно вказують: «Питання інформаційної безпеки та культури в умовах війни є питанням виживання людини, суспільства та держави. Адже забезпечення інформаційної безпеки визначається не тільки інтересами держави, а й інтересами особи в контексті забезпечення її прав і свобод. Основою сучасної інформаційної безпеки є цілісність даних, доступність інформації, конфіденційність і надійність її збереження» [3, с. 60]. Кількість неправдивих повідомлень про війну, внутрішні справи України та рф виросла в багато разів. Це є суттєвою ознакою війни, що проводиться рф. Оскільки кожен українець практично цілодобово відслідковує події за допомогою смартфонів, здатність розпізнавати та реагувати на неправдиву інформацію стає важливим інструментом у протистоянні.

Дезінформація – це неправдива інформація, яка поширюється з метою ввести в оману. Дезінформація спрямована на ліквідацію незалежності нашої держави, повалення конституційного ладу, порушення суверенітету та територіальної цілісності, пропаганду насильства, ворожнечі та ін. В основі сутності феномену дезінформації покладена форма перетворена. Г. Нерсесян характеризує вихідний пункт цієї категорії: «Єдність форми і змісту передбачає, що будь-який зміст має свою форму і будь-яка форма містить у собі певний зміст. Іншими слова ми, не буває форми беззмістовної рівно як і змісту неоформленого. І без винятку, будь-який суспільний поступ здійснюється у невід'ємному взаємозв'язку та взаємообумовленості форми і змісту. За Гегелем, відношення між змістом і формою є взаємовідношення діалектичних протилежностей, тобто їх взаємоперетворення. Немає ні одної матеріальної, біологічної, соціальної системи, яка не мала б форми і змісту: зміст завжди оформлений, а форма – змістовна. Якщо змінюється зміст неодмінно змінюється й форма рівно як і навпаки» [2, с. 59-60]. Ще загроза присутності перетворених форм у онтологічній площині полягає у тому, що подальша редукція форми-змісту може здійснюватися не тільки від межі дійсного суспільного субстрату, але й від попередньої перетвореної форми. Для того щоб дезінформація не мала суттєвого впливу на населення, треба, за можливості, розкривати фейки, що запускаються в український інформаційний простір. Це дасть змогу ефективно боротися з дезінформацією.

Список використаних джерел

1. Михайленко Р.В. Феномен дезінформації в умовах російської агресії. Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи : тези доп. учасників міжн. наук.-практ. конф. (Харків, 12-13 груд. 2023р.) ; Наук.-дослід. ін-т публ.політики і соц. наук. Харків: НДІ ППСН, 2023.- С. 119 -120. DOI: https://doi.org/10.32782/PPSS.2023.1.30

2. Нерсесян Г. Перетворена форма або світ кривих дзеркал. URL: https://ktpu.kpi.ua/wp-content/uploads/2016/02/peretvorena-forma-1.pdf (дата звернення: 06.05.2025).

3. Смотрич Д.В., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету,* 2023. С. 121-127. DOI https://doi.org/10.24144/2307-3322.2023.77.2.20

Нагайник Тарас Григорович,
старший викладач кафедри криміналістики навчально-наукового інституту права та психології Національної академії внутрішніх справ

АКТУАЛЬНІ ПРОБЛЕМИ ДОТРИМАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ІДЕНТИФІКАЦІЇ ТРУПА НЕВСТАНОВЛЕНОЇ ОСОБИ В УМОВАХ ДІЇ ВОЄННОГО СТАНУ

У процесі розвитку суспільства та технологій нарощуються можливості демографічного контролю за населенням, що має сприяти покращенню життя населення при вирішуванні окремих питань. Так, Закон України «Про громадянство України» визначає правовий зміст громадянства України, підстави і порядок його набуття та припинення, повноваження органів державної влади, що беруть участь у вирішенні питань громадянства України, порядок оскарження рішень з питань громадянства, дій чи бездіяльності органів державної влади, їх посадових і службових осіб [1].

З підписанням 14 березня 2014 року Угоди про асоціацію з Європейським Союзом Україна взяла на себе зобов’язання впровадити низку європейських норм. Серед нормативно-правових актів ЄС, які визначають основні засади законодавства у сфері електронної ідентифікації, є, зокрема, про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку. Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» визначає правові та організаційні засади створення та функціонування Єдиного державного демографічного реєстру та видачі документів, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи, а також права та обов’язки осіб, на ім’я яких видані такі документи.

В Законі України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» визначаються такі поняття:

«верифікація» - порівняння даних (параметрів), у тому числі біометричних, для встановлення тотожності особи документам або інформації з Реєстру для підтвердження їх ідентичності;

«біометричні дані» - сукупність даних про особу, зібраних на основі фіксації її характеристик, що мають достатню стабільність та істотно відрізняються від аналогічних параметрів інших осіб (біометричні дані, параметри - відцифрований підпис особи, відцифрований образ обличчя особи, відцифровані відбитки пальців рук);

«біометричні параметри» - вимірювальні фізичні характеристики або особистісні поведінкові риси, що використовуються для ідентифікації (впізнання) особи або верифікації наданої ідентифікаційної інформації про особу [2].

Створення баз даних осіб, які потрапляли в поле зору працівників правоохоронних органів, спростило до певної міри роботу по ідентифікації особи. Однак для широких верств населення існує обмеження щодо доступу до ряду баз даних, що обумовлено оперативно-розшуковою діяльністю, а специфічний вигляд трупів померлих (ушкодження, гниття тощо) унеможливлює або обмежує використання даної інформації для всіх громадян.

Після початку повномасштабного вторгнення кількість невстановлених осіб різко збільшилася з об’єктивних причин. Так, проблеми ідентифікації невстановлених осіб обумовлені:

- недостатністю інформації про зниклу особу;
- спотворенням трупу померлої людини, що не придатний для візуального впізнання (гниття, причини смерті, розчленування, розрив тощо);
- відсутністю відомості про факт зникнення особи;
- відсутністю доступу для всіх верств населення інформації з кримінальних та цивільних справ.

Наказом МВС 29.08.2022 № 535 «Про затвердження Положення про Єдиний реєстр осіб, зниклих безвісти за особливих обставин» створено Єдиний реєстр осіб, зниклих безвісти, для збору та централізації відомостей про таких осіб, а також для обліку інформації, необхідної для їх ефективного розшуку. Впровадження Єдиного реєстру дозволяє:

- впровадити технологію наскрізної ідентифікації та приведення інформації про особу у відповідність до єдиного ідентифікатора, який відповідатиме формату Унікального номера запису реєстру в Єдиному державному демографічному реєстрі;
- привести інформацію в інших національних електронних інформаційних ресурсах у відповідність до єдиного ідентифікатора.

На одному рівні з вищезазначеними, виникають проблеми, обумовлені етичними питаннями, а також питання щодо достовірності інформації, публічності інформації, її “естетичності” тощо. Сукупність та об’єктивність,

потрібність, актуальність вирішується в кожному випадку індивідуально; слідчий особисто приймає рішення та враховує вищезазначені проблеми.

Доступність інформації допомагає в розкриттю кримінальних проступків і встановленню невідомих осіб та обставин, пов'язаних з їх смертю та зникненням, що є одним з основних завдань поліції.

Список використаних джерел

1. Про громадянство України: Закон України від 18.01.2001 № 2235-III. URL: https://zakon.rada.gov.ua/laws/show/2235-14#Text
2. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20.11.2012 № 5492-VI. URL: https://zakon.rada.gov.ua/laws/show/5492-17#Text
3. Про національна поліцію. Закон України Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

Носенко Олександр Володимирович,
доцент кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат філософських наук, доцент

ФОРМУВАННЯ ПОЗИТИВНОГО ІМІДЖУ ПРАЦІВНИКІВ ПОЛІЦІЇ В УМОВАХ ІНФОРМАЦІЙНИХ ВИКЛИКІВ ТА ВОЄННОГО СТАНУ: МІЖ СТАНДАРТАМИ, ДОВІРОЮ І ПРОФЕСІОНАЛІЗМОМ

У період воєнного стану та в умовах післявоєнного відновлення держави особлива увага приділяється зміцненню інституційних гарантій правопорядку, інформаційної безпеки та довіри громадян до органів публічної влади. Поліція в цьому контексті виконує ключову роль не лише як інструмент охорони громадського порядку, але й як носій правових, моральних і комунікативних стандартів, що прямо впливають на інформаційне середовище суспільства. Особистість поліцейського, її професійна і морально-етична якість, перетворюється на чинник, що або зміцнює інформаційну безпеку, або, навпаки, її підриває. Виникає кореляційна взаємозалежність між поведінкою окремого суб'єкта (працівника поліції) та формуванням іміджу всієї інституції, чи виконавчої гілки влади загалом. Гарантією безпеки тут виступає не лише ефективне функціонування інституції, а й образ цієї організації в масовій свідомості. Саме тому формування іміджу Національної поліції України постає не другорядним, а системним завданням у політиці правової, комунікаційної та етичної модернізації правоохоронних органів.

Імідж працівника поліції – це соціально-психологічна конструкція, що поєднує очікування суспільства, реальний професійний і етичний рівень

працівника, а також комунікативні канали взаємодії з громадськістю. Тобто імідж не формується лише інституційно. Він є результатом щоденних практик. У дослідженні шведських науковців виявлено, що «64% громадян, які мали позитивний досвід взаємодії з поліцією, виражали вищий рівень довіри до держави загалом» [1, с. 54]. Отже, гуманістичний підхід у поліцейській діяльності – не риторика, а стратегічна необхідність.

У післявоєнний період зростатиме потреба у швидкому відновленні довіри до держави. Поліція, як одна з найбільш публічних її інституцій, стане маркером цього відновлення. Отже, інституціональні підходи до формування іміджу повинні поєднувати зовнішню комунікацію (медіа, інформаційні кампанії, прозорість діяльності) з внутрішньою трансформацією (етичні стандарти, освіта, внутрішній контроль). У цьому контексті, як зазначається в роботах Маруни та Манна, саме «персоніфікація службовців стає ключем до ефективної комунікації – громадяни не мають справи з абстрактною «поліцією», вони взаємодіють із конкретними особами [3, с. 16].

Як показує досвід США, Канади, Шотландії, застосування «боді-камер», процедур стандартизованого реагування, публічних звітів та незалежного громадського контролю стали рушіями для подолання кризи довіри до поліції [2]. У контексті України подібні ініціативи вимагають адаптації до культурних і воєнно-політичних реалій. Проте ключовою умовою є не лише формальне запровадження таких інструментів, а їхній постійний моніторинг, удосконалення та інституціоналізація в організаційній культурі МВС.

Однією з фундаментальних умов формування стійкої системи інформаційної безпеки держави в умовах воєнного стану та соціальної напруги є системна стандартизація поведінкових та особистісних характеристик працівника поліції, особливо в контексті комунікації з громадськістю. У сучасній Україні поліцейський все частіше сприймається не лише як носій владних повноважень, а як комунікатор держави – перша особа, з якою громадянин стикається у кризових ситуаціях. Від того, як поліцейський себе поводить, говорить, реагує, залежить не лише його індивідуальне сприйняття, а й образ всієї правоохоронної системи, а отже – і самої держави.

Одним із головних викликів є суб’єктивний чинник поведінки окремого працівника, який, у разі відхилення від професійних стандартів, може породжувати диспропорцію між декларованими цілями поліції та реальною практикою. Це вкрай небезпечно в умовах інформаційної війни, де будь-який прояв непрофесійності або грубості миттєво підхоплюється медіа, формуючи загрозливі іміджеві наративи про «поліцію як загрозу», а не як гаранта безпеки. Таким чином, інформаційна безпека держави починається з передбачуваної поведінки її представників – і саме тому стандартизація, як спосіб мінімізації впливу деструктивного ірраціонального чинника, є не просто методологічним інструментом, а складовою національної безпеки.

Особливої уваги заслуговує самопрезентація працівника поліції у публічному просторі. Здатність чітко, грамотно та етично комунікувати з громадянами – це не тільки прояв індивідуального виховання, а результат цілеспрямованої професійної підготовки. Сучасний поліцейський має володіти

навичками кризової комунікації, публічного виступу, реагування на запити журналістів та поведінки у публічному середовищі – тобто, діяти в межах заданого етичного сценарію, який виключає емоційну імпровізацію, що може зашкодити інституції.

У цьому контексті влучною є думка Маруни та Манна, які наголошують, що «публічне довір'я – це не продукт істини, а результат послідовної комунікації очікувань» [3, с. 22]. Тобто, громадянин довіряє поліції не тому, що завжди отримує бажаний результат, а тому, що взаємодія з нею відбувається у передбачуваному, професійному і зрозумілому форматі. Саме стандарти дозволяють нівелювати випадковість, яка у сфері безпеки завжди обертається ризиком.

Враховуючи соціальні реалії України – травматичний досвід зловживань, недовіру до органів влади, поширення дезінформації – уніфіковані моделі поведінки працівників поліції, побудовані на стандартах, мають бути не обмеженням індивідуальності, а засобом захисту як працівника, так і держави. Через це важливо визнати: інформаційна безпека сьогодні – це не лише боротьба з фейками, а й захист публічного обличчя держави, яким для більшості є саме поліцейський.

Аналіз досвіду Індонезії демонструє: наявність чітких SOP та етичних інструкцій пояснює до 72,2 % варіацій в ефективності патрульної служби. Водночас міжнародні дослідження доводять, що застосування носимих камер скорочує випадки застосування сили до 9,6 % [2], а в Шотландії 78 % респондентів вважають body-cams фактором, що підвищує довіру до поліції [4].

Аналіз законодавчого поля в Україні дозволяє виокремити такі ключові проблеми стандартизації діяльності поліцейського:

1) Відсутність чітких оціночних критеріїв для морально-етичних і психологічних якостей;
2) Недостатня валідація методик тестування особистості в межах конкурсного добору;
3) Відсутність постійного аудиту етичної поведінки працівників під час служби;
4) Інертність системи внутрішнього контролю та відсутність ефективних механізмів дисциплінарного нагляду;
5) Необхідність підвищення рівня інституалізації стандартів «soft skills» у підготовці та атестації працівників поліції.

Інформаційна безпека потребує не лише фізичної присутності держави, але й створення позитивного образу через правову, моральну та психологічну відповідність поліцейських займаній посаді. Надзвичайно перспективним є використання інструментів штучного інтелекту для динамічного моніторингу поведінкових патернів поліцейських та виявлення ризиків.

Таким чином, в умовах дії воєнного стану та інформаційної турбулентності, імідж поліцейського стає не лише об'єктом суспільної оцінки, а й чинником національної безпеки. Стандартизація професійної поведінки, комунікаційна відкритість та орієнтація на етику служіння – це ті складові, що мають лягти в основу післявоєнної політики розвитку Національної поліції.

Список використаних джерел

1. Eriksson. Police trust and legitimacy in times of crisis: Swedish citizens' attitudes during the pandemic. *European Journal of Criminology,* 2023. 20(1), 34–51.
2. Lum, C., Koper, C. S., & Stoltz, M. (2020). Body-worn cameras' effects on police officers and citizen behavior: A meta-analysis. *Criminology & Public Policy, 19*(3), 743–772. https://doi.org/10.1002/cl2.1112
3. Maruna, S., & Mann, R. E. Reconciling "Desistance" and "What Works". *Probation Journal, 2019. 68*(1), 12–28.
4. Webster W, Miranda D, Leleux C. Scottish Police Authority. Public Confidence in Body Worn Video. *Edinburgh: SPA Research Reports*. 2022. P.74

Овсянюк Дмитро Іванович,
начальник аналітичного відділу (Центр кримінальної аналітики) Національної академії внутрішніх справ

СИМУЛЯЦІЙНІ ВПРАВИ ЯК ІННОВАЦІЙНИЙ ІНСТРУМЕНТ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ПРАВООХОРОНЦІВ: ПРИНЦИПИ, СТРУКТУРА ТА ЕТАПИ РЕАЛІЗАЦІЇ

Сучасна правоохоронна діяльність вимагає від працівників високого рівня професійної підготовки. Ця підготовка охоплює не лише теоретичні знання, але й розвинені практичні навички. В умовах сьогодення поліцейські мають вміти оперативно аналізувати складні ситуації та адекватно реагувати на них. Вони також повинні приймати виважені рішення в умовах дефіциту часу та психологічного навантаження, ефективно діяти в екстремальних умовах та взаємодіяти з різними категоріями громадян.

Такі високі вимоги до професіоналізму правоохоронців зумовлюють необхідність постійного вдосконалення системи їхньої підготовки, яка, як і освіта в цілому, стоїть на шляху реформації. Від викладачів у цій сфері очікується новаторський підхід, збагачення навчального процесу інноваційними методиками, що дозволяють урізноманітнити види навчальної діяльності, забезпечити її випереджаючий характер та відповідати запитам нового покоління слухачів, зокрема так званого «Net-покоління» [1].

Традиційні методи навчання, хоч і створюють теоретичну базу, не завжди забезпечують формування стійких практичних компетенцій для роботи в реальних, непередбачуваних умовах. Саме тому симуляційні вправи виступають як інноваційний та ефективний інструмент у професійному розвитку правоохоронців. Симуляції вважаються одними з найефективніших форм навчання [2]. Вони є методом навчання, що імітує реальні ситуації для розвитку практичних навичок, прийняття рішень та командної взаємодії. Базуючись на активному зануренні та навчанні через досвід, симуляції створюють міст між теорією та практикою, моделюючи професійні сценарії в безпечному та

контрольованому середовищі. Це сприяє не лише відпрацюванню конкретних дій, але й розвитку критичного мислення, командної роботи та психологічної стійкості. Симуляції використовуються для підготовки фахівців провідними правоохоронними органами [3] та міжнародними організаціями [4]. Наочним прикладом ролі симуляційних вправ у професійній підготовці є тренувальний комплекс ФБР «Алея Хогана» – спеціально створене імітаційне містечко, де правоохоронці відпрацьовують тактичні дії та стратегії реагування в максимально реалістичних модельованих сценаріях [5].

Конус досвіду Дейла (1969) демонструє, що ефективність методу навчання залежить від ступеня залученості того, хто навчається, і, відповідно, засвоєння посилюється в умовах активної діяльності. Таким чином, імітація реального досвіду та безпосередня участь видаються необхідними для досягнення ефективного засвоєння [6]. Дійсно, ефективність навчання через активний досвід, на чому наголошує Конус Дейла, підтверджується широким використанням симуляційних технологій у найрізноманітніших галузях: від підготовки пілотів і медичних фахівців до бізнес-тренінгів та, як демонструє зокрема джерело [6], навіть у таких сферах, як міське планування та розробка екологічних ініціатив. Така універсальність свідчить про фундаментальну цінність симуляцій як методу практичного навчання.

Для досягнення ефективності симуляційних вправ важливо враховувати такі принципи, як:

1. Достовірність, що полягає у створенні максимально реалістичного середовища, сценарію та ролей для глибокого залучення учасників.

2. Активна участь, передбачає що учасники не є пасивними спостерігачами, а безпосередньо виконують завдання та приймають рішення, несучи за них відповідальність у межах симуляції.

2. Безпечне середовище, яке надає можливість відпрацьовувати дії в потенційно небезпечних ситуаціях, наприклад, під час затримання чи спілкування з агресивними особами, без реального ризику.

3. Контрольованість та керованість, завдяки яким інструктор може спрямовувати хід вправи, вносити корективи, зупиняти для аналізу, повторювати епізоди та вводити ускладнення.

4. Структурований зворотний зв’язок, також відомий як дебрифінг, вважається надзвичайно важливим етапом, що передбачає детальний аналіз дій, обговорення помилок та успіхів, а також надання рекомендацій.

5. Повторюваність та варіативність, що дають можливість багаторазового відтворення схожих або змінених сценаріїв для закріплення навичок та відпрацювання різних підходів.

6. Адаптивність та гнучкість, що означають можливість адаптації складності та умов сценаріїв до рівня підготовки учасників та навчальних цілей.

Проведення симуляційної вправи можна поділити на такі етапи:

1. Етап підготовки, що включає чітке визначення навчальних цілей, розробку деталізованого сценарію із сюжетними лініями, профілями персонажів та ввідними даними, включно з коригувальними.

На цьому етапі також визначаються ролі для учасників та акторів, готується матеріально-технічне забезпечення, локації та реквізит, що імітує реальні умови та докази. Важливим кроком є розробка системи оцінювання дій учасників. Завершується підготовка детальним інструктажем усіх учасників щодо мети, сценарію та правил безпеки.

2. Етап проведення симуляції, який починається із введення в ситуацію за сценарієм.

На активній фазі учасники виконують свої ролі, реагують на події та приймають рішення. Інструктор спостерігає, вводить ввідні та контролює дотримання правил. Дії учасників фіксуються спостерігачами, часто за допомогою технічних засобів, для подальшого аналізу.

3. Етап аналізу та обговорення, відомий як дебрифінг.

Це етап розпочинається із зворотного зв'язку від учасників, що включає їхні враження та самооцінку, після чого інструктори та спостерігачі проводять детальний аналіз дій, обговорюючи помилки та успіхи. Мета полягає в ідентифікації засвоєних уроків, формулюванні висновків та наданні рекомендацій для вдосконалення.

4. Етап оцінювання та підтвердження результатів навчання.

Цей етап спрямований на визначення того, наскільки добре учасники засвоїли навички під час симуляції та як ці навички переносяться у реальну службову діяльність. Окрім цього, на даному етапі також оцінюється ефективність самої симуляційної вправи, переважно на основі відгуків учасників та інструкторів, з метою її подальшого вдосконалення..

Симуляційні вправи є потужним та незамінним інструментом у сучасній підготовці правоохоронців. Їхня ефективність досягається завдяки здатності створювати динамічне навчальне середовище, наближене до реалій, дозволяючи відпрацьовувати комплексні компетенції. Системний підхід, забезпечений чітко визначеними етапами від планування до аналізу та підтвердження результатів, є важливим для досягнення цілей симуляційного навчання. Подальший розвиток цього напрямку, зокрема за допомогою новітніх технологій, має бути стратегічним пріоритетом для підвищення якості підготовки правоохоронців.

Список використаних джерел

1. Вембер В.П. Сучасні типи навчального відео та особливості їх використання у навчальному процесі / В.П. Вембер, Д.Л. Бучинська // *Освітологічний дискурс*. 2016. № 1. С. 19-29.

2. Хруленко Г.В. Симуляційні ігри як успішна навчальна технологія // Трансформації в сучасному освітньому просторі: глибинні аспекти розвитку освіти : зб. матеріалів Всеукр. наук.-практ. конф. – Хмельницький, 2023. – С. 54–56.

3. Michelle Khare. I Tried Police Academy [Електронний ресурс]. – YouTube, 2021. – URL: https://www.youtube.com/watch?v=ZJGirITl6sE (дата звернення: 18.05.2025).

4. Organization for Security and Co-operation in Europe. OSCE launches new support programme for Ukraine with major donor funding [Електронний ресурс] :

URL: https://www.osce.org/osce-secretariat-exb-support-programme-for-ukraine/570414 (дата звернення: 12.05.2025).

5. Federal Bureau of Investigation. Hogan's Alley [Електронний ресурс]. URL: https://www.fbi.gov/investigate/how-we-investigate/hogans-alley (дата звернення: 15.05.2025).

6. Brissel L., Morel L., Dupont L. Contribution to setting up a sustainable learning in an eco-neighborhood development plan based on "Serious game" // 2013 International Conference on Engineering, Technology and Innovation (ICE) & IEEE International Technology Management Conference, The Hague, Netherlands, 2013. – P. 1–14. – DOI: 10.1109/ITMC.2013.7352607.

Пендюра Максим Миколайович,
завідувач кафедри теорії, історії та філософії права навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, доцент

ІНФОРМАЦІЙНА БЕЗПЕКА СУСПІЛЬСТВА В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ ТА ПІСЛЯВОЄННИЙ ПЕРІОД

У XXI столітті людство вступило в епоху інформаційного суспільства, у якому знання та інформація стали ключовими ресурсами. Однак з розвитком цифрового середовища зростає і вразливість до нових викликів, особливо в умовах правового режиму воєнного стану. Інформаційна безпека ще більше набуває пріоритетного значення не лише як складова національної безпеки, а як основа стійкості держави, її обороноздатності та суспільної стабільності.

Метою статті є проаналізувати правові та організаційні аспекти забезпечення інформаційної безпеки суспільства в умовах правового режиму воєнного стану та післявоєнний період, окреслити проблеми та напрями їх подолання в контексті розвитку інформаційного суспільства в Україні.

Інформаційне суспільство, як нова стадія цивілізаційного розвитку, характеризується зростанням ролі інформації, цифрових технологій, знань та інформаційної взаємодії в усіх сферах життєдіяльності держави. Концепція інформаційного суспільства була сформована у працях Д. Белла, З. Бжезинського, М. Кастельса, М. Порат, А. Тоффлера, А. Турена, Ю. Хабермаса та інших дослідників, які акцентували увагу на переході від індустріальної до постіндустріальної епохи.

Однак саме в умовах воєнного стану інформаційна сфера стає вразливою до низки загроз: інформаційно-психологічних операцій, дезінформації, кібератак, порушення доступу до критичних інфраструктур, поширення паніки через соціальні мережі тощо. На тлі цих викликів особливої актуальності набуває інформаційна безпека як цілісна система заходів для захисту інтересів держави, суспільства й особи в інформаційній сфері.

Відповідно до Закону України «Про правовий режим воєнного стану», під час його запровадження можливе тимчасове обмеження конституційних прав і свобод громадян, зокрема свободи слова, діяльності ЗМІ, права на інформацію. Основною метою є протидія ворожим інформаційним впливам, охорона стратегічної інформації, блокування каналів деструктивного контенту [1].

Однак ці обмеження повинні бути пропорційними, законними та такими, що відповідають принципам міжнародного права. Водночас воєнний стан вимагає не лише обмеження, а й ефективної стратегії інформаційної протидії, зокрема:

1. нейтралізації пропагандистських кампаній;
2. забезпечення інформаційної гігієни суспільства;
3. розбудови системи стратегічних комунікацій;
4. протидії кіберзлочинності;
5. гарантування захисту персональних даних.

Інформаційна безпека як складова національної безпеки України закріплена в Конституції України, Законах України «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України», а також у Стратегії кібербезпеки та інших нормативних актах. В умовах збройної агресії рф, значного поширення фейкових наративів та кібератак з боку ворожих структур, забезпечення цілісності національного інформаційного простору є ключовим [2; 3, с. 182].

З 2014 року Україна активно розвиває системи протидії гібридним загрозам, зокрема створено Центр протидії дезінформації при РНБО, посилено взаємодію з Європейським Союзом та НАТО у сфері кібербезпеки та стратегічних комунікацій.

Особливу роль відіграє державна політика у сфері медіаграмотності, оскільки суспільна спроможність до критичного сприйняття інформації безпосередньо впливає на рівень загальної безпеки.

Воєнний стан, на відміну від традиційних уявлень, сьогодні є не лише збройним протистоянням, а й боротьбою в інформаційному просторі. Російська агресія проти України супроводжується потужною інформаційною війною, яка включає:

- масштабне поширення фейкових новин;
- психологічне тиснення через соцмережі;
- деструкцію внутрішньої довіри до інституцій влади;
- кампанії з деморалізації ЗСУ та цивільного населення;
- кібератаки на об’єкти критичної інфраструктури.

Відповіддю на ці виклики має бути інтеграція інформаційної політики з національною безпекою, формування сталої цифрової ідентичності, розвиток власного наративу, який об’єднує суспільство та зміцнює його стійкість.

Завершення активної фази бойових дій не означає автоматичного припинення інформаційної агресії. У післявоєнний період Україна буде стикатися з низкою складних завдань у сфері інформаційної безпеки, зокрема:

1. Реінтеграція інформаційного простору деокупованих територій. Багаторічне перебування під впливом ворожої пропаганди потребує комплексної

програми інформаційної реабілітації - від відновлення інфраструктури до відновлення довіри населення до українських інституцій.

2. Контроль за розповсюдженням деструктивних наративів. У післявоєнний період можлива активізація внутрішніх і зовнішніх деструктивних сил, які використовуватимуть «посттравматичний» стан суспільства для поширення паніки, реваншистських або сепаратистських настроїв.

3. Ризики політичної поляризації. В умовах зміни політичного ландшафту після завершення воєнного стану загострюються суспільні суперечності, що можуть бути використані в інформаційних кампаніях для розколу суспільства.

4. Вплив іноземних медіа. Після послаблення воєнних обмежень активізується присутність іноземних інформаційних платформ, не завжди лояльних до України, що вимагає посилення інформаційного суверенітету.

Отже, післявоєнна інформаційна політика повинна поєднувати демократичні принципи свободи слова з безпековими пріоритетами, дотримуючись балансу між відкритістю та стійкістю.

Для формування сталого та безпечного інформаційного середовища в умовах трансформації безпекового контексту необхідна реалізація цілісної стратегії. Вона має ґрунтуватися на нашу думку на таких базових напрямках:

1. Законодавче удосконалення:

Потрібно адаптувати нормативно-правову базу до нових викликів цифрової доби. Особливо актуальними є:

– розмежування понять «інформаційна безпека» і «свобода слова» в умовах особливих режимів;

– закріплення механізмів захисту критичної інформаційної інфраструктури;

– визначення правових основ цифрової ідентичності;

– створення єдиного реєстру інформаційних інцидентів у сфері нацбезпеки.

2. Інституційна координація:

Забезпечення міжвідомчої взаємодії між Радою Національної безпеки і оборони України, Міністерством оборони України, Службою безпеки України, Держспецзв’язку, Міністерством цифрової трансформації, медіарегулятором та громадянським суспільством є критично важливим. Особливу роль у цьому має відігравати Центр протидії дезінформації, який може стати центральним координатором державної інформаційної політики.

3. Розвиток національного інформаційного продукту:

Інформаційна безпека неможлива без створення якісного національного контенту – українськомовного, патріотичного, інтелектуального. Це стосується:

– розвитку суспільного мовлення;

– підтримки незалежних медіа;

– стимулювання виробництва українських документальних та художніх фільмів, серіалів, освітніх платформ;

– протидії монополізації інформаційного ринку іноземними технологічними гігантами.

4. Освітні ініціативи:

Підвищення рівня цифрової грамотності населення – один із ключових чинників запобігання маніпуляціям. Потрібно:

– запровадити системну медіаосвіту у дошкільних закладах, школах (ліцеях, коледжах) та університетах (академіях);

– створити державні і приватні платформи для навчання кібергігієні;

– проводити загальнонаціональні і регіональні (місцеві) кампанії з інформування щодо інформаційної безпеки.

5. Міжнародна співпраця:

Україна має інтегруватися в європейські та трансатлантичні механізми інформаційної безпеки. Участь у відповідних програмах ЄС, НАТО, співпраця з кіберкомандуваннями партнерських країн, особливо закладів вищої освіти дозволять підвищити ефективність вітчизняної системи захисту.

6. Людина в центрі інформаційної безпеки:

Особливість сучасного підходу до інформаційної безпеки – зміщення акценту з державоцентризму на людиноцентризм. Основна мета – не просто захистити державу, а гарантувати безпечне і гідне інформаційне середовище для кожного громадянина. Це означає:

1. забезпечення доступу до достовірної інформації;
2. недопущення інформаційної дискримінації;
3. захист персональних даних і приватності;
4. можливість громадян реалізувати право на відповідь, спростування, доступ до правди.

Інформаційна безпека у цьому контексті – не лише технічний чи військовий захист, а передусім – умова якісного демократичного розвитку.

Інформаційна безпека в умовах воєнного стану та в післявоєнний період – це довгостроковий різнорівневий процес, який вимагає системності, адаптивності та активної участі держави, суспільства і кожного громадянина. Від ефективності державної інформаційної політики залежить не лише захищеність від зовнішніх впливів, а й здатність нації до самозбереження, відновлення та розвитку після війни.

Після перемоги Україна потребуватиме не лише фізичної, а й інформаційної реконструкції. Сформований під час воєнного стану досвід має бути інтегрований у довготривалу політику інформаційної стійкості, що ґрунтується на цінностях прав людини, демократичного розвитку та технологічного суверенітету.

Список використаних джерел

1. Закон України «Про правовий режим воєнного стану» від 12.05.2015 №389-VIII // *Відомості Верховної Ради України*. 2015. № 28. Ст. 250. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII // *Відомості Верховної Ради України.* 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. Милосердна І.М. Інформаційна безпека як елемент національної безпеки: теоретичний вимір та особливості впровадження / І.М. Милосердна // *Політикус :* наук. журнал. 2024. № 4. С. 179-185. URL: http://politicus.od.ua/4_2024/28.pdf

4. Посібник з протидії дезінформації. URL: https://cpd.gov.ua/announcement/posibnyk-z-protydiyi-dezinformacziyi/

Пендюра Максим Миколайович,
завідувач кафедри теорії, історії та філософії права навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, доцент
Пилипенко Вікторія Вікторівна,
доцент кафедри теорії, історії та філософії права навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат історичних наук, доцент

ФОРМУВАННЯ НАВИЧОК МЕДІАГРАМОТНОСТІ ЯК ОСНОВА ПРОФЕСІЙНОЇ ПІДГОТОВКИ ЮРИСТІВ В УМОВАХ ВІЙНИ

В умовах війни інформація є зброєю, яку у вигляді фейків, дезінформації, маніпуляцій використовують для морального та психологічного придушення опору населення. За результатами проведеного протягом травня-червня 2024 року на замовлення Громадянської мережі ОПОРА опитування, було встановлено, що 73,4% українців використовують соцмережі як джерело новин. Серед них найпопулярніші – Telegram (78.1%), YouTube (59.5%) та Facebook (44.6%) [1]. Виходячи з такої популярності заявлених соцмереж й не представленого в опитуванні, але стрімко набираючого темпи популярності TikTok, юристи, особливо початківці, намагаються зайняти серед них свою нішу. Дедалі частіше можна зустріти коментарі юристів з приводу тієї чи іншої урядової ініціативи, законопроєкту або оголошення правової оцінки проведеним заходам. З одного боку така доступність покращує правову обізнаність населення, а з іншого, юрист сам того не усвідомлюючи, стає популяризатором фейків та неправдивих новин. Останнє особливо стосується численних коментарів щодо заявлених законопроєктів, які ще навіть не пройшли перше читання. Ось чому сьогодні загострилася проблема формування в юристів навичок медіаграмотності та основ критичного мислення під час їх професійної підготовки та перепідготовки.

Медіаграмотність являє собою сукупність мотивів, знань, умінь і можливостей, що сприяють добиранню, використанню, критичному аналізові, оцінюванню, створюванню та передаванню медіатекстів різних форм, жанрів, а також аналізові складних процесів функціонування медіа в суспільстві. Іншими

словами медіаграмотність полягає у формуванні критичного ставлення до отриманої інформації, виробляє уміння захисту персональних даних та дотримання інформаційної гігієни.

Головною метою медіаграмотності юриста є вироблення в нього медіаімунітету, що містить баланс між свободою слова, вільним доступом до інформації та дотриманням прав людини, стандартів професійної етики й норм стосовно захисту та не розголошення інформації. Про першочерговість включення в освітній процес настанов щодо поведінки юристів в соціальних мережах, які відповідатимуть правилам професійної етики та морально-етичним нормам, наголошується в прийнятих 2014 році Міжнародних принципах поведінки в соціальних мережах для юридичних професій. Прийняття міжнародного стандарту вказує на наявність вкрай важливої потреби захисту професійних прав юристів у віртуальному просторі, адже соціальні медіа слугують майданчиком, завдяки якому, зокрема, правники можуть сприяти здійсненню ефективного правосуддя шляхом залучення до обговорення широких верств населення. Соціальні медіа надають доступ до безмежної аудиторії та відкривають нові інструменти, такі як моніторинг правових змін у режимі реального часу та можливість їх обговорення з колегами в усьому світі. Ці ж якості також вказують на те, що соціальні медіа можуть бути використані неналежним чином, що може нести за собою дисциплінарну відповідальність [2]. Тож потрібно студентів спеціальності «Право» вчити використовувати соціальні медіа так, щоб це не шкодило професійним зобов'язанням юриста та, у більш ширшому сенсі, здійсненню ефективного правосуддя загалом.

У даному контексті варто звертати увагу на основні виклики, що постають перед юристом в його професійній діяльності через неузгодженість його віртуальної поведінки з нормами професійної етики. При цьому така актуалізація має відбуватися не лише на рівні репродуктивного засвоєння теоретичних знань, але й шляхом опрацювання дисциплінарної практики кваліфікаційно-дисциплінарних комісій адвокатури щодо дотримання адвокатами норм адвокатської етики при використанні мережі Інтернет. Як приклад для розгляду можна подати Рішення Вищої кваліфікаційно-дисциплінарної комісії адвокатури № Х-020/2021 від 01.10.2021 [3].

Загалом же, випускники спеціальності «Право» мають володіти наступними навичками медіаграмотності: оцінка професійних наслідків публічної демонстрації зв'язку з клієнтом; дотримання основ доброчесності, як академічної, так і антикорупційної; слідкування за проявами професійної репутації й не допущення аморальної поведінки (нецензурні коментарі, переказування не перевіреної інформації, тощо); відстеження налаштувань конфіденційності сторінки; подача правдивої та перевіреної інформації, адже інформація надана юристом сприймається людьми як частина консультації; дотримання правил чесної реклами й самореклами; уникнення світоглядних конфліктів через некоректні дописи; гармонічна демонстрація ідентичної поведінки в соцмережах і в реальному житті; захист конфіденційності інформації, отриманої від клієнта. Усі перераховані навички мають найперше

зберігати незалежність професії юриста у всіх її проявах, аналогічно тим, які діють в реальному житті.

Таким чином, вивчення юристами основ медіаграмотності, в умовах, коли соцмережі набувають все більшого значення в життя громадян, має стати складовою їх професійної підготовки та запорукою відповідального ставлення до обраної професійної діяльності.

Список використаних джерел

1. Медіаспоживання українців: третій рік повномасштабної війни. ОПОРА. 2024. 10.07. URL: https://www.oporaua.org/viyna/doslidzhennya-mediaspozhivannya-ukrayinciv-tretiy-rik-povnomasshtabnoyi-viyni-25292 (дата звернення: 01.12.2024).

2. Принципи Міжнародної асоціації юристів (IBA) щодо поведінки в соціальних мережах для юридичних професій від 24 травня 2014 р. URL: https://tomorrowslawyer.org/wp-content/uploads/2017/10/IBA-International-Principles-media_ukr.pdf (дата звернення: 01.12.2024).

3. Рішення Вищої кваліфікаційно-дисциплінарної комісії адвокатури № Х-020/2021 від 01.10.2021. URL: https://vkdka.org/uzagalnennya-distsiplinarnoji-praktiki-kvalifikatsijno-distsiplinarnih-komisij-advokaturi-schodo-dotrimannya-advokatami-norm-advokatskoji-etiki-pri-vikoristanni-merezhi-internet/ (дата звернення: 01.12.2024).

Петрова Ганна Миколаївна,
доцент кафедри теорії, історії та філософії права навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат філософських наук

РОЛЬ МЕДІА, БЛОГЕРІВ ТА СОЦМЕРЕЖ У ФОРМУВАННІ ІНФОРМАЦІЙНОГО ПРОСТОРУ

Роль медіа, блогерів та соцмереж у формуванні інформаційного простору є ключовою у дослідженні інформаційної безпеки, особливо в умовах воєнного стану та повоєнного періоду, оскільки ця роль виявляє себе у впливі різних інформаційних акторів на суспільну свідомість, поширення правдивої та маніпулятивної інформації, а також у формуванні й застосуванні механізмів протидії дезінформації.

Прийнято вважати, що діяльність традиційних медіа (телебачення, радіо, преси) полягає в інформуванні населення про події в країні та світі, а також здійсненні аналітичної роботи (наданні експертних оцінок, коментарів). Невід'ємною рисою традиційних медіа є й консолідація суспільства в умовах кризи. Разом із тим в умовах воєнного часу наявне в країні інфополе продукує ряд значимих проблем: таких, що пов'язані із воєнним станом, а також тих, що є

“вічними”, універсальними. Зокрема, це стосується протипоставлення об’єктивності висвітлення інформації та пропаганди, орієнтованої на реалізацію чужої волі, впливу державного та комерційного контролю на контент, цензури та самоцензури в умовах воєнного стану.

Не можна оминути увагою вплив блогерів та незалежних медіа на інформаційний простір сучасної України, що є його суттєвою ознакою. Так, порівняно з традиційними медіа незалежний контент відрізняється гнучкістю та швидкістю реакції на події, оприлюднює альтернативні погляди, які можуть ігноруватися (або ж замовчуватися) офіційними джерелами. Важливою рисою і здобутком недержавних медіа і блогерів стає персоналізація контенту (авторський стиль, суб’єктивність подачі матеріалу), що формує довіру і прихильність аудиторії – споживачів даного контенту. Зворотнім боком процесу “авторизації” і – відповідно – суб’єктивізації подачі інформації може виступати поширення неперевіреної інформації (фейків, теорій змов), відсутність редакційного контролю та фактчекінгу. Не можна оминути увагою і можливість маніпуляцій з боку ворожих до національного суверенітету України сил через фінансування або тиск і погрози.

До того ж навіть під час війни не можна ігнорувати й загальнолюдської, універсальної і загальнозначимої проблеми – недостатності спілкування, самотності у сучасному світі. Люди йдуть до контентмейкерів, зростаються з ними, ділять із ними своє життя, призвичаюються мислити й описувати навколишній світ голосом своїх обранців. Контентмейкерам вдається підмінити ідентичність глядачів, навязуючи, пропонуючи їм своє бачення світу, подій, власну оцінку ситуації, що склалася. І коли лунає конструктивна критика стосовно ворожого і деструктивного контенту (такого, що транслює російські наративи, записаного російською мовою, ширить комплекс нижчовартості українців тощо), споживачі такого контенту сприймають цю критику як зазіхання на власну ідентичність – зазіхання на власне “Я”. Як зазначає відома контентмейкерка Тетяна Микитенко: “Якщо нападати на, умовно, Дудя, то людина захищатиме себе, свою ідентичність споживача Дудя, а не, власне, самого Дудя” [1].

У цілому ж формування сучасного інформаційного простору, якщо розуміти його як динамічну систему, де технології, люди та інституції взаємодіють через потоки даних, – відбувається під впливом різних механізмів і має суттєві соціальні, економічні та політичні наслідки. До позитивних аспектів цього процесу можна віднести мобілізацію суспільства (волонтерські ініціативи, збори коштів), громадянський журналізм (подієвість, коли очевидці подій поширюють інформацію в реальному часі) та ін. механізми. До негативних аспектів належить інформаційна перевантаженість медіаконтенту (стрес, тривожність, загроза власному життю), розкол суспільства через використання амбівалентних і/чи поліваріантних наративів, і, у цілому, втрата довіри до будь-яких джерел інформації – та тенденція, що її нині масово спостерігаємо у вітчизняних користувачів соціальних мереж.

Регулювання та саморегулювання інформаційного простору може здіснюватися як за допомогою застосування заходів з боку державної влади -

блокування проросійських ресурсів, санкції проти пропагандистів, котрі поширюють проросійські наративи і месиджі, через ініціативи медіаплатформ, що пропонують маркування неперевіреного контенту, бан фейкових акаунтів тощо, так і шляхом виявлення громадянської відповідальності українців.

Інформаційний простір - це арена боротьби за владу, увагу та ідентичність. Сталий розвиток інформаційного простору вимагає нині технологічної грамотності користувачів, формування етичних рамок для використання ШІ, алгоритмів діяльності медіа, вироблення загальноприйнятних прозорих нормативних стандартів для діяльності контентмейкерів.

Медіа, блогери та соцмережі є потужними інструментами формування інформаційного простору, який може як об'єднувати суспільство, так і роз'єднувати його. В умовах війни їх роль стає ще критичнішою, тому на першому місці в діяльності державних і громадських інституцій має постати підвищення медіаграмотності населення, розвиток критичного мислення, ефективне регулювання медіапростору без порушень свобод контентмейкерів і медіаспоживачів.

Список використаних джерел

1. Рагулівна. Блоґ про агресивний несмак українського бомонду і не тільки. URL: https://www.youtube.com/@ragulivna

Пилипенко Вікторія Вікторівна,
доцент кафедри теорії, історії та філософії права навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат історичних наук, доцент

ФОРМУВАННЯ СТАЛИХ ІСТОРИЧНИХ НАРАТИВІВ ЯК СКЛАДОВА ВОРОЖИХ ІПСО

Починаючи з оголошення АТО в 2014 році і особливо після повномасштабного вторгнення в лютому 2022 року росія використовує проти українців всі три складових сучасних війн: конвенційну (безпосереднє ведення бойових дій), інформаційну (поширення фейків і дезінформації), смислову (викривлення системи цінностей). Смислова війна, за словами Рени Марутян, покликана змінити національну ідентичність, викривити свідомість поколінь на основі сфабрикованих переконань і знань, які сприймаються за «чисту монету» [1]. Найпершим і надважливим інструментом смислової війни є історичні наративи, які апелюють до колективної пам'яті та мають формувати так званий міф основи як візуальний та задокументований, перетворений на юридичне джерело, доказ ідентичності нації, що формується у процесі злиття окупованої території з тілом держави агресора. Таким чином російська військово-ідеологічна машина перетворила історію на важливий гнучкий, а головне

слухняний в руках пропагандистів, інструмент, а смислову війну на основний метод ІПСО або PSYOPS.

Міністерство оборони США визначає ІПСО як «заплановану політичну, економічну, військову та ідеологічну діяльність, спрямовану на іноземні країни або окремих осіб з метою створення емоцій, ставлень, розумінь, переконань і поведінки, сприятливих для досягнення політичних і військових цілей» [2, с. 77]. Отож, російські спецслужби використовують історичні наративи в ІПСО одразу для двох стратегічних цілей: створення міфу основи існування своєї держави з сукупності анексованих територій і залучення до служіння цьому міфу адептів з окупованих територій, що мають у підсумку виправдати її територіальні зазіхання та воєнні злочини. Якщо із залученням служителів культу «руського міра» завдяки дезінформації і пропаганді проблем в агресора ніколи не було, то формування міфу основи викликало цілу низку питань.

Міф основи, за дослідженням філософа з Єльського університету Джейсона Стенлі, має бути фундаментом ідентичності штучно сформованої нації, наріжним каменем її монолітності, де першооснову складає славетна національна історія, в якій члени цієї обдарованої нації панували над іншими. Взятий для цього історичний факт спільної перемоги приналежних осіб до заявленої «нації переможців» повинен викликати емоцію ностальгії й бажання повторити минулу велич за будь-яку ціну (от звідки гасло в російській концепції пам'яті Другої світової війни – «Можем повторить» – автор) [3, с. 17].

Про проблеми російської пропагандистської машини з пошуком міфу основи свідчать численні взаємосуперечливі заяви путіна про те, спадкоємцем якої держави є сучасна росія. Однією із найбільш стабільних версій є переконання про спадкоємність росією ідеалів і завдань Радянського Союзу. Для народів пострадянського простору москва мала залишитися центром комуністичної землі обітованої, а російський президент єдиною силою, здатною подолати економічні труднощі, що виникли після розпаду СРСР. Однак, стрімкий розвиток держав колишнього радянського табору, вступ більшості з них до ЄС та НАТО, а надто українська Революція Гідності знищили й до того хитку ідею про відродження радянської спільності.

Вихід 12 липня 2021 року статті путіна «Про історичну єдність росіян та українців» засвідчив остаточний поворот в пошуку історичної героїчної основи росії в сторону Київської Русі та величі перемоги в так званій Великій Вітчизняній війні. І якщо теза про єдність трьох братніх народів та колиску християнства під захистом москви не знайшла широкої підтримки пересічних росіян, то титул «народа побєдітєля», який не програв жодної битви і захистив світ від нацистів та фашистів стала тим довгоочікуваним підґрунтям виправдання будь-яких проявів агресії та воєнних злочинів [4].

Виявилося, що в росіян тема війни, а головне «великої перемоги», що прийшла після звільнення від гітлерівської армії держав Східної й Центральної Європи, викликає настільки високу емоційну ностальгію, що може слугувати не лише обґрунтуванням доцільності війни з Україною, але й працювати на «внутрішній ринок» для здійснення мобілізації й виправдання будь-яких економічних чи політичних обмежень. Ось чому одна із перших російських

ІПСО про «розп'ятого хлопчика в трусіках» – сюжет на російському телеканалі про нібито страту хлопчика українськими військовими під час звільнення Слов'янська у 2014 році, попри його подальше спростування, укорінився у свідомості росіян як доказ того, що українці є нацистами [5]. Усі подальші сюжети про: «біолабораторії» (подається як аналог нацистських біологічних експериментів), мітки для наведення ракет (мали провести паралелі з партизанським рухом опору Другої світової війни і підживити ідею про не сприйняття «київської влади» народом України, а в подальшому – виправдати тезу про «рятувальну спецоперацію»), масові здачі українців в полон (висвітлювалися з аналогією корінного перелому 1943 року, коли під Сталінградом німці масово здалися в полон), підготовку до перемовин і капітуляцію України через відсутність західної допомоги (акцент робився саме на капітуляцію, знову ж таки, щоб зайвий раз акцентувати на «священній переможній місії росії у війні з нацизмом») лише розширювали межі сприйняття пересічним росіянином війни з Україною як «священної», заради якої можна понизити моральний бар'єр та бути готовим терпіти всі незручності економіки держави, що веде цю війну.

Скандали навколо ТЦК, особливо пов'язані із замахом на життя військових, теж є професійно спланованою, і на жаль, певною мірою вдало проведеною російською ІПСО. Росія прагне створити картинку, що в Україні назріває внутрішній спротив війні, а мобілізація через залучення на контракт 18-річних нагадує ситуацію в агонізуючій гітлерівській Німеччині, де в останні місяці перед капітуляцією намагалися мобілізовувати не навчену молодь. При цьому паралельно нав'язується думка, що мирним прагненням українців, які втомилися від війни, заважає «київська хунта», яка відправляє на смерть своїх громадян. Кінцева мета такої ІПСО – внутрішній спротив і громадянська війна в Україні, на тлі яких можна буде протягнути ідею виборів і поставити ручне керування. І в цьому кейсі лише питання до сформованого критичного мислення українців та їх імунітету на ворожі інформаційні вкиди [6].

Небезпека ІПСО полягає в тому, що попередити чи завадити їх появі практично неможливо. Величезна ж включеність в реалізацію одного кейсу ІПСО широкого кола фахівців, навчених впливати на поведінкові реакції людей, ускладнює процес розвінчування вже сформованого впливу й подолання його наслідків. Об'єкт дії ІПСО завжди залишається в програшній позиції, адже він має обмежений інструментарій впливу – лише верифіковані дані й баланс думок. Ось чому перед журналістами в умовах війни стоїть першочергове завдання формування інформаційної гігієни та відмова від поширення новин з не перевіреним фактажем. Перед юристами ж постає виклик нормотворчої діяльності в сторону посилення відповідальності за порушення журналістських стандартів, маніпулювання інформацією та використання інформації в цілях, що шкодять національній безпеці. ІПСО, їх складові та методи, мають бути криміналізовані та прирівняні до злочинів, що несуть загрозу територіальній цілісності й безпеці держави.

Отже, ІПСО є вагомою складовою сучасних гібридних воєн, що потребує детального аналізу та посиленої законотворчої діяльності, у першу чергу в

частині обґрунтування прирівнення поширення ворожих наративів до колабораціонізму.

Список використаних джерел

1. «ІПСО і люди»: Рена Марутян про смислові війни. Центр протидії дезінформації. 2024. 28.06. URL: https://cpd.gov.ua/announcement/ipso-i-lyudy-rena-marutyan-pro-smyslovi-vijny/ (дата звернення: 06.06.2025).

2. Modrzejewski LtCol Zbigniew. Psychological operations after the Second World War. С. 74-99. URL: https://securityanddefence.pl/pdf-103237-36119?filename=36119.pdf (дата звернення: 06.06.2025).

3. Стенлі Дж. Як діє фашизм. Політика «ми» і «вони» / Пер. з англ. Я. Войтка. Київ: Видавнича група КМ-БУКС, 2025. 200 с.

4. Путін опублікував статтю про Україну, у якій апелює до «єдності росіян та українців». Детектор медіа. 2021. 12 липня. URL: https://detector.media/infospace/article/190048/2021-07-12-putin-opublikuvav-stattyu-pro-ukrainu-u-yakiy-apelyuie-do-iednosti-rosiyan-ta-ukraintsiv/ (дата звернення: 06.06.2025).

5. Дудченко А. «У трусіках, як Ісуса прибили на дошку»: як росіяни 10 років тому створили фейк про «розіп'ятого хлопчика» і які «шедеври» генерують зараз. Вчасно. 2024. 12 липня. URL: https://vchasnoua.com/news/u-trusikax-iak-isusa-pribili-na-dosku-iak-rosiiani-10-rokiv-tomu-stvorili-feik-pro-rozipiatogo-xlopcika-i-iaki-sedevri-generuiut-zaraz (дата звернення: 06.06.2025).

6. Ліскович М. Як російські спецслужби причетні до вбивства військових ТЦК. Укрінформ. 2025. 4 лютого. URL: https://www.ukrinform.ua/rubric-ato/3956165-ak-rosijski-specsluzbi-pricetni-do-vbivstva-vijskovih-tck.html (дата звернення: 06.06.2025).

Пікуля Тетяна Олександрівна,
професор кафедри теоретичної юриспруденції Київського національного економічного університету імені Вадима Гетьмана, кандидат юридичних наук, доцент

ПРАВОВЕ ТА ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІД ЧАС ВОЄННОГО СТАНУ ТА ПОВОЄННОГО ПЕРІОДУ

У сучасних умовах воєнного стану та післявоєнного відновлення інформаційна безпека суспільства набуває критичного значення, оскільки військові дії та гібридні загрози посилюють вразливість державних і цивільних інформаційних інфраструктур. Закон України «Про правовий режим воєнного стану» чітко визначає повноваження органів державної влади й місцевого самоврядування щодо захисту інформаційного простору та гарантування прав і свобод громадян під час введення воєнного стану [1]. Одночасно Указ

Президента України № 64/2022 зобов'язав оперативно впроваджувати заходи кіберзахисту як невідкладні державні інтереси, що вимагає узгодженої взаємодії військових адміністрацій, сектору безпеки і оборони та операторів критичної інфраструктури [2].

Відповідно до рішення Ради національної безпеки і оборони України від 14 травня 2021 року затверджено «Стратегію кібербезпеки України» як основоположний документ державної політики, що закладає принципи стримування, кіберстійкості та міжнародної співпраці, а також визначає ключові напрями посилення спроможностей суб'єктів сектору кібербезпеки для протидії атакам воєнного характеру й кібершпигунству [3]. У період воєнного стану ці положення мають доповнюватися нормами щодо пріоритетного захисту державних електронних систем та безперебійного функціонування засобів комунікації, а після завершення бойових дій – планами відновлення та модернізації за підтримки міжнародних партнерів.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» встановлює базові вимоги до об'єктів та суб'єктів захисту інформації, визначає порядок контролю доступу, відповідальність за порушення й механізми міжвідомчої взаємодії [4]. Проте в умовах воєнного стану слід розширити повноваження відповідальних органів, передбачивши прискорені процедури підтвердження відповідності систем критичної інфраструктури вимогам захисту, а також запровадити державний резерв спеціалістів і обладнання для негайного реагування на інциденти.

Відновлення післявоєнного періоду має спиратися на довгострокові програми підвищення кваліфікації державних службовців, кіберспеціалістів і IT-аудиторів, зокрема шляхом створення навчальних центрів при ключових відомствах. Не менш важливим є розвиток медіаграмотності громадян і формування культури інформаційної гігієни задля зниження ризиків дезінформації та ворожої пропаганди.

Лише комплексна реалізація правових, організаційних та технологічних заходів – від негайного захисту в умовах воєнного стану до системної модернізації та навчання у повоєнний час – забезпечить стійкість інформаційного простору держави та безпеку громадян від поточних і майбутніх кіберзагроз.

Отже, забезпечення інформаційної безпеки суспільства в умовах воєнного стану та в повоєнний період потребує злагодженої роботи державних органів, чітких правових норм, оперативних технологічних рішень і системи навчання фахівців, а також підвищення медіаграмотності громадян; лише така комплексна стратегія – від пріоритетного захисту критичної інфраструктури й швидкого реагування на кібератаки до довгострокових програм відновлення, модернізації та просвітницьких ініціатив — здатна гарантувати стійкість інформаційного простору та безпеку держави й кожного її громадянина.

Список використаних джерел

1. Про правовий режим воєнного стану : Закон України від 12.05.2015 р. № 389-VIII. Верховна Рада України. URL: https://zakon.rada.gov.ua/go/389-19 (дата звернення: 16.05.2025 р.).
2. Про введення воєнного стану в Україні : Указ Президента України від 24 лютого 2022 р. № 64/2022. Офіційне інтернет-представництво Президента України. URL: https://www.president.gov.ua/documents/642022-41397 (дата звернення: 16.05.2025 р.)
3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 р. «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. Верховна Рада України. URL: https://zakon.rada.gov.ua/go/447/2021 (дата звернення: 16.05.2025 р.).
4. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. ІПС «ЛІГА:ЗАКОН». URL: https://ips.ligazakon.net/document/z008000?ed=2020_06_04 (дата звернення: 16.05.2025 р.).

Тараніч Євген Анатолійович,
викладач кафедри поліцейської діяльності Національної академії внутрішніх справ, кандидат юридичних наук

ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Проблема забезпечення прав людини та національної безпеки для сучасної України є пріоритетною. Як відомо, права людини є невід'ємним надбанням всіх людей, незалежно від раси, кольору шкіри, статі, мови, релігії, національного чи соціального походження, або будь-яких інших обставин. Права людини включають право на життя і свободу, свободу від рабства та тортур, свободу переконань та їх вільне вираження, право на працю та освіту й багато інших. Вказані права повинні мати всі люди, без будь-якої дискримінації. При цьому права людини розглядаються паралельно з обов'язками. Порушення цього правила призводить до зловживання правами і свободами, негативних наслідків для соціуму і держави, загрожує національній безпеці.

Зміст національної безпеки охоплює безпеку людини, суспільства і держави. Особиста безпека передбачає наступне: відсутність загроз від будь-кого у межах кордонів держави; використання громадянами всіх, передбачених конституцією прав; верховенство закону, юридична рівність та справедливість; можливість брати участь у суспільному житті та реалізувати всі законні інтереси.

Вказаним правам і свободам можуть загрожувати різні фактори. Національній безпеці загрожує війна, що веде Росія проти України, корупція, несправедливість, глибоке розшарування суспільства на багатих і бідних, до числа останніх вже належить більшість громадян. Нині особливої гостроти набуває загроза криміналізації суспільних відносин, поява нових

правопорушень, які раніше такими не визнавались. Причини цього в істотних прорахунках, що мали місце на початкових етапах проведення реформ в різних сферах, перш за все в економіці та правоохоронній діяльності, недосконаліть та застарілість законодавчої бази, деформація правосвідомості населення, зниження морального потенціалу суспільства. Проблемою є також відсутність контролю за виконанням обов'язків як громадянами, так і державою щодо громадян. Держава сама в деяких випадках змушена обмежувати права громадян з огляду на загрози національній безпеці. Однак є певні межі, за які держава не повинна виходити.

Загрози безпеці виникають переважно не через фактори, що впливають на державу, тобто політичну боротьбу партій, взаємодію гілок влади, зміни урядів і т. ін. Здебільшого вони залежать від факторів, які впливають на громадянське суспільство, таких як зниження якості та рівня життя, економічні та фінансові кризи, рівень злочинності, міжнаціональні конфлікти. Саме незбалансованість у соціальній практиці інтересів суспільства, держави, різних соціальних груп та конкретної особистості є однією з найбільш серйозних проблем країни, від вирішення якої залежить стабільність соціуму.

На особливу увагу заслуговує особиста безпека, економічна, політична, продовольча, екологічна, суспільна безпека, якій загрожують раптові та небезпечні потрясіння, що руйнують звичний спосіб життя. Держава зобов'язана захищати своїх громадян у випадку викликів, загроз безпеці та з появою будь-яких ризиків.

Значна роль у забезпеченні безпеки людини належить кримінально-правовому регулюванню, реалізації охоронної функції кримінального права. Організація кримінально-правової охорони людини від злочинних посягань являє собою лише частину багатопланової проблеми забезпечення безпеки особи. За необхідності держава має створювати та утримувати мережу спеціальних установ для маргінальних верств населення: алкоголіків, наркоманів, волоцюг, соціально небезпечних дітей та підлітків, які не досягли віку кримінальної відповідальності, а також контролювати виконання санітарно-гігієнічних норм. У всіх розвинених країнах діють спеціалізовані медико-реабілітаційні центри для десоціалізованих категорій громадян і цей факт не розглядається як порушення прав людини.

Зараз головна проблема реального забезпечення прав людини у кримінальному процесі лежить, на жаль, не в процесуальній, а в політичній площині. Притягненні до кримінальної відповідальності олігархів та високопоставлених осіб чинне законодавство нерідко порушується, причому завжди на користь правопорушників. Щодо пересічних громадян ситуація протилежна: до них нерідко застосовуються методи протиправного впливу в процесі проведення як оперативних та слідчих заходів, так і при відбуванні покарання. Суспільство все більше переконується, що сьогодні держава захищає не стільки економічну безпеку держави, скільки безпеку вузької групи осіб та структур, що привласнили національні багатства та ряд функцій держави.

Істотну загрозу безпеці людини складає несправедливість, нерівність, зокрема економічна. Величезний розрив між бідними і багатими призводить до

виключення людини з низькими доходами із суспільства, що провокує соціальну нестабільність та порушення прав людини. На перший погляд права людини виявляються безсилими та неефективними у боротьбі зі зростаючою економічною нерівністю, адже вони орієнтовані на мінімальні або достатні потреби, тому їх недостатньо для досягнення справедливості. Однак все ж таки права людини є причиною обмеження нерівності, вони можуть певною мірою допомогти нам обмежити національну та глобальну економічну нерівність і заповнити простір глобальної справедливості. Якщо існують глобальні норми справедливості крім прав людини, вони, ймовірно, дадуть додаткові причини небезпеки матеріальної нерівності.

На державу покладається обов'язок забезпечення національної безпеки, запобігання загрозам щодо добробуту суспільства та якості життя громадян країни. Головною умовою захисту прав громадян є сильна державна влада, яка спирається на закон, та дієве громадянське суспільство, що толерантно ставиться до принципів правової держави. Потрібний розумний баланс між правами та обов'язками, між інтересами особистості, суспільства та держави.

Юридична наука мусить обґрунтувати як механізми забезпечення прав людини в державі, так і способи подолання протиріч між правами і свободами людини та необхідністю, що можливо на основі усвідомлення цінності людської особистості та узгодження їх із факторами стабільності держави, забезпечення національної безпеки.

Список використаних джерел

1. Про національну безпеку України: Закон України від 21.06.2018р. № 2469-VIII: станом на 31 березня 2023 р. URL.: https://zakon.rada.gov.ua/laws/show/2469-19#Text

2. Дзьобань О.П., Жданенко С.Б. Права людини і національна безпека: філософсько-правові аспекти взаємозв'язку. *Інформація і право*. 2020. № 2 (33). С. 9-22. URL.: https://ippi.org.ua/sites/default/files/3_16.pdf

3. Мелеганич Г.І. Суспільна безпека в Україні: теоретичний та практичний аспекти. *Політичне життя*. 2019. № 4. С. 39-44. DOI 10.31558/2519-2949.2019.4.6

4. Павленко І., Нагірний В., Потапенко В., Маляревський Є. Аналіз загроз національній безпеці у сфері внутрішньої політики. 2023. https://doi.org/10.53679/NISS-analytrep.2023.06

Тарахонич Тетяна Іванівна,
старший науковий співробітник Інституту держави і права імені В.М. Корецького НАН України, кандидат юридичних наук, старший науковий співробітник

УПОРЯДКУВАННЯ ЗАКОНОДАВСТВА В УМОВАХ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Проблема упорядкування законодавства, надання йому дієвості та ефективності була і залишається актуальною особливо в умовах дії режиму воєнного стану, необхідності збереження державного суверенітету, забезпечення національної та інформаційної безпеки. Сучасні зміни у світовому правопорядку, в українському суспільстві та державі потребують вагомих кроків у даному процесі.

На думку Н.М. Пархоменко «упорядкування законодавства - доволі широке поняття, що охоплює систематизацію, різновидами якої є інкорпорація, кодифікація, консолідація законодавства. Окрім того, упорядкування законодавства означає і його облік, і ревізію. Можливим є упорядкування законодавства відповідно до певних вимог чи обставин зокрема, це може бути воєнний стан, входження у європейський правовий простір, вступ до міжнародних альянсів та блоків тощо. У зв'язку з цим зазвичай йдеться про окремі складові законодавчого масиву або загальні засади, які потребують упорядкування шляхом узгодження законодавства з конкретними вимогами, принципами, стандартами. У такому випадку упорядкування відбуватиметься шляхом уніфікації, адаптації, гармонізації, імплементації, стандартизації та ін. форм удосконалення законодавства. Така діяльність потребує опрацювання не лише чинних правових актів, а й розробки і прийняття нових, скасування не діючих»[1, с. 28-29].

Слід констатувати, що процес упорядкування законодавства досить часто не вивчається в теорії права як самостійний теоретико-правовий феномен. Поряд з цим, його розглядають крізь призму новелізації, модернізації законодавства, його реформування, удосконалення та розвитку. Окрім того, упорядкування законодавства також аналізується через його види, а саме: систематизацію та ревізію.

З огляду на зазначене В.І. Риндюк підкреслює, що «в юридичній літературі використовується цілий ряд близьких за значенням термінів для позначення тієї діяльності, об'єктом (предметом) якої є законодавство. Наявні дефініції цих термінів містять взаємні суперечності, і не дають можливості встановити більш менш чітке співвідношення між ними, визначити необхідні їх взаємозв'язки та з'ясувати особливості і місце упорядкування законодавства, що є предметом нашого дослідження, предмета, що залишається дискусійним у сучасній теорії права і тому потребує подальших наукових досліджень» [2, с. 27].

Потреба приведення законодавства до певних вимог обумовлена не лише входженням до європейського правового простору, особливостями національної правової системи, воєнними діями, а і проблемами забезпечення національної та інформаційної безпеки тощо. Слід погодитися з думкою Н.М. Пархоменко, що «правовий масив потребує ревізії щодо відповідності об'єктивно існуючим суспільним відносинам (виявлення застарілих правових актів); існування об'єктивної потреби у правовому впливі; конституційності та відповідності міжнародним принципам та європейським стандартам; узгодженості між правовими системами різної юридичної сили та різних суб'єктів правотворчості; здатності справляти регулятивний вплив на суспільні відносини; існування механізмів реалізації правових приписів і подолання декларативності права тощо» [3, с. 32].

На даний процес впливає цілий ряд чинників об'єктивного та суб'єктивного характеру, серед яких слід виокремити наступні: потреба приведення законодавства до європейських вимог шляхом його гармонізації, уніфікації, адаптації, стандартизації та зближення; необхідність подолання недосконалості законодавства, наявних прогалин та колізій, дублювань та множинності правових актів; необхідність приведення діючих норм права у відповідність до динамічного розвитку суспільних відносин, пов'язаних з новими інформаційними технологіями та запровадженням штучного інтелекту тощо.

Важливою складовою упорядкування законодавства є необхідність забезпечення національної та інформаційної безпеки. Так Т.А. Костецька зазначає, що «у сучасних реаліях, коли інформаційні технології вивели суспільні комунікації на принципово інший рівень, ніж попередні періоди, коли для України до першочергових завдань належить захист національних інтересів в інформаційній сфері, прогнозування зовнішніх та внутрішніх загроз національній безпеці держави, вироблення стратегії входження українського суспільства в трансграничний інформаційний простір, освоєння міжнародних стандартів інформаційного обміну та захисту інформаційних ресурсів тощо…» [4, с. 309].

Узагальнивши слід зазначити, що удосконалення законодавства, дотримання вимог щодо його якості, ефективності та результативності, його адаптація до міжнародних стандартів є стратегічним напрямом розвитку нашої держави, забезпечення її національної та інформаційної безпеки.

Реалії сьогодення, існуючі проблеми та загрози актуалізують питання правового регулювання інформаційної політики держави, її цифрової трансформації, уніфікації законодавства в інформаційній сфері суспільних відносин, приведення його до єдиної системи, ліквідація прогалин та колізій тощо.

Список використаних джерел

1. Пархоменко Н.М. Упорядкування законодавства як спосіб підвищення ефективності на сучасному етапі. *Альманах права.* Трансформація законодавства України в сучасних умовах. Вип. 14. Київ : Інститут держави і права імені В.М. Корецького НАН України, 2023. С. 27-34, С. 28-29.

2. Риндюк В.І. Упорядкування законодавства України; теоретико-методологічний та техніко-юридичний аспекти : монографія, Київ : КНЕУ, 2021. 407 с. С. 27.

3. Пархоменко Н.М. Правові засади нормотворчої діяльності: національний та зарубіжний досвід. *Альманах права.* Правовий моніторинг як складова правотворчого процесу. До 75-річчя Інституту держави і права імені В.М. Корецького НАН України. 2024. Вип. 15. Київ : Інститут держави і права імені В.М. Корецького НАН України, С. 32-37. С. 32.

4. Костецька Т.А. Про інформаційну функцію держави у контексті сучасної національної доктрини унітаризму. *Альманах права.* Роль правової доктрини у забезпеченні прав людини. 2020. Вип. 11. Київ : Інститут держави і права імені В.М. Корецького НАН України, С. 307-312. С. 309.

Шовкошитний Ігор Іванович,
кандидат військових наук, провідний науковий співробітник науково-дослідного відділу інституту інформаційно-комунікаційних технологій та кібероборони Національного університету оборони України
Старинський Іван Михайлович,
кандидат технічних наук, старший науковий співробітник науково-дослідного відділу інституту інформаційно-комунікаційних технологій та кібероборони Національного університету оборони України
Міненко Людмила Миколаївна,
доктор філософії, старший науковий співробітник науково-дослідного відділу інституту інформаційно-комунікаційних технологій та кібероборони Національного університету оборони України
Василенко Ольга Анатоліївна,
ад'юнкт, ЦНДІ Збройних Сил України

КОНЦЕПТУАЛЬНІ ПОГЛЯДИ ЩОДО ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

У сучасних умовах ведення війни технологічна перевага стає критично важливою для забезпечення національної безпеки. Збройні Сили (ЗС) України, перебуваючи в умовах повномасштабного протистояння, потребують

впровадження новітніх рішень, зокрема технологій штучного інтелекту (ШІ). Концептуальні підходи до інтеграції ШІ в оборонний сектор мають враховувати не лише технічні, а й етичні, правові та стратегічні аспекти, спрямовані на підвищення ефективності бойових дій, управління військами та захисту особового складу.

На державному рівні зазначена проблематика окреслена двома постановами Кабінету Міністрів України, у яких у загальному вигляді обґрунтована потреба у розвитку технологій ШІ [1], зокрема в оборонній сфері, а також визначені елементи цільової науково-технічної програми з використання технологій ШІ в пріоритетних галузях економіки на період до 2026 року [2]. Проте напрямки впровадження таких технологій у ЗС України досі чітко не визначені, що й зумовлює актуальність розроблення відповідної концепції, яка відображатиме цілісну систему стратегічних, організаційних, технічних та етичних засад, які визначатимуть, як саме ШІ має інтегруватись у різних системах (аспектах діяльності) Збройних Сил України.

Для формування Концепції впровадження технологій ШІ в ЗС України, на наш погляд, необхідно вирішити низку взаємопов'язаних задач.

По-перше. Передусім слід визначити потенційні напрями впровадження ШІ в ЗС України. Це завдання має базуватись на результатах аналізу:

а) світових тенденцій впровадження технологій ШІ в системах військового призначення, концептуальних поглядів (концепцій, доктрин, стандартів, дорожніх карт, інші нормативних документів) військово-політичного керівництва інших країн світу, що вважаються передовими у військово-технічному відношенні;

б) потреб складових сектору безпеки і оборони (зокрема ЗС України) у використанні технологій ШІ, що сприятимуть більш оперативному та/або більш ефективному виконанню певних завдань та функцій у системах прийняття рішень, системах озброєння та військової техніки тощо;

в) потенційних обмежень існуючих технологій ШІ або їх практичного використання. В цьому плані значущими є питання: етичності та безпеки застосування ШІ у критичних ситуаціях; (наприклад, автономна зброя без контролю людини); недосконалості алгоритмів ШІ та пов'язаних із цим можливих помилок; уразливості до кібератак з боку противника; недостатньої адаптивності систем на основі ШІ до швидко змінюваних обставин і непередбачуваних сценаріїв на полі бою; залежності технологій ШІ від інфраструктури (зв'язку, енергопостачання і обчислювальних ресурсів).

Проте попередній аналіз можливостей існуючих технологій ШІ у військовій сфері свідчить про їх використання для: автоматизації бойових з впровадженням елементів ШІ у системах розвідки, спостереження та ураження цілей; збирання та аналізу великих обсягів даних (Big Data) в інформаційно-аналітичних системах з метою виявлення загроз, прогнозування і планування застосування сил і засобів у реальному часі; виявлення та нейтралізація кібератак, аномальної активності в мережах (проблема кіберзахисту); оптимізації процесів управління операціями, автоматизації процесів прийняття рішень у системах військового управління; підготовки військових кадрів у симульованих бойових умовах з

використанням навчальних систем, тренажерів на основі віртуальної і доповненої реальності (VR), які моделюють складні бойові сценарії; розпізнавання об'єктів (цілей) або потенційних загроз; вирішення (оптимізації) завдань логістики та постачання (автоматизація управління ресурсами, прогнозування потреб, оптимізації маршрутів постачання тощо).

По-друге, рішення щодо впровадження технологій штучного інтелекту в ЗС України мають бути науково обґрунтованими. Тому логічним важливим питанням буде розроблення методологічних засад технологій ШІ та вибору напрямів їх впровадження в системах військового призначення. Основи методології, на наш погляд обов'язково мають включати:

а) основні концепції та принципи ШІ. Зокрема, нині відомі такі основні концепції ШІ: імітація людського інтелекту; машинне навчання (ML); методологія навчання ШІ на основі даних (контрольоване навчання (supervised learning), неконтрольоване навчання (unsupervised learning); навчання з підкріпленням (reinforcement learning)); глибинне навчання (Deep Learning); обробка природної мови (NLP); комп'ютерний зір на основі ШІ; інтеграція ШІ в фізичні системи (робототехніка));

б) класифікацію існуючих технологій ШІ (машинне навчання, нейронні мережі, обробка даних тощо). Класифікація технологій ШІ може здійснюватися за різними критеріями: рівень інтелекту, функціональні можливості, типи завдань, сфери застосування тощо;

в) етичні аспекти застосування ШІ у військовій сфері. Принципово важливим при цьому є: дотримання міжнародного гуманітарного права; заборона автономних систем з правом прийняття рішень про ураження; прозорість і пояснюваність алгоритмів, що приймають рішення; запобігання (зниження) ризику технічних і програмних збоїв у системах на основі ШІ, що вимагає впровадження заходів щодо їх тестування і сертифікації або зловмисному використанню; пошук балансів, розроблення міжнародних угод, які регулюють використання ШІ у військовій сфері; етичне використання даних; гуманітарний аспект; мінімізація потенційних людських втрат; відповідальність і підзвітність суб'єктів, що використовують системи на основі ШІ;

г) особливості впровадження ШІ в системах військового призначення. При цьому, на нашу думку, технології ШІ у таких системах мають впроваджуватись у системах управління операціями (бойовими діями), розвідки та аналізу даних, кіберзахисту (протидії кіберзагрозам), а також в автономних системах (БпЛА, роботизованих платформах тощо). Крім того, важливим питанням буде розроблення системи критерії ефективності та безпеки впровадження технологій ШІ;

д) методика вибору напрямів впровадження ШІ, яка має базуватись на врахування взаємодії груп факторів «ефекту-ризику» та «потреб-можливостей».

Сформовані методологічні засади дозволять сформувати концепцію та практичні рекомендації щодо пріоритетних напрямів використання технологій штучного інтелекту в системах військового призначення Збройних Сил України.

З урахуванням визначення поняття “концепція” та підходів до її формування [3], як варіант розроблювана “Концепція впровадження технологій штучного інтелекту в Збройних Силах України” може мати такі структурні елементи:

1. Загальні положення, у яких визначатиметься актуальність впровадження ШІ у військовій сфері, цілі та завдання Концепції, ключові поняття й терміни.
2. Аналіз існуючої проблеми з оглядом стану впровадження ШІ у ЗС провідних країн світу, існуючих розробок і технологій у сфері ШІ в Україні, потенціалу України у створенні та інтеграції технологій ШІ.
3. Пріоритетні напрями впровадження ШІ в ЗС України (основні з них наведені вище).
4. Етапи реалізації Концепції: короткостроковий (1–2 роки) – пілотні проєкти та дослідження; середньостроковий (3–5 років) – масштабування успішних рішень; довгостроковий (5–10 років) – інтеграція технологій ШІ у всі рівні управління та бойових дій.
5. Організаційні та правові аспекти (створення нормативно-правової бази для використання ШІ у військовій сфері, впровадження стандартів і протоколів сумісності систем, забезпечення етичного використання ШІ відповідно до міжнародного права).
6. Ресурси для реалізації Концепції (фінансування програм та проєктів, підготовка кадрів та освітні ініціативи, співпраця з приватним сектором, науковими установами та партнерами).
7. Очікувані результати.
8. Моніторинг і оцінка ефективності впровадження з визначенням: ключових показників ефективності; механізми контролю та корекції Концепції.
9. Висновки та рекомендації (узагальнення стратегічних переваг впровадження ШІ у ЗС України, подальші кроки для досягнення цілей).

Отже очевидно, що в сучасних умовах технології ШІ стають життєво необхідними для досягнення переваги над противником. Запропоновані концептуальні погляди, за умови їх реалізації, сприятимуть обґрунтованому прийняттю рішень щодо впровадження зазначених технологій в Збройних Силах України. Результатом реалізації Концепції, на наш погляд, буде: підвищення ефективності військового управління та виконання бойових завдань, оптимізація ресурсів та зниження втрат в операціях (бойових діях), підвищення технологічної незалежності та загалом посилення обороноздатності України.

Список використаних джерел

1. Концепція розвитку штучного інтелекту в Україні. Розпорядження Кабінету Міністрів України від 02 грудня 2020 р. № 1556-р. URL: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220.
2. Про схвалення Концепції Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року. Розпорядження Кабінету Міністрів України від 13 квітня 2024 р. № 320-р. Київ. 2024. URL: https://zakon.rada.gov.ua/laws/show/320-2024-%D1%80#Text

3. Концепція. Encyclopedia of Modern Ukraine. URL: https://esu.com.ua/article-3256.

НАУКОВІ ПОВІДОМЛЕННЯ

Базиляк Ірина Олегівна,
студент навчально-наукового експертно-криміналістичного інституту Національної академії внутрішніх справ

ХАКТИВІЗМ ЯК ФЕНОМЕН СУЧАСНОГО КІБЕРПРОСТОРУ

Хактивізмом називають синтез соціальної активності та хакерства, використання компютерів та компютерних мереж для просування політичних ідей, забезпечення свободи слова та інформації, прав людини [1, С.109].

Хактивісти – це окремі особи, чи групи осіб, які займаються онлайн-активністю, з метою впливу на суспільство або просування певної теми у громадському чи політичному житті. Вони не отримують прибутків, не крадуть гроші в жертв взлому – їм просто потрібно дістати якусь важливу інформацію для привернення уваги на когось або на деякий час паралізувати чиюсь діяльність. Цілями атаки можуть бути різні об'єкти – від електронної пошти топ-менеджера компанії і до сервера, на якому є база даних її співробітників, постачальників, клієнтів [2].

Незважаючи на те, що діяльність хактивістів спрямована на привернення уваги громадськості до певних політичних, соціальних чи релігійних питань, розкриття певної інформації тощо, таке втручання є протиправним, а в багатьох країнах кримінально караним.

У контексті свободи слова хактивізм є формою цифрового протесту, але на правовому рівні питання досі не вирішено.

Хактивісти використовують у своїй діяльності різні методи і тактики. Найпоширенішими серед них є:

1. Дефейсинг веб-сайтів. За допомогою зміни зовнішнього вигляду, контенту або функціональності веб-сторінки, хакери можуть передати певне повідомлення або показати свої погляди.
2. DDoS-атаки, або атаки відмови в обслуговуванні. Під час неї використовуються кілька систем або пристроїв, щоб «затопити» ціль масовим обсягом трафіку, що унеможливлює її роботу. Створюючи незручності в роботі онлайн-сторінки, хактивісти привертають увагу до певного питання.
3. Витік даних. Хактивісти можуть отримати доступ до баз даних або систем, з метою розкриття конфіденційної або секретної інформації, щоб викрити неправомірні дії та привернути увагу до проблем, що ігноруються. Витік інформації може призвести до несанкціонованого розкриття особистої інформації та урядових даних [3].

Даний вид кіберзлочинності зародився ще у 80-х роках минулого століття, паралельно із розвитком Інтернету. Перші атаки мали дещо анархічну мету: комп'ютерні генії хотіли показати владі, що здатні пробити захист мережі. Згодом, атаки мали й ідеологічні мотиви: у 1989-му австралійські противники атомної енергетики запустили у мережі NASA та Міністерства енергетики США

вірус англ. WormsAgainstNuclearKillers (укр. Черв'яки Проти Ядерних Вбивць). Таким чином вони протестували проти першого запуску шатлу із радіоактивним плутонієм на борту.

Політизація і перехід Інтернету в комерційну площину прискорили розвиток хактивістського руху. Після розпаду Югославії та війни на Балканах, сербські хакери регулярно втручались у роботу ресурсів НАТО, щоб висловити свій протест діям Альянсу, які вони вважали агресією. Також вони публікували в мережі докази військових злочинів, які здійснювалися югославською армією [4].

Однією з відомих міжнародних груп хакерів-хактивістів є Anonymous. Його адепти виступають проти цензури, нагляду і переслідування у віртуальному просторі. Якщо окремі особи, компанії або уряди діють проти переконань хактивістів, «анонімуси» відповідають їм зломом сайтів і систем безпеки. Сьогодні на їхньому рахунку цілий ряд протестів і акцій [5]. Одними з таких є взлом у 2022 всіх державних телеканалів рф, сайту Федеральної Служби Безпеки рф, ще цілої низки прокремлівських ресурсів [6].

В Україні також здійснюють діяльність групи хактивістів. «Жертвами» їхніх атак стали сервери виробничого підприємства рф, які підтримують агресивні дії росії щодо України – на їхніх веб-сторінках з'явилась картинка з написом «1999-2024. 25 років війни ФСБ з власним народом» і зображенням путіна на тлі підірваних будинків у Рязані [7].

Також була здійснена атака на сайт, який є онлайн-платформою проєкту «Безсмертний полк росії», що використовує пам'ять героїв Другої світової війни для виправдання сучасної агресії проти України [8]. Крім цього, хактивістам «Кібер Супротиву» та KibOrg вдалось завантажити шпигунський вірус на особистий комп'ютер командувача сил рф на Запорізькому напрямку А. Романчука. Операція спостереження, яка тривала понад півтора роки дала змогу отримати інформацію про плани ворога, місцезнаходження його сил та розвідувальних засобів [9].

Хоча на даний час діяльність хактивістів розглядається як незаконна, але її можна використовувати з користю. Наприклад, як інструмент в інформаційній війні, а також для отримання розвідувальних даних про ворога тощо. Тому дане питання є дуже актуальним в сучасних умовах та потребує правового регулювання.

Список використаних джерел

1. Варналій Є.О., Єсіна О.Г. Хакерство як соціальне явище. *Інформатика та інформаційні технології*. Одеса : ОНЕУ. С. 107-109.

2. 5 типів кіберзлочинців. *АрміяInform.* веб-сайт. URL : https://armyinform.com.ua/2022/01/31/5-typiv-kiberzlochyncziv/

3. Визначення хактивізму. веб-сайт. URL : https://www.vpnunlimited.com/ua/help/cybersecurity/hacktivism?srsltid=AfmBOoqlLPqnuffcwGOCopY74hYpgJuAilxtbEHqu0F_JSvUcw3NwIhc

4. Як хактивісти змінюють природу соціальних протестів. *Український тиждень.* веб-сайт. URL : https://tyzhden.ua/iak-khaktyvisty-zminiuiut-pryrodu-sotsialnykh-protestiv/

5. Anonymous: історія створення та успіху «Анонімус». *WorldBank.* веб-сайт. URL : https://worldbank.org.ua/4616-anonymous.html

6. Даємо 48 годин. Anonymous закликали західні компанії припинити роботу в Росії. *Суспільне новини.* веб-сайт. URL : https://suspilne.media/amp/220003-daemo-48-godin-anonymous-zaklikali-zahidni-kompanii-pripiniti-robotu-v-rosii/

7. Хактивісти нагадали росіянам, як путін підривав мирних людей 25 років тому. *АрміяInform.* веб-сайт. URL : https://armyinform.com.ua/2024/09/22/haktyvisty-nagadaly-rosiyanam-yak-putin-pidryvav-myrnyh-lyudej-25-rokiv-tomu/

8. Хактивісти «Кібер-АТЕШ» вивели з ладу сайт пропагандистського проєкту «Безсмертний полк». *Ukr.net.* веб-сайт. URL : https://www.ukr.net/news/details/technologies/111210691.html

9. Українські хактивісти зламали комп'ютер командувача сил РФ на Запорізькому напрямку: побачене шокує (фото, відео). *TSN.* веб-сайт. URL : https://tsn.ua/ato/ukrayinski-haktivisti-zlamali-komp-yuter-komanduvacha-silami-rf-na-zaporizkomu-napryami-foto-video-2701356.html

Білодід Катерина Сергіївна,
курсант навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ

СОЦІАЛЬНІ МЕРЕЖІ ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ ВІЙНИ: АТАКИ, ФЕЙКИ ТА ПРОТИДІЯ

У сучасному світі соціальні мережі перетворилися на потужний інструмент, що виходить далеко за рамки простого спілкування чи самовираження. Вони стали могутнім важелем впливу на колективну свідомість, формування суспільної думки, поширення інформації, мобілізацію населення, а також організацію як патріотичної активності, так і протестних рухів. Особливої ваги соцмережі набули в умовах гібридної війни, яка поєднує як військові, так і інформаційні аспекти.

Інформаційна війна ґрунтується на цілеспрямованому поширенні фальшивої або маніпулятивної інформації. Її мета – дестабілізувати суспільство, підірвати довіру до державних установ, знизити моральний дух населення та оборонних сил. У цьому контексті соцмережі демонструють свою вразливість: вони слугують ідеальним середовищем для дезінформації завдяки швидкості поширення вмісту, масштабній аудиторії та відсутності належного контролю за достовірністю інформації.

Серед найбільш небезпечних проявів інформаційної війни в соціальних мережах – поширення фейкових новин [1]. Такі повідомлення спеціально створюються або навмисно викривляються, вводячи аудиторію в оману стосовно подій, осіб чи явищ. Щоб ускладнити розкриття фейків, застосовуються хитрощі, зокрема використання стилю офіційних джерел, емоційно насиченої мови, супровід фото- та відеоматеріалами.

Сучасні підходи до ведення інформаційної війни в соціальних мережах включають створення мереж ботів і фейкових акаунтів, маніпуляції через таргетовану рекламу та використання алгоритмів для просування потрібного контенту. Ці технології дозволяють швидко змінювати акценти у публічному дискурсі, відволікати увагу громадськості від важливих питань та формувати вигідне агресорові сприйняття подій.

У відповідь на такі виклики правоохоронні органи повинні адаптувати свою діяльність до реалій інформаційних загроз. Їхня роль сьогодні охоплює не лише забезпечення фізичної безпеки, але й систематичний моніторинг інформаційного простору. Критично важливим стає виявлення джерел дезінформації, ідентифікація осіб, які залучені до деструктивної діяльності, та нейтралізація їхнього впливу [2]. Усе це потребує освоєння нових компетентностей, тісної співпраці з кіберполіцією та Службою безпеки України, а також використання сучасних технологічних рішень.

В Україні зараз діє значна кількість ініціатив, спрямованих на боротьбу з фейками. Це включає платформи перевірки фактів, телеграм-канали для спростування дезінформації, а також кампанії, що популяризують медіаграмотність серед громадян. Однак проблема залишається надзвичайно актуальною через активну діяльність ворожих інформаційних операцій та обмежені можливості для продуктивної протидії.

Ефективна боротьба із поширенням фейкової інформації не обмежується технічними чи репресивними методами [3]. Вона вимагає відкритості державних структур, послідовної роботи з населенням, конструктивного діалогу з медіа та активної участі офіційних джерел у соціальних мережах. Прозора комунікація від імені держави суттєво зменшує вплив панічних настроїв і загрозливих дезінформаційних хвиль.

Окрему увагу потрібно приділяти захисту персональних даних користувачів у соцмережах, оскільки ці дані можуть стати інструментом для маніпуляцій. Їхній витік або незаконне використання створює можливість для цільових інформаційних атак, посилюючи їх ефективність. У цьому ключі надзвичайно важливе правове регулювання та застосування сучасних заходів кібербезпеки. У сучасних умовах роль кіберполіції значно зростає.

Ще однією важливою частиною протидії дезінформації є розвиток інформаційної культури громадян. Медіаграмотність – це уміння критично мислити, перевіряти джерела інформації та розпізнавати ознаки маніпуляцій. Відтак систематична робота у цьому напрямі має зайняти одну з провідних позицій у сферах освіти й професійної підготовки, особливо для фахівців правоохоронної сфери.

Таким чином, соціальні мережі в сучасних умовах війни є важливим інструментом поширення інформації. Їхня експлуатація агресором для поширення фейків, послаблення моралі населення та підриву довіри до правоохоронних органів стала одним із найгостріших викликів сьогодення. Проте саме ці платформи надають державі та громадянському суспільству можливість ефективно взаємодіяти та боротися з інформаційними загрозами.

Список використаних джерел

1. Інформаційні атаки в соціальних мережах: дослідження впливу російської дезінформації через рекламу в Facebook. Центр стратегічних комунікацій та інформаційної безпеки. URL: https://cedem.org.ua/wp-content/uploads/2024/05/informaczijni-ataky-v-soczialnyh-merezhah.-doslidzhennya-vplyvu-rosijskoyi-dezinformacziyi-cherez-reklamu-v-facebook.pdf (дата звернення: 16.05.2025).

2. Данько Ю. Соціальні мережі як інструмент інформаційної війни рф проти України: особливості та механізми протидії. *Сучасне суспільство: політичні науки, соціологічні науки, культурологічні науки*. Наукові фахові видання ХНПУ імені Г.С. Сковороди. 2023, Випуск 2 (27). С.54–66. URL: http://journals.hnpu.edu.ua/index.php/politology/article/view/14247

3. Савлюк М. Важливість інформаційної безпеки в соціальних мережах для загальнонаціональної безпеки: безпековий вимір України. *Вісник Прикарпатського університету. Серія: Політологія*. 2024. № 18. С.300–309. URL: https://journals.pnu.if.ua/index.php/politology/article/view/167

Богдан Ігор Васильович,
аспірант кафедри теорії держави та права Національної академії внутрішніх справ

ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ОБОРОННОЇ ФУНКЦІЇ УКРАЇНИ В КОНТЕКСТІ ВІДСУТНОСТІ ЧЛЕНСТВА В НАТО

Повномасштабна збройна агресія Російської Федерації проти України, що триває з лютого 2022 року, та пов’язана з нею стратегічна невизначеність щодо термінів і умов набуття Україною повноправного членства в Організації Північноатлантичного договору (НАТО) надають особливої актуальності дослідженню правових засад забезпечення оборонної функції Української держави. За відсутності колективних гарантій безпеки, передбачених статтею 5 Північноатлантичного договору, Україна постає перед унікальними юридичними викликами у реалізації свого невід’ємного суверенного права на оборону. Це вимагає глибокого правового аналізу наявних національних та міжнародно-правових механізмів, що забезпечують цю функцію, а також пошуку шляхів їх посилення.

Ключова проблема полягає у визначенні достатності та ефективності чинного національного законодавства та міжнародних угод України для гарантування її обороноздатності в умовах екзистенційної загрози поза системою колективної безпеки Альянсу. Необхідно критично оцінити наявні правові інструменти та виявити прогалини й потенційні напрями вдосконалення нормативно-правового забезпечення оборони.

Нормативно-правову основу оборонної функції України становить передусім її Конституція, яка закладає фундаментальні принципи та розподіл повноважень у цій сфері. Ключове значення має стаття 17, яка проголошує захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки найважливішими функціями держави та справою всього Українського народу. Цією ж статтею оборона України, захист її суверенітету, територіальної цілісності і недоторканності покладаються на Збройні Сили України, а забезпечення державної безпеки і захист державного кордону – на відповідні військові формування та правоохоронні органи держави. Таким чином, Основний Закон не лише визначає оборону як державну функцію, але й підкреслює її всенародний характер, що має важливі юридичні наслідки.

Розподіл повноважень у сфері оборони чітко визначений Конституцією. Стаття 106 наділяє Президента України статусом Верховного Головнокомандувача Збройних Сил України. Президент здійснює керівництво у сферах національної безпеки та оборони держави, очолює Раду національної безпеки і оборони України, вносить до Верховної Ради України подання про призначення Міністра оборони, а також у разі збройної агресії проти України приймає рішення про використання Збройних Сил України та інших військових формувань. Така концентрація повноважень в руках глави держави покликана забезпечити єдність командування та оперативність прийняття рішень, особливо в умовах воєнного стану.

Водночас, Конституція передбачає механізми парламентського контролю. Відповідно до статті 85 Верховна Рада України має повноваження щодо оголошення стану війни і укладення миру (за поданням Президента), а також схвалення рішення Президента про використання Збройних Сил України та інших військових формувань у разі збройної агресії проти України (повноваження щодо схвалення випливає з необхідності подання Президентом такого рішення до ВРУ згідно п. 19 ст. 106. Ця модель розподілу повноважень, хоча й забезпечує оперативність президентських рішень, містить потенціал для взаємодії та контролю з боку законодавчої гілки влади. Хоча в умовах повномасштабної агресії спостерігається високий рівень політичної єдності, юридична структура передбачає необхідність узгодження дій між Президентом та Парламентом у ключових питаннях війни та миру, що є важливим елементом системи стримувань і противаг.

Формулювання статті 17 Конституції про оборону як «справу всього Українського народу» має глибокий юридичний зміст, виходячи за межі простої декларації. Воно слугує конституційним обґрунтуванням для широкого кола обов’язків громадян щодо захисту Вітчизни, закріплених, зокрема, в Законі України «Про військовий обов’язок і військову службу». Більше того, цей

принцип легітимізує залучення до оборони не лише регулярних збройних сил, але й інших складових сектору безпеки і оборони, включаючи сили територіальної оборони та, в певних межах, організований рух спротиву та волонтерську діяльність, що знаходить своє відображення у концепції всеохоплюючої оборони України.

Окремий аспект становить конституційно закріплений стратегічний курс держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору. Відповідні зміни до Преамбули статей 85, 102, 116 Конституції, ухвалені у 2019 році, юридично зобов'язують державу здійснювати політику, спрямовану на досягнення цієї мети. Це безпосередньо впливає на оборонну сферу, вимагаючи постійної адаптації національного законодавства, структури та функціонування Збройних Сил та інших складових сектору безпеки і оборони до стандартів НАТО. Навіть за відсутності формального членства, цей конституційний імператив стимулює процес реформ у таких сферах, як оборонне планування, управління ресурсами, демократичний цивільний контроль, оперативна сумісність, що знаходить своє відображення і в міжнародних зобов'язаннях України, зокрема, у двосторонніх безпекових угодах.

В умовах відсутності членства в НАТО, міжнародно-правовою основою для захисту України від збройної агресії є передусім норми Статуту Організації Об'єднаних Націй. Стаття 51 Статуту закріплює «невід'ємне право на індивідуальну або колективну самооборону, якщо відбудеться збройний напад на Члена Організації». Це право є фундаментальним принципом сучасного міжнародного права і слугує беззаперечною легітимацією оборонних дій України проти агресії росії, незалежно від її участі чи неучасті у військових альянсах. Характеристика цього права як «невід'ємного» підкреслює його природний характер, пов'язаний із самим існуванням держави та її суверенітетом.

Право на самооборону згідно зі Статутом ООН, існує доти, доки Рада Безпеки ООН не вживе заходів, необхідних для підтримання міжнародного миру та безпеки. Однак, у ситуації, коли агресором є постійний член Ради Безпеки, що володіє правом вето (як у випадку рф), ефективність механізмів колективної безпеки ООН виявляється паралізованою. За таких умов реалізація Україною свого невід'ємного права на самооборону стає основним міжнародно-правовим інструментом захисту її суверенітету та територіальної цілісності. Статут також вимагає, щоб дії, вжиті державами при здійсненні права на самооборону, були негайно повідомлені Раді Безпеки.

Важливо чітко розуміти юридичний зміст статті 51 Статуту ООН. Хоча вона надає Україні беззаперечне право на захист від агресії, вона сама по собі не створює юридичного обов'язку для інших держав надавати їй військову чи іншу допомогу. Стаття 51 легітимізує оборонні дії самої України та дозволяє іншим державам надавати допомогу в рамках колективної самооборони, якщо вони ухвалять таке політичне рішення. Проте, вона не містить механізму примусу до надання такої допомоги. Ця обставина підкреслює критичну важливість укладання Україною додаткових міжнародних угод – двосторонніх чи

багатосторонніх – які б створювали конкретні юридичні зобов'язання для партнерів щодо надання підтримки.

Починаючи з січня 2024 року, Україна уклала значну кількість двосторонніх угод про співробітництво у сфері безпеки (або угод з подібними назвами) з ключовими міжнародними партнерами. Такі угоди були підписані з Великою Британією, Німеччиною, Францією, Данією, Канадою, Італією, Нідерландами, Фінляндією, Латвією, Іспанією, Бельгією, Португалією, Швецією, Ісландією, Норвегією, Японією, США, а також з Європейським Союзом як інституцією, та низкою інших країн. Ця мережа угод формує новий контур безпекової підтримки України поза структурами НАТО.

З юридичної точки зору, ці документи є міжнародними договорами, які створюють права та обов'язки для сторін у міжнародному праві. Вони укладаються у письмовій формі, регулюються міжнародним правом і породжують юридичні наслідки для їх учасників. Водночас, обсяг та характер зобов'язань визначаються положеннями самих угод та, як часто зазначається, національним законодавством сторін і наявністю відповідних ресурсів (фінансування).

Принципово важливим є те, що ці угоди не містять положень, аналогічних статті 5 Північноатлатничного договору про колективну оборону. Вони не передбачають автоматичного зобов'язання сторін надати військову допомогу, включаючи застосування збройної сили, у разі нового нападу на Україну. Натомість, угоди зазвичай встановлюють механізм консультацій. Наприклад, угода зі США передбачає, що у разі майбутнього збройного нападу або загрози такого нападу на Україну, сторони негайно, на прохання будь-якої зі сторін, проведуть зустрічі (по можливості протягом 24 годин) на найвищому рівні для визначення відповідних подальших кроків та додаткових потреб у сфері оборони. Подібні механізми консультацій містяться і в угодах з іншими країнами.

Основний зміст зобов'язань партнерів за цими угодами стосується надання Україні довгострокової та всебічної підтримки, яка включає: постачання озброєння та військової техніки; тренування та навчання українських військовослужбовців; обмін розвідувальною інформацією; допомогу в розвитку оборонно-промислового комплексу України, включаючи спільні виробництва; фінансову допомогу; підтримку у здійсненні реформ у секторі безпеки і оборони з метою досягнення оперативної сумісності зі стандартами НАТО; співпрацю у сферах кібербезпеки, протидії дезінформації, розмінування тощо. Багато угод прямо вказують на підтримку євроатлантичних прагнень України, підтверджуючи, що її майбутнє – в НАТО, а укладені угоди розглядаються як «міст» або проміжний етап на шляху до повноправного членства.

Оцінка юридичної ефективності цих угод потребує зваженого підходу. З одного боку, вони створюють чітку міжнародно-правову базу для довгострокової підтримки України, що підвищує передбачуваність та стабільність для оборонного планування. Термін дії угод, як правило, становить 10 років з можливістю продовження, що закріплює стратегічний характер співпраці. Юридично обов'язковий характер механізмів консультацій у кризових ситуаціях

також є позитивним аспектом. Угоди формалізують та структурують допомогу, яка вже надавалася, переводячи її на більш системну договірну основу.

З іншого боку, ефективність виконання зобов'язань значною мірою залежить від політичної волі сторін та наявності фінансових ресурсів, що прямо зазначено в текстах угод («за умови наявності коштів»). Формулювання багатьох положень мають рамковий характер («сторони мають намір співпрацювати», «зобов'язуються підтримувати»), що залишає простір для інтерпретації обсягів та конкретних форм допомоги. Хоча механізм консультацій є юридично обов'язковим, сам результат цих консультацій – тобто рішення про надання конкретної допомоги у відповідь на агресію – залишається суверенним правом кожної сторони-партнера. Це ключова відмінність від автоматизму колективної оборони НАТО, на що вказують і деякі аналітики, розрізняючи підтримку та гарантії взаємної оборони.

Формулювання про «міст до НАТО», яке часто зустрічається в угодах, має значне політичне значення, підтверджуючи стратегічну мету України та її партнерів. Однак, з юридичної точки зору, воно не створює автоматичного чи гарантованого шляху до членства в Альянсі, процес вступу до якого регулюється Північноатлантичним договором та вимагає консенсусу всіх членів. Важливим аспектом є те, що багато рамкових угод передбачають укладання додаткових, більш детальних імплементаційних домовленостей чи протоколів.

Україна має міцну національну законодавчу базу для забезпечення оборони, яка включає Конституцію та профільні закони, що визначають оборону як найважливішу державну функцію та закріплюють стратегічний курс на членство в НАТО. Міжнародне право, зокрема Статут ООН, підтверджує право України на самооборону, але не зобов'язує інші держави надавати військову допомогу. Для отримання реальної підтримки Україна уклала низку двосторонніх безпекових угод з ключовими партнерами. Ці угоди формалізують довгострокову допомогу та механізми консультацій, проте не є аналогом колективних гарантій безпеки НАТО. Хоча досвід деяких європейських країн показує можливість ефективної оборони поза військовими альянсами, їхні моделі мають обмежену застосовність для України через її унікальні обставини: триваючу повномасштабну війну та конституційно закріплений курс на вступ до НАТО.

Список використаних джерел

1. Конституція України : від 28.06.1996 р. № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 21.04.2025).

2. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2469-19 (дата звернення: 21.04.2025).

3. Про оборону України : Закон України від 06.12.1991 № 1932-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/1932-12 (дата звернення: 21.04.2025).

4. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII // База даних «Законодавство України» / Верховна Рада
України. URL: https://zakon.rada.gov.ua/go/389-19 (дата звернення: 21.04.2025).
5. Про військовий обов'язок і військову службу : Закон України від 25.03.1992 № 2232-XII : станом на 17 січ. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2232-12#Text (дата звернення: 21.04.2025).

Василинчук Артем Вікторович,
аспірант Національного університету «Києво-Могилянська Академія»

ПРАВОВЕ РЕГУЛЮВАННЯ МОБІЛІЗАЦІЇ В ПЕРІОД ГЕТЬМАНА ПАВЛА СКОРОПАДСЬКОГО

З початком широкомасштабного вторгнення рф в Україну, питання історії правового регулювання мобілізаційних процесів у розрізі історичного минулого, зокрема періоду Української Держави часів гетьмана Павла Скоропадського є актуальним.

Сам термін «мобілізація» походить від французького слова (mobilisation, від лат. mobilis — рухомий). Мобілізацію почали застосовувати наприкінці XVIII - на початку XIX ст. у більшості країн світу із виникненням масових армій, що були сформовані на основі загальної військової повинності [1]. Сучасних рис мобілізація набула під час І-ї і ІІ-ї світових воєн, що вимагали залучення до ЗС значної кількості людських ресурсів і максимального навантаження на економіку країн-учасниць [1]. Отже, мобілізація – це комплекс узгоджених та взаємопов'язаних заходів, які проводить держава шляхом переведення Збройних сил, національної економіки, державних інститутів у зв'язку із запровадженням воєнного стану.

Період П. Скоропадського свідчить, що під його керівництвом був детально розроблений реальний план військового будівництва, зокрема введення військової повинності.

П. Скоропадський, на відміну від лідерів Центральної Ради, розумів місце і роль армії в утвердженні та забезпеченні української державності [2, с.77-83], в першу чергу з огляду на складну геополітичну ситуацію, а також класичне (а не утопічно-соціалістичне) розуміння поняття «держава» невід'ємною складовою якої є наявність збройних сил. Варто зауважити, що тривалий час формування збройних сил було фактично неможливе у зв'язку з принциповою позицією Німеччини та Австро-Угорщини, війська яких розташовувалися на території України і вбачали у створені збройних сил Української Держави потенційну небезпеку [3, с. 215-216]. З огляду на вищевказане, тривалий час зазначений процес (в тому числі і стосовно підходів до поповнення Збройних сил шляхом мобілізації) здійснювався виключно у правовому полі і не мав практичного застосування.

Одним із семи основних законів Української держави, що стали правовою основою її функціонування, був закон «Про права та обов'язки громадян», який передбачав, що громадяни зобов'язані захищати свій рідний край.

Підвалини військового будівництва Української держави заклали закони від 24 липня 1918 р. «Про загальний військовий обов'язок» [4, с. 482]. Відповідно до Закону, призов на дійсну військову службу мав здійснюватися двічі на рік – 15 листопада та 1 березня. Тривалість дійсної військової служби була такою: у піхоті – 2 роки, у кінноті і артилерії – 3 роки, а на флоті – 4 роки. Служба у запасі тривала до 38 років, а в ополченні від 39 до 45 років. Не допускались до військової служби позбавлені судом прав стану. Загальна чисельність армії мала становити майже 310 тисяч військовиків, з них: 175 генералів, 14 930 старшин, 2975 військових урядовців [5, с. 39].

1 серпня 1918 року приймається закон «Про політично-правове становище служачих військового відомства» де говорилось про заборону участі у виборах, маніфестаціях, демонстраціях, роботі будь-яких політичних організацій [6, с. 56-64]. Таким чином, Збройні сили Української держави задумувалися як цілком аполітична структура.

Законодавча база щодо обліку військовослужбовців почала створюватись лише восени 1918 року. 20 жовтня був оприлюднений Закон «Про облік і призов офіцерів, унтер-офіцерів та юнкерів колишньої армії, які перебувають в Українській Державі», а 13 листопада Закон «Про доповнення закону про облік і призов офіцерів, унтер-офіцерів та юнкерів колишньої російської армії від 20 жовтня 1918 р.» та від 18 листопада «Про доповнення і зміну законів про облік і призов офіцерів, унтер-офіцерів та юнкерів колишньої російської армії, від 20 жовтня і 13 листопада 1918 р.» [7, с. 33 – 37].

У цей же час набрав чинності Закон «Про обов'язковість військової повинності і про заклик 5000 чоловіків для комплектування Сердюцької дивізії» [8]. Відповідно до Закону було визначено, що «загальну військову повинність вважати повинністю, яку усі громадяни Української Держави мусять обов'язково виконувати в свій час» [8]. Відповідно до «Інструкції відбору молодих людей для комплектування Сердюцької Гетьманської дивізії» в першу чергу відбиралися молоді особи віком 18-25 років, виключно з сімейств землевласників-хліборобів, які мали більшу кількість землі [8].

8 листопада 1918 р. Гетьман видав наказ про достроковий призов 164 тисяч юнаків до війська. Призову підлягали новобранці 1899 року народження, а саме юнаки, які не досягли віку 19 років, скінчили середню і не вступили до вищої школи, а також старших від 19 років, у яких закінчилися відстрочки [9, с. 54]. Перший призов рекрутів Військовим міністерством було призначено на 15 листопада 1918 р., другий – на 1 березня 1919 р. [10, с. 63 - 67].

Отже, мобілізація мала розпочатися в жовтні 1918 р. Якщо враховувати, що за офіційною статистикою в країні тоді нараховувалося 300 тис. здатних до військової служби чоловіків, то перший призов рекрутів мав дати армії 85 тис. вояків, а другий, призначений на 1 березня 1919 р. – ще 79 тис. [11, с. 90 - 97]. У зв'язку з масштабними планами мобілізаційних заходів, Генеральним штабом і командирами армійських корпусів впродовж жовтня-листопада 1918 р.

обговорювалися різноманітні питання забезпечення майбутніх військовослужбовців, зокрема питання їх розміщення та забезпечення [12, с. 61-106].

20 жовтня 1918 р. гетьман П. Скоропадський затвердив урядову постанову «Про окремий корпус» і закон, що зобов'язав усіх офіцерів і надстрокових унтер-офіцерів колишньої Російської армії віком до 35 років та колишніх юнкерів військових шкіл, які перебували на території Української Держави, протягом тижня прибути до місцевого військового начальника і стати на облік. Урядом передбачалося створення в Українській армії зразкових інструкторських частин [11, с. 90-97].

З 8 листопада 1918 р. Рада Міністрів ухвалила новий Статут військової повинності, що проголошувалась обов'язковою для всіх громадян Української Держави чоловічої статі. Ті, хто з різних причин не закликався до армії чи флоту, за винятком зовсім непрацездатних, мали сплачувати військовий податок. Юнаки віком від 15 років і вище могли вийти з українського громадянства лише після відбуття військової повинності [13].

Відповідно до пунктів 34 – 41 Статуту громадяни під час перебування на дійсній військовій службі зберігали всі політичні та громадянські права, але підлягаючи всім вимогам і правилам військової служби, не мали права:

а) користуватися активним виборчим правом до установ Української Держави законодавчих, громадських та самоврядувальних;

б) входити в склад і приймати участь в будь – яких спілках, товариствах, партіях, радах, комітетах, що мають політичний характер [13].

Таким чином, Статут оголошував про «повну аполітичність армії». Статут передбачав цілу систему відстрочок і пільг по відбуванню військової повинності:

1) за фізичними вадами;

2) за родинним становищем;

3) за освітою;

4) за освітою і родом занять.

Розпис фізичних вад і хвороб, які перешкоджали прийому до служби, затверджувався міністерствами внутрішніх, військових справ та народного здоров'я [14, с. 367].

Так, військовій повинності не підлягали духовні особи, викладачі та непрацездатні. Усі інші категорії чоловічого населення, які звільнялися від дійсної військової служби, мали сплачувати військовий податок. Згідно зі Статутом, військовослужбовці позбавлялися активного виборчого права, натомість пасивне право їм надавалось лише під час виборів до законодавчих установ. Заборонялася участь військовиків у мітингах, зборах, маніфестаціях і демонстраціях. Зменшувався призовний вік молоді до 19 років, скорочувався термін дійсної служби – до двох років у піхоті та артилерії, крім кінної і фортифікаційної, і до трьох – в інших родах військ [10, с. 63-67].

Слід зазначити, що всі вищезгадані нормативно-правові акти і загалом військова стратегія держави передбачала розбудову збройних сил в першу чергу у зв'язку з небезпекою від Радянської Росії і не враховувало можливостей для використання Збройних сил проти потенційних заворушень всередині країни.

Ситуація однак різко змінилися із початком Антигетьманського повстання Директорії.

18 листопада 1918 р., ймовірно у зв'язку з поразкою Німеччини у Першій світовій війні (а значить і перспективою виведення німецьких військ), загрозою війни з Радянською Росією і розгортанням Антигетьманського повстання вийшов новий закон, за яким призову підлягали офіцери до 50 років, а надстроковики – незалежно від віку. Скасовувались майже всі пільги: до армії призивались державні службовці і студенти. Водночас значно збільшувалась чисельність добровольчих дружин [2, с.77-83].

29 листопада 1918 р., під час масового розгортання Антигетьманського повстання і де-факто облоги Києва Республіканськими військами Директорії, головнокомандувач Збройних сил Української Держави князь В. Долгорукий віддав наказ про призов усіх офіцерів до лав армії, хто ж не зробить цього до 12 години 2 грудня, «будуть віддані до військово-польових судів і розстріляні». Накази головнокомандувача мали впроваджувати в життя начальники військових залог, яким після оголошення військового стану безпосередньо стали підлягати губернські, повітові старости і міські отамани.

5 грудня 1918 р. на фоні фактичної облоги Києва і надважкої ситуації у боротьбі з військами Директорії було оголошено тотальну мобілізацію в м. Києві. Мобілізованими мали бути усі чоловіки 1889-1898 рр. народження, окрім тих, хто нині знаходився на державній або військовій службі [15, с. 413]. Мобілізація, судячи із звіту Державної Варти від 09.12.1918, була сприйнята без будь-якого ентузіазму. Українська інтелігенція через цей акт почала залишати місто і йти у штаб Петлюри. Російська ж інтелігенція також не підтримала мобілізацію, хоча вказується, що якби вона була оголошена керівництвом Добровольчої Армії, то ентузіазм від цього серед російських кіл був значно вищий. В цьому ж документі вказується і кількість людей, яку хотів отримати гетьман в ході мобілізації – 12.000, в ньому ж і заявляється, що реальна цифра буде значно нижча [16]. Не сприяло покращенню ситуації і досить активна пропагандиська діяльність спрямована на залучення потенційних військовослужбовців до лав Збройних сил [17, с. 19-29].

Отже, не дивлячись на наявність якісно розробленої правової бази, практичне застосування мобілізаційних заходів зазнало значних труднощів в першу чергу у зв'язку з непопулярністю гетьманської влади, а також фактично було зірване в результаті розгортання Антигетьманського повстання Директорії.

Список використаних джерел

1. Мобілізація / М.Г. Гончарук, В.Ф. Смолянюк, М.Г. Гончарук // Енциклопедія Сучасної України [Електронний ресурс] / редкол. : І.М. Дзюба, А.І. Жуковський, М.Г. Железняк [та ін.] ; НАН України, НТШ. Київ: Інститут енциклопедичних досліджень НАН України, 2019. Режим доступу: https://esu.com.ua/article-68146.

2. Подковенко Т.О. Правове регулювання організації та діяльності Збройних Сил в період гетьманату Павла Скоропадського // Т. О. Подковенко // *Держава і*

право: Збірник наукових праць Інституту держави і права ім. В. М. Корецького. Секція юридичні і політичні науки. К., 2008. Вип. 42. С. 77-83.

3. Пиріг Р. Я. Відносини України і Центральних держав: нетипова окупація 1918 року. Київ : Ін-т історії України НАН України, 2018. 358 с.

4. Громадянська війна в Україні 1918-1920: Збірник документів і матеріалів. Т. 1. К., 1967.

5. Кравчук М. Українська держава та військове будівництво в період Гетьманату // *Нова політика.* 1998. № 1. С. 39.

6. Осадчий Ю.Г. Формування збройних сил Української держави гетьмана П. Скоропадського [Текст] // Сучасна картина світу: природа, суспільство, людина : збірник тез та доповідей Міжнародної наукової конференції (16-17 квітня 2008 р.). Суми: УАБС НБУ, 2008. С. 56-64. Режим доступу: https://essuir.sumdu.edu.ua/bitstream-download/123456789/63224/4/Osadchij.pdf;jsessionid=E73F67205DE1BAA3A19EE0FED4C5817B.

7. Дьякова О.В. Бондаренко А.Б. Законодавча база збройних сил гетьманату. Збірник наукових праць «Історія та географія» / Харк. нац. пед. університет імені Г. С. Сковороди. Випуск 58. Харків, 2020. С. 33-37.

8. Центральний державний архів вищих органів влади та управління України. Ф. 1064. Оп. 1. Спр. 270. Арк. 1.

9. Мироненко О., Римаренко Ю., Усенко І., Чехович В. Українське державотворення: Словник-довідник. К.: Либідь, 1997. С. 54.

10. Барановська Н.М., Макарчук О.Г. (2008). Армія в охоронній системі Гетьманату Павла Скоропадського // *Вісник Національного університету "Львівська політехніка".* Держава та армія. № 634. С. 63-67.

11. Барановська Н.М. Підвалини військової політики гетьмана Павла Скоропадського / Н.М. Барановська // *Вісник Національного університету "Львівська політехніка".* 2014. № 784 : Держава та армія. С. 90-97.

12. Центральний державний архів вищих органів влади та управління України. Ф. 1078. Оп. 2. Спр. 37. Арк. 61-106.

13. Статут військової повинності, ухвалений Радою Міністрів Української держави. К., 1918. 51 с.

14. Мала енциклопедія етнодержавознавства / НАН України. Ін-т держави і права ім. В.М. Корецького; Редкол.: Ю. І. Римаренко (відп. ред.) та ін. К.: Довіра: Генеза, 1996. С. 367.

15. Українська Держава (квітень - грудень 1918 року). Документи і матеріали. У двох томах, трьох частинах. Т. 2 / Упоряд.: Р. Пиріг (керівник) та ін. К.: Темпора, 2015.

16. Державний архів міста Києва. Ф. Р-1671. Оп. 1. Спр. 16. Арк. 1.

17. Василинчук А.В. Листівкова пропаганда гетьманських сил під час повстання директорії (Листопад-Грудень 1918 р.):. *Вісник Київського національного університету імені Тараса Шевченка.* Історія. 2024. № 159. С. 19-29.

Васюта Юлія Володимирівна,
ад'юнкт кафедри криміналістики та судової медицини Національної академії внутрішніх справ

СУЧАСНІ ТЕНДЕНЦІЇ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СПІЛЬНИХ СЛІДЧИХ ГРУП ПІД ЧАС РОЗСЛІДУВАННЯ ТРАНСНАЦІОНАЛЬНОЇ ЗЛОЧИННОСТІ

Однією з тенденцій сучасної криміналістичної науки є інтеграція знань та розробка інноваційних підходів, спрямованих на вирішення завдань з протидії транснаціональній злочинності в умовах глобальних викликів, а також за умов дії воєнного стану та процесу цифровізації громадянського суспільства. Відтак, інформаційне забезпечення правоохоронної діяльності стало критично важливим питанням.

Кіберзагрози спонукають до формування надійного правового фундаменту для зміцнення інформаційної безпеки. Під час розслідування транснаціональних кримінальних правопорушень компетентні органи держав, зокрема члени спільної слідчої групи, стикаються з необмеженою кількістю інформації з численних джерел даних, що потребують аналізу та оцінки слідчої ситуації. Одним із шляхів вирішення проблемних питань у цьому аспекті є формування єдиного підходу до інтеграції різних баз даних для встановлення криміналістично значущої інформації. Так, інформаційні системи набувають актуальності, оскільки новітні інформаційні технології дозволяють оперувати репозитарієм криміналістичних даних шляхом використання спеціальних методів.

Окрім цього, формування нових наукових напрямів в криміналістичній науці, наприклад, воєнної та цифрової криміналістики, передусім зумовлено практичними потребами у застосуванні криміналістичних інновацій, а також сучасними тенденціями і завданнями розвитку науки [1, с. 151].

Слід зазначити, що аналітична діяльність спільних слідчих груп є фундаментальним складником під час розслідування кримінальних правопорушень. Так, постає потреба у розробці унікальної інформаційної системи, за допомогою якої органи та підрозділи Національної поліції України матимуть можливість обробляти та завантажувати матеріали (фото, відео, документи) для встановлення осіб. Наприклад, в СУ ГУНП в Харківській області з'явилася ідея пілотного проєкту зі створення інформаційної системи управління даними, обробки та аналізу для розслідування кримінальних проваджень «SORC». Ця система може вміщувати низку даних, а саме: показання у текстовому форматі; речові докази; аудіо- та відеоматеріали; фотографії; документи; висновки експертів; схеми, карти та інші графічні матеріали; локаційні дані; електронну кореспонденцію; електронну інформацію; супутникові знімки; розвідку на основі відкритих даних – OSINT; аналітичні звіти та ін. Використання інформаційної системи дозволяє забезпечити основні функції, наприклад, створити та наповнити базу доказами воєнних злочинів і

матеріалами кримінальних проваджень; забезпечити пошук воєнних злочинців та контроль за їхньою діяльністю; взаємодіяти з різними підрозділами та обмінюватися інформацією. З огляду на практичну значущість, роботу з інформаційною системою «SORC» суттєво спрощують наявні підсистеми: «Докази», «Воєнні злочинці», «Кримінальні провадження». За допомогою цієї інформаційної системи можливо отримати максимальну інформацію про окреме кримінальне провадження, інформаційні звіти, що дозволяють здійснити обробку інформації, а також ідентифікувати воєнних злочинців [2, с. 537-540].

З огляду на вищезазначене, до переваг використання сучасних інформаційних технологій в ході розслідування кримінальних правопорушень віднесено: системність інформації, що сприяє забезпеченню результативності розслідування кримінальних правопорушень; інформаційно-аналітичну роботу, що охоплює збирання, зберігання, систематизацію та аналіз доказової й орієнтуючої інформації з метою прийняття оптимальних тактичних і процесуальних рішень; інформаційно-аналітичне забезпечення, яке дозволяє слідчому вирішувати складні тактичні та пізнавальні завдання під час розслідування кримінальних правопорушень; інтенсивне впровадження в діяльність правоохоронних органів засобів комп'ютерної та цифрової техніки, що сприяє використанню інформаційно-аналітичних методів. Цей процес помітно впливає на організацію розслідування кримінальних правопорушень, методичне забезпечення слідчої, оперативно-розшукової, експертної діяльності, наукову організацію їх праці, оптимізує збирання, зберігання, систематизацію та аналіз доказової та орієнтуючої інформації. Автоматизація як процес загального якісного поліпшення технології обробки інформації забезпечує оперативний підхід та засвідчує ефективність криміналістичних інформаційно-пошукових систем [3, с. 565].

Перспективними напрямами використання електронних інформаційних систем під час розслідування воєнних злочинів вважають здійснення комунікації в дистанційному форматі між органами досудового розслідування, міжнародними інституціями та судом, створення спільної платформи для обміну інформацією, досвідом та знаннями; використання електронних інформаційних систем для індексування доказової інформації; застосування технологій хмарного зберігання інформації про кримінальне провадження; розпізнавання особи за різними фізіологічними особливостями шляхом використання спеціальних застосунків; складання опису кожного доказу з метою швидкого пошуку; використання цифрових інструментів для збирання інформації з відкритих джерел та проведення аналізу на предмет доказовості [4, с. 40]. Так, використання спільною слідчою групою електронних інформаційних систем сприятиме виконанню завдань кримінального провадження під час розслідування кримінальних правопорушень, зокрема воєнних злочинів.

Також підкреслимо значущість утворення Eurojust бази даних – Core International Crimes Evidence Database (CICED), яку розроблено для зберігання та аналізу доказів вчинення міжнародних злочинів. Ця база даних покликана підтримувати національні та міжнародні розслідування кримінальних правопорушень, сприяє наданню тактичних та стратегічних рекомендацій з

кримінального переслідування, обміну інформацією та доказами щодо міжнародних злочинів. Одним із пріоритетних завдань CICED є уникнення повторної віктимізації потерпілих, спричинених неодноразовими допитами у різних кримінальних провадженнях [5].

Таким чином, одним із напрямів забезпечення швидкого, повного та ефективного розслідування кримінальних правопорушень спільними слідчими групами є цифровізація підходів в роботі з інформацією, отриманою під час проведення слідчих процесуальних дій. В умовах технологічних викликів сьогодення, зокрема в кіберпросторі, зросли вимоги щодо підвищення ефективності та результативності діяльності органів правопорядку на основі інформаційно-аналітичного забезпечення. Інформаційне забезпечення діяльності спільних слідчих груп є ключовим складником для успішного проведення тактичних операцій, вирішення криміналістичних завдань стратегічного і тактичного рівня, а також забезпечення міжнародного співробітництва під час розслідування кримінальних правопорушень.

Список використаних джерел

1. Шевчук В.М. Криміналістичні інновації та цифрові технології у протидії сучасній злочинності. *Слідча та детективна діяльність: виклики і перспективи:* збірник тез Всеукраїнської науково-практичної конференції (Харків, 25 травня 2023 р.). Харків: Юрайт 2023, 212 с. С. 148-153.

2. Болвінов С.П. Практичні аспекти застосування інформаційних систем під час розслідування воєнних злочинів (на прикладі системи SORC). *Вісник кримінологічної асоціації України.* 2024. № 2 (32). С. 531-543. DOI: https://doi.org/10.32631/vca.2024.2.38.

3. Капустіна М.В., Демидова Є.Є., Латиш К.В. Використання сучасних інформаційних технологій при розслідуванні воєнних злочинів. *Юридичний науковий електронний журнал*. № 4/2023. С. 564-566. DOI: https://doi.org/10.32782/2524-0374/2023-4/134.

4. Стратонов В.М. Актуальні напрями використання електронних інформаційних систем в умовах воєнного стану. *Науковий вісник ХДУ*. Серія: юридичні науки. № 1 (2025). С. 36-41. DOI: https://doi.org/10.32999/ksu2307-8049/2025-1-6.

5. Резнікова А. Робота спільної слідчої групи в процесі документування злочинів рф: воєнний досвід України. 2 черв. 2023 р. *Юридична платформа "Just talk".* URL: https://justtalk.com.ua/post/robota-spilnoi-slidchoi-grupi-v-protsesi-dokumentuvannya-zlochiniv-rf-voennij-dosvid-ukraini.

Градюк Іванна Миколаївна
студент навчально-наукового інституту права та психології Національної академії внутрішніх справ
Шутенко Світлана Василівна,
завідувач кафедри правничої лінгвістики Національної академії внутрішніх справ

ПОВЕДІНКА СПІЛКУВАННЯ ПІД ЧАС ВІЙНИ. СПІВІДНОШЕННЯ СВОБОДИ СЛОВА, НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ЕТИКИ КОМУНІКАЦІЇ

У XXI столітті мережа Інтернет стала головним простором для спілкування, обміну думками, інформація стала частиною не тільки національного спротиву, а мова – інструментом впливу, захисту та опори. Сучасний світ переживає епоху інформаційних трансформацій, де доступ до інформації став визначальним фактором для розвитку суспільства та кожного окремого індивіда [3].

Поведінка спілкування в мережі Інтернет під час війни зазнає значних трансформацій, відображає соціальну та емоційну атмосферу, потребу в швидкому обміні критично важливою інформацією. Особливо у час війни зростає прагнення людей отримувати перевірену інформацію про події на фронті, офіційні заяви представників.

Значну роль у період війни відіграють соціальні мережі, вони виконують роль як оперативного передавання повідомлень щодо безпеки рідних, змін ситуацій та потреб у допомозі. Під час війни мовна поведінка зазнає суттєвих змін: активізується використання національної лексики, зростає вплив інформаційної агресії.

Інтернет-комунікація – це особлива форма взаємодії, яка користується своєю автономністю, швидкістю, публічністю та потенційністю вірусних повідомлень. Із початком війни в Україні комунікація у соціальних мережах перетворилася на важливий інструмент психологічної підтримки, волонтерської діяльності та інформаційної боротьби. У таких умовах поведінка спілкування користувачів у соціальних мережах стала предметом особливої уваги як з боку суспільства, так і правоохоронних структур.

Важливе місце посідає правовий вимір поведінки. Відповідно до чинного законодавства України, інформація та публікації неправдивих інформацій про Збройні Сили України, заклики до колабораціонізму або приниження національної гідності можуть тягнути за собою адміністративну та кримінальну відповідальність. Чинний Кримінальний кодекс України містить низку норм, у яких містяться кримінальна відповідальність, наприклад: стаття 109. Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, караються позбавленням волі на строк від п’яти до десяти років з конфіскацією майна або без такої [2]; стаття 111. Державна зрада, карається позбавленням волі на строк від 12 до довічного[2]; стаття 111-1. Колабораційна діяльність, караються позбавленням права обіймати певні посади

або займатися певною діяльністю на строк від десяти до п’ятнадцяти років [2]; стаття 111-2. Пособництво державі-агресору, караються позбавленням волі на строк від десяти до дванадцяти років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк від десяти до п’ятнадцяти років та з конфіскацією майна або без такої [2]; стаття 114-2. Несанкціоноване поширення 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, вчинене в умовах воєнного або надзвичайного стану, карається позбавленням волі на строк від трьох до дванадцяти років [2]; стаття 436-2. Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників, частина 1: карається виправними роботами до 2 років, або пробаційним наглядом до 3 років, або позбавленням волі до 2 років**,** частина 2 (виготовлення й поширення відповідних матеріалів): обмеженням волі до 5 років або позбавленням волі до 5 років з можливою конфіскацією майна**,** частина 3 (якщо дії вчинено службовою особою, повторно, групою чи із використанням ЗМІ): позбавленням волі від 5 до 8 років з можливою конфіскацією майна [2].

Фактчекінг – це важливий процес перевірки фактів і тверджень на їхню точність та правдивість. Це допомагає забезпечити, що інформація, яку сприймаємо, є достовірною та об’єктивною. Фактчекінг може включати перевірку джерел, пошук додаткової інформації й аналіз логіки та доказів, щоб визначити правдивість твердження [4].

Свобода слова – одна із основоположних цінностей демократичного суспільства, яка забезпечує «кожному гарантується право на свободу думки і слова, на вільне використання своїх поглядів і переконань»[1]. Проте чинне законодавство України передбачає деякі обмеження цього права, зокрема в інтересах національної безпеки, територіальної цілісності або громадського порядку (стаття 34 Конституції України), що є особливо важливим у період війни.

В епоху цифрового розвитку комунікація здійснюється через соціальні мережі, кожне повідомлення стає публічним і впливає на інформаційний простір. Під час війни виникає потреба у переосмисленні меж свободи слова. Де закінчується право на висловлення думки і починається відповідальність за слова, які можуть нести загрозу безпеці країни чи сприяти дезінформації. Відповідно до статті 17 Конституції України «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [1]. Ця норма підтверджує, що під час воєнного стану інформація є стратегічним ресурсом етики спілкування в інтернеті, стає не лише моральним вибором, а й фактом безпеки держави.

Етика комунікації є системою моральних норм, що регулюють відповідальність людини за зміст, форму та наслідки сказаного чи написаного. Етика комунікації передбачає: уникнення поширення неперевіреної інформації; відмова від мови ворожнечі та агресивної риторики; повага до гідності інших

осіб; усвідомлення сили слів, що можуть впливати на психологічний стан людини, інформаційну безпеку та навіть бойові дії.

Свобода слова, національна безпека та етика комунікації – вони не суперечать один одному, а існують у взаємозалежності. Лише усвідомлене й відповідальне мовлення, в основі якого лежать як правові, так і етичні норми, може бути безпечним і конструктивним у сучасних реаліях.

Поведінка спілкування в мережі Інтернет під час війни є складним і багатогранним, він охоплює взаємодію між фундаментальними правами, нагальними потребами національної безпеки та етичного міркування.

Спілкування в Інтернеті під час війни вимагає від кожного громадянина високого рівня відповідальності критичного мовлення та усвідомлення наслідків своїх дій. Збереження балансу між свободою слова, національною безпекою та етикою спілкування є основним фактором для стійкості суспільства, протидії ворожій пропаганді та наближення перемоги.

Список використаних джерел

1. Конституція України // https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text // від 28 червня 1996 р

2. Кримінальний кодекс України // https://zakon.rada.gov.ua/laws/show/2341-14#Text // від 05 квітня 2001 р.

3. Градюк І. М. // Збірник українська мова в юриспруденції: стан, проблеми, перспективи // Українська мова як інструмент правової комунікації в сучасній правовій системі // 31.10.2024 // ст. 215-218 // https://elar.navs.edu.ua/handle/123456789/35400

4. Інтернет – безпека під час війни (Частина 2) // https://www.softkey.ua/ua/useful/articles/internet-bezopasnost-vo-vremya-voyny-chast-2/ // від 14 травня 2024 р.

Джафарова Лейла Саваланівна,
слухач інституту заочного та дистанційного навчання Національної академії внутрішніх справ, інструктор відділення домедичної підготовки Національної академії внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА СУСПІЛЬСТВА В СФЕРІ ДОМЕДИЧНОЇ ПІДГОТОВКИ

Інформаційна безпека суспільства в сфері домедичної підготовки – це комплекс заходів та способів, які спрямовані на захист, достовірність і ефективне поширення знань, навичок та інформації, необхідної для надання домедичної допомоги до прибуття медиків на місце події.

Важливість інформаційної безпеки та фільтрування отриманої інформації на просторах інтернету є вкрай вагомим, особливо в сьогоднішній час. Правильна та точна інформація в комплексі навичок і знань, рятують життя!

Інформаційна революція XXI століття та подальший невпинний розвиток інновацій у сучасному світі не залишає жодної сфери діяльності людства поза межами впливу новітніх інформаційних технологій. Сфера охорони здоров′я не є виключенням. Водночас разом з перевагами і новими можливостями цифровізації сфера охорони здоров′я стикається зі значними викликами.

А саме загроза інформації в цифровому просторі є найбільш актуальним і масштабним подразником. Відповідно це вимагає від організацій сучасних підходів і заходів захисту інформації. Сталим терміном для захисту інформації в цифрових (комп'ютерних) технологіях є «кібербезпека» [1].

Тому як же ми можемо повпливати на покращення інформаційної безпеки? У сфері домедичної допомоги поширення недостовірної або застарілої інформації може призвести до фатальних наслідків, а саме до смерті. Щоб цього уникнути ми зобов'язані пам'ятати що:

Стаття 3. Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю[2]. Тому ми маємо на етапі домедичної допомоги без вагань зробити все від себе можливе для порятунку життя.

Треба для себе вкоренити, що сьогодні хтось, а завтра це можеш бути ти! Все змінюється, та покращується, інфо-простір зараз на піку свого розкриття в повній силі.

Але інформаційний потік, потрібно фільтрувати від паразитарних джерел. Це можуть бути або просто вигадані, ніким не опрацьовані та не затверджені джерела або просто застаріла інформація яка може нести важкі наслідки та втрати.

Щоб цього уникнути, треба: використовувати офіційні джерела (МОЗ, ВООЗ) та слідкувати за змінами, які відбуваються в них.

Необхідно перевіряти дані, які поширюються у соцмережах або через месенджери.

У періоди криз або війни ворог може навмисно поширювати фейки, щоб викликати паніку або дезорганізувати надання допомоги:

Треба вміти розпізнавати фейки та інформацію яка офіційно не підтверджена.

Варто вчити цьому дітей і дорослих на курсах домедичної допомоги.

Для ознайомлення та при проходженні навчання можемо використовувати: онлайн-курси в яких все максимально доступно розповідається, симулятори та додатки для навчання домедичної допомоги, можуть занурити в світ місце подій, та поетапно відтворити сценарій допомоги та порятунку. Але і тут можемо зустріти хибні кроки та інформацію яка вже змінилась, тому важливою складовою є інформаційна грамотність населення.

Фундаментальною частиною інформаційної грамотності є:

Проведення доступних для всіх, регулярних навчань і тренінгів на яких людина зможе ознайомитись з базою домедичної допомоги або відпрацювати навички які вже були вивченні.

Поширення перевіреної інфографіки, відео та інтерактивних матеріалів, для того щоб сценарії які неможливо відтворити у реальному житті, змогли на відеоматеріалах зрозуміло показати ідею виконання тих або інших навичок.

Відкриті інформаційні портали для самостійного вивчення допоможуть, відпрацювати знання та знайти слабкі точки, які треба доопрацювати та вивчити, задля точної ідеї виконання дій.

У реальному часі немає бути думки, що ці знання можна відкласти на пізніше або ж взагалі вони будуть потрібні комусь, а не мені. Об'єктивно маємо брати до уваги, що в цьому питанні нам допомогають волонтерські організації та інші структури які намагаються сприяти розвитку населення , щоб підготувати всіх до різних критичних та стресових ситуацій. Влаштовуючи програми та навчання по підвищенню інформаційної безпеки, поширення відкритої та прозорої інформації, вебінари та онлайн зустрічі, на яких можна обговорити проблематику та зауважити для себе аспекти доцільної допомоги.

Отже, забезпечення інформаційної безпеки в домедичній підготовці та в будь якій спеціалізації – це не лише питання технологій, а й свідомості, освіти та співпраці між державою, громадянським суспільством і технологічними платформами.

Варто зауважити, щоб бути свідомим та відповідальним громадянином нашої держави потрібно користуватися тільки перевіреними джерелами. Перевіряти інформацію на практиці або спілкуватися з безпосередніми діячами цієї практики в реальному житті. Розвивати свою обізнаність за допомогою навчань, тренінгів та курсів. Як тільки є можливість, відпрацьовувати та підвищувати рівень своїх знань якомога частіше.

Таким чином, для надання ефективної домедичної допомоги нам допомогає наказ МОЗ України від 09.03.2022 № 441 «Про затвердження порядків надання домедичної допомоги особам при невідкладних станах». В цьому наказі йдеться про 29 алгоритмів допомоги, які допоможуть при невідкладних станах та критичних ситуаціях [3].Тому, не бійтеся вчитися та бути корисними в першу чергу собі та своєму оточенню, бо ці знання – рятують життя!

Список використаних джерел

1. Основи кібербезпеки URL: https://moz.gov.ua/uk/osnovi-kiberbezpeki-2
2. Офіс Президента України. Конституція України. URL: https://www.president.gov.ua/ua/documents/constitution/konstituciya-ukrayini-rozdil-i
3. Наказ МОЗ України від 09.03.2022 № 441 "Про затвердження порядків надання домедичної допомоги особам при невідкладних станах". URL: https://moz.gov.ua/uk/decrees/nakaz-moz-ukraini-vid-09032022--441-pro-zatverdzhennja-porjadkiv-nadannja-domedichnoi-dopomogi-osobam-pri-nevidkladnih-stanah

Клеван Віолета Євгенівна,
курсант навчально-наукового інституту № 1 Харківського національного університету внутрішніх справ

ЦИФРОВИЙ СУВЕРЕНІТЕТ ДЕРЖАВИ В ЕПОХУ ШТУЧНОГО ІНТЕЛЕКТУ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ ПРАВОВОГО РЕГУЛЮВАННЯ

У XXI столітті держави все частіше стикаються з необхідністю переосмислення природи власного суверенітету в умовах глобальної цифрової трансформації. Впровадження технологій штучного інтелекту (ШІ), поширення великих даних і автоматизованих інформаційних систем зумовлює появу нових викликів у сфері державного управління, прав людини та інформаційної безпеки. У зв'язку з цим актуалізується поняття цифрового суверенітету, що означає здатність держави здійснювати суверенний контроль над цифровими потоками даних, інфраструктурою, платформами, а також нормотворенням у сфері цифрових технологій.

На міжнародному рівні, особливо в рамках Європейського Союзу, посилюється прагнення до цифрової автономії. Прикладом є ініціатива GAIA-X, яка передбачає створення власної безпечної хмарної інфраструктури, що відповідає вимогам Загального регламенту захисту даних (GDPR) і зменшує залежність від іноземних платформ [1]. Іншим важливим кроком стало прийняття Регламенту ЄС про штучний інтелект (AI Act), який класифікує системи ШІ за ступенем ризику, забороняє використання технологій для соціального скорингу та масового біометричного нагляду, а також передбачає правові механізми для забезпечення прозорості алгоритмів [5, с. 1].

На відміну від ЄС, Україна ще перебуває на стадії концептуального осмислення цифрового суверенітету. В умовах гібридної війни держава стикається з викликами інформаційної безпеки, маніпуляції громадською думкою, використанням бот-мереж і алгоритмів ШІ у пропагандистських кампаніях [2]. Як зазначається в дослідженні Інституту Просвіти, сучасні цифрові платформи стали основними каналами поширення фейкової інформації, що формує спотворену реальність для користувачів і підриває стабільність суспільства [2].

Додаткову загрозу становить явище цифрового колоніалізму, коли країни, що не мають власних технологій, змушені покладатися на іноземне програмне забезпечення для зберігання, обробки й захисту державних даних. Як слушно зазначає І.М. Милосердна, в умовах цифрової глобалізації така залежність є не менш небезпечною, ніж економічна чи політична, і здатна спричинити втрату цифрової автономії [3, с. 2].

Загроза цифровій безпеці також пов'язана з недостатнім рівнем цифрової грамотності населення. У ситуації, коли громадяни не володіють навичками критичного мислення, технології ШІ можуть бути використані як засіб когнітивного контролю. Це підкреслює необхідність формування не лише

техніко-правових інструментів цифрового суверенітету, а й суспільної стійкості до маніпуляцій [2].

На цьому тлі особливої ваги набуває Рекомендація ЮНЕСКО з етики ШІ (2021), яка містить принципи, орієнтовані на забезпечення прав людини, прозорість, недискримінацію, безпеку та інклюзію при використанні штучного інтелекту [4]. Її положення можуть стати основою для імплементації національного законодавства України у сфері ШІ.

Отже, формування цифрового суверенітету України потребує поєднання технічної незалежності, етичного правового регулювання, освітніх програм та міжнародної інтеграції стандартів. Без цього держава залишатиметься вразливою до зовнішніх технологічних впливів.

Список використаних джерел

1. Компанієць Ф. Контроль над хмарою – контроль над майбутнім. *Speka – онлайн-медіа про підприємництво та технології.* URL: https://speka.media/cifrovii-suverenitet-jevropi-9qy53k.

2. Цифрові пропагандисти та інформаційний суверенітет. Як захистити свої права в онлайн-епоху. *Інститут Просвіти.* URL: https://iprosvita.com/tsyfrovi-propahandysty-ta-informatsijnyj-suverenitet-iak-zalyshytysia-neoshukanym-ta-zakhystyty-svoi-prava-v-onlajn-epokhu/

3. Милосердна І.М. Цифровий суверенітет держави: наукова риторика та реальні зміни. *Репозитарій ПНПУ ім. К. Д. Ушинського.* URL: http://dspace.pdpu.edu.ua/bitstream/123456789/21794/1/25.pdf.

4. Recommendation on the Ethics of Artificial Intelligence. UNESCO, 2021. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137.

5. Regulation (EU) 2024/1365 of the European Parliament and of the Council of 13 March 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1365.

Ковальова Дар'я Юріївна,
слухач навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ

ЗАХИСТ ДІТЕЙ ТА ВРАЗЛИВИХ ГРУП У ЦИФРОВОМУ СЕРЕДОВИЩІ

Цифрове середовище стало невід'ємною частиною повсякденного життя, і воно надає безліч можливостей для дітей та молоді, зокрема в навчанні, соціалізації, культурному обміні і навіть у професійному розвитку. Однак, разом із цими можливостями виникають нові загрози для здоров'я та безпеки, особливо для дітей та вразливих груп. Цифровий простір парадоксально поєднує у собі освітні можливості й механізми впливу, які часто використовуються

зловмисниками у своїх психологічних стратегіях, що ставить під загрозу права дітей, їхнє фізичне та психологічне благополуччя.

Основними ризиками, які можуть виникнути для дітей у цифровому середовищі, є кібербулінг, шахрайство, маніпуляції, педофілія онлайн, а також доступ до шкідливого контенту. Кібербулінг є серйозною загрозою для психічного здоров'я дітей, оскільки вони можуть зазнати насмішок, погроз чи переслідувань в соціальних мережах та інших цифрових платформах. Діти, як правило, не мають достатньої обізнаності для того, щоб виявити небезпечні ситуації та відреагувати на них відповідно.

Крім того, цифрові платформи часто слугують середовищем для популяризації деструктивних наративів, таких як радикалізація і насильство. Це особливо небезпечно для підлітків, які ще формують своє світосприйняття та мають вразливу психіку. Дослідниця феномену сексуальних злочинців Анна Солтер, у своїй книзі «Хижаки» детально описує, як зловмисники використовують довіру, емоційний зв'язок та психологічні вразливості дитини для реалізації своїх цілей. У цифровому середовищі ці механізми лише посилюються завдяки можливості довготривалого прихованого контакту та імітації безпечних стосунків [1].

Останнім часом в мережі Інтернет дуже розповсюджені такі явища, як секстинг, тобто інтимне листування з дитиною, а також ґрумінг – встановлення дружніх відносин, входження в довіру до дитини з метою подальшої особистої зустрічі для вступу в сексуальні відносини, експлуатації чи шантажу. Нерідко діти стають жертвами секстингу, тому що не вбачають в цьому реальної загрози, вважаючи це нешкідливим, простим способом отримання компліментів на рахунок своєї зовнішності за допомогою схвальних коментарів чи «лайків» [2]. Але досить часто жертва примушується до участі в порнографічних сценаріях через шантаж із використанням інформації, яка попередньо була зібрана про неї в Інтернеті, адже була у відкритому доступі.

До останнього часу в Україні подібні діяння не розглядалися в площині кримінального законодавства (лише в лютому 2021 року було криміналізоване домагання дитини в сексуальних цілях, в тому числі з використанням інформаційно-телекомунікаційних систем або технологій (ст. 156-1 Кримінального кодексу України) [3]), тоді як в деяких країнах вже є судові рішення, якими визнано факти зґвалтування через Інтернет. Зокрема, ще в 2017 році у Швеції засудили чоловіка, який таким чином зґвалтував 27 дітей, змушуючи їх виконувати сексуальні дії з використанням веб-камери, записуючи їх на відео або демонструючи в прямому ефірі [2].

Захист дітей у цифровому середовищі потребує чіткої правової регламентації. Національні законодавчі органи повинні створювати та впроваджувати закони, які сприяють захисту дітей від цифрових загроз. Одним з таких кроків є впровадження законів, що зобов'язують інтернет-платформи блокувати доступ до небезпечного контенту, а також застосовувати механізми перевірки віку користувачів.

Процес розслідування кіберзлочинів, які стосуються дітей, повинен враховувати особливості збору доказів в Інтернеті. Оскільки інтернет-

платформи часто не мають можливості безпосередньо перевірити вік користувачів, це потребує інтеграції нових механізмів моніторингу та фільтрації контенту на рівні законодавства.

Для забезпечення безпеки дітей у цифровому середовищі важливо підвищувати рівень цифрової грамотності серед усіх учасників освітнього процесу. Це включає навчання дітей основам кібербезпеки, навичкам захисту персональних даних, а також вмінням критично оцінювати інформацію в Інтернеті. Включення курсів з цифрової грамотності в шкільні програми є необхідним кроком для підготовки молоді до реалій сучасного інформаційного середовища.

Батьки та освітяни відіграють важливу роль у забезпеченні безпеки дітей у цифровому середовищі. Так, Анна Солтер наголошує на центральній ролі батьків у запобіганні сексуальному насильству, у тому числі — в умовах цифрової доби. Вона критикує наївність, довірливість і небажання бачити загрози навіть тоді, коли вони очевидні [1]. Для захисту дітей від небезпек Інтернету важливо активно контролювати їхню активність, встановлювати обмеження на доступ до шкідливого контенту та регулярно проводити бесіди про правила безпечного використання мережі. Це також включає заходи обережності при спілкуванні з незнайомими людьми онлайн, усвідомлення небезпек кібербулінгу, важливість захисту персональних даних та безпеку фінансових операцій.

Підсумовуючи вищевикладене, слід зазначити, що забезпечення цифрової безпеки дітей – це багаторівнева система, в якій поєднуються право, психологія, освіта, технічна інфраструктура та культура довіри. Лише інтегрований підхід може забезпечити стійкий захист від тих загроз, які з кожним роком стають дедалі складнішими й витонченішими.

Список використаних джерел:

1. Хижаки. Педофіли, ґвалтівники та інші сексуальні злочинці: хто вони такі, як вони діють і як ми можемо захистити себе та своїх дітей / пер. З анг. О. Татаренко. Харків: Вид-во «Ранок»: Фабула, 2022. 288 с.

2. Іонан В.В Інтернеті що 5 хв. відбувається сексуальне насильство над дитиною. Як це зупинити? *Українська правда*. 2020. URL: https://life.pravda.com.ua/columns/2020/02/4/239800/.

3. Про внесення змін до деяких законодавчих актів України щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської конвенції): Закон України від 18 лютого 2021 р. № 12560-IX. URL: https://zakon.rada.gov.ua/laws/card/1256-20.

Костенок Андрій Михайлович,
аспірант Інституту держави і права імені В.М. Корецького НАН України

ПРИНЦИП СПРАВЕДЛИВОСТІ ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДІЯЛЬНОСТІ ЗМІ

У сучасному інформаційному суспільстві засоби масової інформації (ЗМІ) відіграють ключову роль у формуванні громадської думки, конструюванні реальності та впливають на стан національної безпеки. В епоху гібридних загроз, інформаційних війн і глобальної цифровізації особливої актуальності набуває формування ефективної та етично вивіреної інформаційної політики держави. При цьому концепція справедливості постає не лише як правовий принцип, а як соціально-політична категорія, що забезпечує баланс між безпековими заходами та дотриманням прав людини, зокрема права на свободу вираження поглядів. Саме такий підхід пропонують сучасні дослідники інформаційного права та медіаетики, зокрема О. Задорожній [1], В. Лисенко [2] та інші.

Інформаційна безпека трактується як стан захищеності особи, суспільства і держави від інформаційних загроз, що забезпечується через комплекс заходів у сфері інформаційної політики, права, кіберзахисту тощо. Як зазначає В. Цимбалюк, інформаційна безпека повинна гарантувати не лише захист від деструктивного інформаційного впливу, а й сприяти формуванню критичного мислення в громадян [3]. У цьому контексті роль ЗМІ полягає в тому, що з одного боку, вони слугують каналами інформування та демократичного контролю, з іншого – можуть бути інструментами маніпуляцій, пропаганди або дезінформації, зокрема під час воєнних чи політичних конфліктів. Сучасні кейси медіавпливу в умовах російсько-української війни чітко демонструють потужний потенціал ЗМІ, як у зміцненні національного духу, так і в дестабілізації ситуації через розповсюдження фейкових новин.

Справедливість як етичний і правовий принцип вимагає збалансованого підходу до регулювання медіапростору. Це передбачає як забезпечення безпеки, так і дотримання прав громадян, зокрема свободи слова, права на приватність, доступу до інформації. І. Кушнарьова підкреслює, що без належного дотримання стандартів справедливості державна політика в сфері інформації може скотитися до авторитаризму й цензури [4]. Водночас, абсолютна свобода слова без відповідальності призводить до інформаційного хаосу. Законодавство України, зокрема, Конституція України, Закон «Про інформацію», Закон «Про телебачення і радіомовлення» – містить правові механізми, які закладають підґрунтя для неупередженого регулювання інформаційної сфери. Важливими є також міжнародні стандарти, включно з Європейською конвенцією з прав людини, що гарантує свободу вираження із застереженнями щодо захисту безпеки та моралі.

На думку Н. Костенко та О. Мельника [5], сучасні ЗМІ все частіше стають інструментом гібридної війни, спрямованої на психологічну та ідеологічну дестабілізацію. Соціальні мережі, месенджери та стрімінгові платформи активно

використовуються для поширення дезінформації, вкидання фейкових наративів, зниження довіри до інституцій. Аналітичні дослідження Центру стратегічних комунікацій та інформаційної безпеки вказують, що понад 70% інформаційних атак РФ на Україну здійснюються саме через маніпулятивний контент у соцмережах [6]. Проблема посилюється низьким рівнем медіаграмотності населення, що робить споживачів інформації вразливими до впливів. Ситуація вимагає не лише технічного реагування, але й стратегічного переосмислення ролі ЗМІ як безпекового чинника. Як зазначає В. Різун, у відкритому демократичному суспільстві інформаційна безпека не може досягатися суто репресивним контролем за ЗМІ, а має базуватися на засадах інформаційної культури, етичної журналістики та свідомого споживання інформації [7, с. 34]. Отже, справедливість у політиці інформаційної безпеки – це не лише правовий, а й моральний орієнтир, що визначає межі допустимого втручання держави в сферу комунікації.

Правове регулювання інформаційної безпеки в Україні формується на основі низки ключових документів, серед яких Закон «Про основи національної безпеки України», Доктрина інформаційної безпеки, Стратегія кібербезпеки. Згідно з цими актами, інформаційна безпека розглядається як складова національної безпеки, що охоплює захист інформаційних ресурсів, недопущення інформаційної агресії та забезпечення стійкості інформаційного простору. Водночас, як наголошують експерти Інституту інформаційного суспільства, правова база потребує оновлення з урахуванням нових технологічних викликів (зокрема, штучного інтелекту, deep fake, бот-мереж). Важливо, щоб нові правові ініціативи відповідали принципам пропорційності та справедливості.

Слід констатувати, що в інформаційній політиці важливо не лише приймати виважені закони, але й забезпечувати їх реалізацію. В галузі медіаправа виділяють такі ключові умови інформаційної політики:

- прозорість прийняття рішень щодо обмеження чи припинення діяльності ЗМІ.
- доступність процедур апеляції та правового захисту для медіаорганізацій.
- підвищення рівня медіаграмотності громадян шляхом системної просвітницької роботи.
- підтримка незалежних, громадських та суспільних ЗМІ як альтернативи олігархічному медіапростору.

Такий підхід сприяє забезпеченню свободи слова та розвитку демократичного медіасередовища, де ключовими цінностями залишаються довіра, критичне мислення та свобода.

Принцип справедливості у сфері інформаційної безпеки - це не лише правова декларація, а практичний механізм забезпечення балансу між захистом держави та правами людини. Він дозволяє уникнути крайнощів - як тотального контролю, так і інформаційної анархії. В умовах постійних гібридних загроз дотримання цього принципу є запорукою демократичного розвитку суспільства, посилення його резистентності до деструктивних впливів та збереження фундаментальних свобод.

Список використаних джерел

1. Задорожній О.В. Інформаційне право України: навч. посіб. / О.В. Задорожній. К. : Юрінком Інтер, 2015. 272 с.
2. Лисенко В.І. Свобода слова та інформаційна безпека: баланс інтересів / В. І. Лисенко // *Вісник Національної академії правових наук України.* 2019. № 4. С. 115–125.
3. Цимбалюк В. Права людини в інформаційному суспільстві / В. Цимбалюк // *Право України.* 2020. № 1. С. 43–50.
4. Кушнарьова І.В. Правове регулювання свободи слова в Україні: монографія / І.В. Кушнарьова. Х. : Право, 2017. 320 с.
5. Костенко Н., Мельник О. Інформаційна безпека та гібридні загрози: аналіз сучасних викликів / Н. Костенко, О. Мельник // *Науковий вісник Інституту інформаційного суспільства.* 2021. № 2. С. 21–29.
6. Центр стратегічних комунікацій та інформаційної безпеки. Інформаційна боротьба РФ проти України: ключові наративи [Електронний ресурс]. Режим доступу: https://spravdi.gov.ua/
7. Різун В.В. Інформаційна безпека в системі національної безпеки України: навч. посіб. / В.В. Різун. К. : Інститут журналістики КНУ імені Тараса Шевченка, 2010. 176 с.

Кривенко Валерія Вадимівна,
ад'юнкт кафедри теорії, історії та філософії права Національної академії внутрішніх справ

ПРЕВЕНТИВНА КОМУНІКАЦІЯ ЯК ІНСТРУМЕНТ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ

У сучасному глобалізованому інформаційному середовищі інформаційні загрози набувають нових форм і масштабів, стаючи одним із головних інструментів гібридних впливів, маніпуляцій громадською думкою та підриву національної безпеки. У цьому контексті превентивна комунікація виступає як стратегічний інструмент, що дозволяє не лише реагувати на інформаційні атаки, а й попереджати їх, зменшуючи їхню ефективність ще на етапі формування.

Превентивна комунікація – це комплексна система заходів інформаційного впливу, спрямованих на запобігання виникненню конфліктів, деструктивних суспільних процесів, поширенню дезінформації та фейків. Вона передбачає не лише інформування, але й активну взаємодію з громадянами, формування довіри до державних інституцій, насамперед поліції.

Інформаційна загроза – потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України

і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні [1]. Таке розуміння інформаційної загрози фактично вказує на її складний системний характер, що проявляється у формі цілеспрямованого негативного впливу на свідомість, поведінку та інститути суспільства, становить реальну або потенційну загрозу національній безпеці держави. Її наслідки проявляються у підриві демократичних процесів, дестабілізації внутрішнього середовища та послабленні обороноздатності. Відповідно, враховуючи стратегічну важливість інформаційного простору, ефективне виявлення, нейтралізація та превенція таких загроз має розглядатися як пріоритетна складова державної політики у сфері національної безпеки, що потребує науково обґрунтованого підходу, міжвідомчої координації та високого рівня інформаційної культури суспільства.

Сьогодні збройна агресія російської федерації проти України є не лише воєнним конфліктом у традиційному розумінні, а й масштабною гібридною війною, де інформаційний компонент відіграє критично важливу роль. Інформаційні загрози в цьому контексті не лише супроводжують бойові дії, а й формують окремий фронт, спрямований на підрив морального духу населення, дестабілізацію державного управління, ослаблення міжнародної підтримки та легітимацію агресії в очах як власної, так і іноземної аудиторії.

Збройна агресія рф спричинила інтенсивне зростання кількості та складності інформаційних загроз, зокрема:

- фейкові новини та дезінформація;

Дезінформація – це недостовірна, оманлива, маніпулятивна інформація, створена навмисно заради отримання економічних, політичних або інших вигод, а фейкові новини є одним із методів її поширення. Фейковим новинам притаманні такі риси як неправдивий маніпулятивний зміст; спрямованість на навмисне введення в оману, дезорієнтацію споживача; подання інформації від імені хибних або анонімних джерел; використання чуток та сатири; поширення в мережі Інтернет; економічні або політичні мовити створення [2, с. 183].

- пропагандистські кампанії активізувались у вигляді системної державної політики рф. Вони спрямовані на створення «альтернативної реальності», demonізацію України, виправдання агресії, зокрема через міфи про «визвольну місію» [3].
- кібератаки синхронізуються з військовими діями. Зокрема, у перші дні вторгнення у лютому 2022 року було зафіксовано масові кібератаки на урядові ресурси України, що супроводжували фізичний наступ.
- інформаційно-психологічні операції (ІПСО);

Інформаційно-психологічні спеціальні операції (далі – *ІПСО*) – це комплекс заходів щодо поширення спеціально підготовленої інформації з метою впливу на емоції, почуття та поведінку людей [4, с. 189]. Необхідно погодитись з М. Савлюком, який наголошує на тому, що ІПСО в соціальних мережах стали ключовим елементом гібридної війни проти України. Сьогодні можна виділити такі організаційні аспекти проведення ІПСО:

- створення мереж ботів і фейкових акаунтів;
- використання лідерів думок та псевдо експертів;

– координація дій через закриті групи та канали;
– застосування технологій глибинних шейків;
– використання алгоритмів соціальних мереж для посилення ефекту [5, с. 303; 6].

В умовах збройної агресії рф зазвичай ІПСО спрямовані на деморалізацію українського суспільства, посів паніки та підрив довіри до владних інституцій.

➢ deepfake-технології.

Дипфейк (від deep learning – глибинне навчання нейронних мереж і fake – підробка) – це технологія створення фальсифікованого, але візуально правдоподібного контенту, яка є новітньою формою онлайн-дезінформації. Його особливістю є можливість достатньо переконливо імітувати реальні, наприклад, відео, при цьому глядач може сумніватися у власному сприйнятті. Створення дипфейків може здійснюватись на основі поєднання голосу однієї особи із зображенням або відео іншої. У результаті формується реалістичний фальшивий відеозапис, на якому начебто виступає справжня людина. У більшості випадків у глядача не виникає підозри щодо фейковості побаченого [7, с. 74].

Наукові дослідження свідчать, що в умовах гібридної війни інформаційний фронт є критично важливим для досягнення стратегічних цілей противника. Згідно з висновками Національного інституту стратегічних досліджень, інформаційні впливи мають на меті трансформацію поведінки соціуму, вплив на ухвалення політичних рішень та деморалізацію військових структур [8]. Відповідно, це вимагає системного посилення національної інформаційної безпеки, розвиток стратегічної комунікації, підвищення критичного мислення та медіаграмотності суспільства.

Одним із ключових інструментів у протидії інформаційним загрозам є превентивна комунікація, зокрема і здійснювана з боку правоохоронних органів. Адже вона дозволяє формувати стійкість суспільства до маніпуляцій, забезпечує довіру до офіційних джерел і знижує рівень паніки та дезінформації.

Превентивна комунікація являє собою перш за все стратегію інформаційного впливу, яка має на меті:

– *попередження конфліктів* – інформування про потенційні ризики та конфліктогенні фактори, що можуть призвести до загострення ситуації або ескалації насильства;

– *зниження напруги*, зокрема, шляхом поширення інформації, що сприяє розумінню і співпраці між різними групами населення, що допомагає знижувати соціальну та політичну напругу;

– *інформування населення* – надавання точних і достовірних відомостей про права людини, заходи безпеки і можливості отримання допомоги в умовах воєнного конфлікту [9, с. 31-32].

Успішна протидія інформаційним загрозам потребує від органів влади, зокрема і поліції, переходу від реактивної до проактивної моделі дій. Йдеться про системне використання таких інструментів превентивної комунікації, як:

– *взаємодія з місцевими громадами*. Зокрема, поліцейські, постійно перебуваючи в певному районі, формують зв’язки з мешканцями, ідентифікують проблемні зони та разом із громадою шукають шляхи їх вирішення. Така модель

дозволяє не лише швидко реагувати на правопорушення, а й запобігати їм завдяки зміцненню довіри до поліції [10].

– медіаосвіта: навчання громадян критичному мисленню та перевірці джерел інформації. Працівники поліції систематично проводять заходи у навчальних закладах, робочих колективах, громадах – тренінги, лекції, майстер-класи щодо правової обізнаності, кібербезпеки, ненасильницького вирішення конфліктів тощо [11].

– інформаційні кампанії: створення контенту, спрямованого на розвінчання міфів і протидію пропаганді. Так, у своїй діяльності поліція активно використовує соціальні платформи (Facebook, Twitter, Instagram, YouTube) для інформування громадськості, спростування фейків, поширення рекомендацій, а також встановлення зворотного зв'язку з населенням. Цифрові канали комунікації створюють можливість для оперативного інформування про загрози та попередження злочинів [12].

– технологічні рішення: використання ІКТ для захисту інформації, наприклад, шифрування даних і моніторингу кіберпростору [13].

Прикладом ефективного використання інструментів превентивної комунікації є діяльність підрозділів комунікації Національної поліції України, зокрема у періоди соціальної напруги, терористичних загроз або масових заходів. Вчасна, правдива та цільова комунікація у таких випадках сприяє зниженню рівня паніки, протидії дезінформації та посиленню авторитету поліції.

Незважаючи на ефективність превентивної комунікації, її впровадження, зокрема з боку поліції, стикається низкою структурних, технологічних і суспільних бар'єрів. Зокрема, недостатня цифрова грамотність населення призводить до порушення ними правил кібергігієни. В свою чергу, недостатня кількість поліцейських, які належно володіють інструментами цифрової комунікації та кризових комунікацій, не дозволяє здійснювати ефективну превентивну діяльність у цьому напрямі, особливо на деокупованих територіях. Також, необхідно погодитись з Ю.В. Шевченко, який наголошує на тому, що відсутність системи моніторингу ІПСО та оперативного реагування на ворожі меседжі створює суттєві ризики для суспільної довіри [14].

Існує потреба у формуванні належної взаємодії між усіма органами державної влади, зокрема і поліцією, оргранами місцевого самоврядування, медіа та громадськими організаціями. Доцільно, на наш погляд, створити постійно діючі платформи такої взаємодії.

Підсумовуючи вищевикладене, необхідно зазначити, що превентивна комунікація є ефективним інструментом протидії інформаційним загрозам, що дозволяє мінімізувати вплив дезінформації, пропаганди та кібератак. Вона ґрунтується на освітніх, організаційних і технологічних заходах, які забезпечують інформаційну безпеку та стійкість суспільства. Для успішної реалізації превентивної комунікації необхідно посилити цифрову грамотність громадян, удосконалити організаційно-технічну модель кіберзахисту. Доцільно здійснити інституційну реформу комунікаційної функції органів влади, зокрема і поліції, створити сталі партнерства із громадськими та медійними структурами тощо.

Список використаних джерел

1. Стратегя інформаційної безпеки України: Указ Президента України від 21 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text
2. Тищенко В.С., Мужанова Т.М. Дезінформація і фейкові новини: ознаки та методи виявлення в мережі Інтернет. *Кібербезпека: освіта, наука, техніка.* 2022. № 2 (18). С. 175-186. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/413/341
3. Pomerantsev, P. This Is Not Propaganda: Adventures in the War Against Reality. London : Faber & Faber, 2019. 288 p.
4. Бартельова А., Рудь О. Інформаційно-психологічні операції як основна загроза інформаційній безпеці держави. / Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи. Харків, 2023. С. 188-190. URL: https://www.researchgate.net/publication/376773925_Informacijno-psihologicni_operacii_ak_osnovna_zagroza_informacijnij_bezpeci_derzavi
5. Савлюк М. Важливість інформаційної безпеки в соціальних мережах для загальнонаціональної безпеки: безпековий вимір України. *Вісник Прикарпатського університету.* Серія: Політологія. 2024. Випуск 18. С. 300-309. URL: https://journals.pnu.if.ua/index.php/politology/article/view/167/164
6. Благодарний А.М., Штельмах О.В. Організаційні аспекти протидії інформаційній агресії як складовій гібридної війни. *Інформаційна безпека людини, суспільства, держави.* 2015. № 3. С. 48–54.
7. Доскіч Л.С. Фейкові новини як новітній засіб маніпуляції та дезінформації. *Бібліотекознавство. Документознавство. Інформологія.* 2022. № 4. С. 72–77.
8. Національний інститут стратегічних досліджень. Превентивна комунікація як елемент інформаційної політики держави. URL: https://niss.gov.ua
9. Кривенко В.В. Роль превентивної комунікації у забезпеченні прав людини в умовах збройного конфлікту. / Актуальні питання становлення та розвитку сучасного конституціоналізму в Україні: матеріали науково-практичного столу (Київ, 28 червня 2024). 2024. 87с. С. 31-33. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/6c086bb4-2a42-4a9a-9728-3b09c99d6e2a/content
10. Войтович, О.М. Community policing як складова запобігання злочинності в Україні. *Право і безпека*. 2021. № 2. С. 37–42.
11. Антонюк, А.В. Освітні ініціативи поліції як засіб профілактики правопорушень серед молоді. *Юридичний вісник України*. 2020. № 4. С. 52–58.
12. Науменко, Д.І. Комунікаційна стратегія Національної поліції у соціальних мережах. *Інформаційне суспільство*. 2022. № 3. С. 28–33.
13. Яремчук Ю.Є., Павловський П.В., Катаєв О.В. Комплексні системи захисту інформації. Вінниця: ВНТУ, 2023. URL: https://web.posibnyky.vntu.edu.ua
14. Шевченко, Ю.В. Стратегії протидії ІПСО в діяльності правоохоронних органів. *Сучасні інформаційні технології і суспільство*. 2023. № 2. С. 66–72.

Курачик Тарас Володимирович,
аспірант відділу теорії держави і права Інституту держави і права імені В.М. Корецького НАН України

НАСЛІДКИ НЕПРАВОМІРНОГО ОБМЕЖЕННЯ ПРАВ ЛЮДИНИ

Питання забезпечення прав людини в умовах надзвичайного чи воєнного стану набуло особливої актуальності в умовах повномасштабної збройної агресії проти України. Воєнний стан, як особливий правовий режим, неминуче передбачає певне обмеження конституційних прав і свобод, однак ключовим залишається питання дотримання меж допустимості таких обмежень. Право не визнає довільності навіть у період надзвичайних викликів.

В умовах реалій 2022−2025 років Україна продемонструвала приклад балансу між захистом національної безпеки, зокрема в інформаційній сфері, та збереженням основоположних прав людини. Водночас деякі ситуації свідчать про ризики надмірних чи неправомірних обмежень, що породжують не лише юридичні, а й соціально-економічні та політичні наслідки.

Юридична відповідальність держави за неправомірні дії щодо прав людини ґрунтується на принципі верховенства права. Держава, навіть у період воєнного стану, залишається відповідальною за дотримання міжнародних зобов'язань, передбачених міжнародними договорами, такими як Міжнародний пакт про громадянські і політичні права, Європейська конвенція з прав людини, а також нормами Конституції України.

Зловживання правом введення надзвичайного стану, надмірні обмеження свободи слова, мирних зібрань, необґрунтовані затримання громадян чи тиск на опозицію можуть кваліфікуватися як порушення міжнародного права. Такі дії можуть стати предметом розгляду в міжнародних юрисдикційних органах, зокрема в Європейському суді з прав людини.

В українській правовій системі відповідальність держави передбачена, зокрема, у формах: відшкодування шкоди, завданої незаконними рішеннями, діями чи бездіяльністю органів державної влади; реабілітації постраждалих внаслідок неправомірних дій; відновлення порушених прав через судові процедури.

Правова доктрина і міжнародні стандарти однозначно виходять з того, що жодне обмеження прав людини не може бути свавільним, а будь-які дії держави повинні бути засновані на законі, бути необхідними, обґрунтованими та пропорційними реальним потребам безпеки.

Унікальність української правової моделі функціонування режиму воєнного стану у період 2022−2025 років полягала у широкому залученні інститутів парламентського контролю, громадянського суспільства та міжнародних партнерів до процесу правової оцінки запроваджених обмежень, зокрема у сфері інформаційної безпеки. Запровадження обмежувальних заходів без правової підстави, у разі їх доведення, тягне відповідальність посадових осіб, які

перевищили службові повноваження.

Також важливим є механізм індивідуальних скарг, коли громадяни мають можливість оскаржити дії влади в національних судах, а за потреби – в міжнародних інстанціях.

Неправомірне обмеження прав людини має не лише юридичні, а й значні соціально-економічні та політичні наслідки. Порушення прав громадян у період дії воєнного стану може призводити до зростання соціального напруження, недовіри до державних інституцій та формування протестних настроїв. Зокрема, безпідставне обмеження свободи слова, права на доступ до інформації чи свободи пересування стає однією з основних причин дестабілізації суспільства, що особливо небезпечно в умовах збройного конфлікту.

Український досвід останніх років продемонстрував, що навіть в умовах війни надмірні обмеження чи дискримінаційні заходи в інформаційній сфері, у сфері праці або соціального захисту здатні спровокувати широкий суспільний резонанс та міжнародну критику. Відповідно, держава має виважено застосовувати обмежувальні заходи, постійно оцінюючи їх пропорційність і відповідність міжнародним стандартам.

Соціальною проблемою можуть стати і наслідки порушень права на працю, права на освіту чи права на соціальне забезпечення. Втрата роботи, переміщення підприємств, обмеження мобільності населення внаслідок неправомірних дій органів влади посилюють соціальну вразливість громадян, що може призвести до довгострокових наслідків навіть після завершення дії воєнного стану.

Особливо актуальним є питання впливу неправомірних обмежень на інформаційну безпеку суспільства. З одного боку, забезпечення національної безпеки вимагає оперативного реагування на загрози інформаційної війни, кібератак та дезінформації. З іншого боку, надмірне блокування ресурсів, обмеження доступу до джерел інформації або переслідування журналістів можуть призводити до порушення основоположних прав громадян.

З міжнародної точки зору, такі практики можуть кваліфікуватися як порушення статті 19 Міжнародного пакту про громадянські і політичні права, яка гарантує свободу вираження поглядів. Україна, яка перебуває в центрі глобальної уваги, повинна забезпечити максимально прозорі, обґрунтовані та легітимні рішення, щоб не допустити погіршення міжнародного іміджу та втрати підтримки з боку ключових партнерів.

Політичні наслідки неправомірного обмеження прав можуть бути ще більш серйозними. Серед громадян зростає скепсис щодо здатності держави діяти в рамках права, знижується довіра до органів влади та правоохоронної системи. У повоєнний період такі тенденції можуть перерости в глибоку політичну кризу, особливо якщо не будуть прийняті своєчасні рішення щодо реабілітації постраждалих та відновлення довіри.

Водночас аналіз зарубіжного досвіду показує, що країни, які вміло поєднували забезпечення національної безпеки та дотримання прав людини, зуміли уникнути негативних довгострокових наслідків. Наприклад, після завершення надзвичайного стану в Ізраїлі або Франції були створені спеціальні механізми парламентського та судового контролю, а також незалежні інституції

для моніторингу дотримання прав людини.

Для України цей досвід є надзвичайно важливим. Забезпечення прав людини в умовах воєнного стану та повоєнного періоду повинно стати частиною стратегії постконфліктного врегулювання і демократичного відновлення. Збереження довіри громадян, захист прав і свобод, дотримання принципів верховенства права мають стати основними орієнтирами для державної політики.

Підсумовуючи, можна зазначити, що неправомірне обмеження прав людини в умовах воєнного стану не лише створює юридичні підстави для відповідальності держави, а й має масштабні соціально-економічні та політичні наслідки. Відповідальне застосування державою надзвичайних повноважень є визначальним чинником стабільності в умовах кризи та формування демократичної моделі розвитку в повоєнний період.

Забезпечення балансу між захистом національних інтересів, інформаційною безпекою суспільства та гарантіями основоположних прав людини є однією з ключових умов збереження громадської довіри та міжнародного авторитету України. У цьому контексті важливо посилювати інституційні механізми контролю, забезпечити реальне право громадян на ефективний захист і оскарження дій державних органів, а також поступово адаптувати правову систему до викликів сучасних воєн і гібридних загроз.

Особливу увагу в повоєнний період слід приділити питанням реабілітації постраждалих від неправомірних обмежень, відновленню соціальних гарантій, компенсацій та відшкодування шкоди. Для України це є шансом посилити правові інститути, оновити національне законодавство відповідно до міжнародних стандартів і забезпечити реальний захист прав та свобод людини навіть у найскладніших безпекових умовах.

Інформаційна безпека у цьому контексті має стати одним із пріоритетних напрямів, адже сучасна війна має не лише військовий, а й інформаційний вимір. Пошук ефективних механізмів запобігання дезінформації, захисту інформаційного простору при одночасному забезпеченні свободи слова та доступу громадян до інформації має бути ключовим завданням державної політики в сфері прав людини.

Логінов Сергій Євгенійович,
слухач інституту заочного та дистанційного навчання Національної академії внутрішніх справ

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ ФУНКЦІЇ ПАТРУЛЬНОЇ ПОЛІЦІЇ В УМОВАХ ВОЄННОГО СТАНУ

В 2014 році російською федерацією щодо України було здійснено акт збройної агресії в результаті якого виникла анексія Криму, окупація частин Донецької та Луганської областей. Проте ворог на цьому не зупинився і у 2022

році агресія набула повно масштабного характеру. В результаті повномасштабного вторгнення російської федерації на територію України указом Президента України було введено воєнний стан в країні [1], задля здійснення належної протидії діяльності ворога. Введення воєнного стану в Україні широко видозмінила діяльність ряду державних інститутів і патрульну поліцію ці зміни не оминули.

В умовах збройної агресії проти України особливого значення набуває ефективна діяльність правоохоронних органів, зокрема патрульної поліції, у сфері забезпечення громадського порядку, безпеки та довіри населення до держави. Одним із ключових аспектів цієї діяльності є реалізація інформаційної функції, яка в умовах воєнного стану набуває стратегічного значення як елемент превентивної комунікації, протидії дезінформації та посилення соціальної згуртованості.

В загальному функції Національної поліції України – це визначені та закріплені на правовому рівні напрями діяльності суб'єктів поліцейської діяльності, які є взаємопов'язаними і взаємоузгодженими та спрямованими на вирішення поставлених перед нею завдань [2, с. 73]. Аналіз Закону України «Про Національну поліцію України» [3] вказує, що у ньому не закріплено переліку функцій, що покладаються на поліцію. Натомість, щодо діяльності патрульної поліції у розділі ІІІ «Функції патрульної служби» Положення про патрульну службу МВС [4] зазначено, що вона відповідно до покладених на неї завдань здійснює реалізацію таких функцій:

1) цілодобове патрулювання території обслуговування з метою забезпечення належної охорони громадського порядку, громадської безпеки та контролю за дотриманням правил дорожнього руху, забезпечення його безпеки. У разі необхідності здійснює регулювання дорожнього руху;

2) перше реагування на повідомлення про правопорушення, надання невідкладної допомоги; своєчасне реагування на повідомлення про вчинення правопорушень, а також з метою надання допомоги громадянам. Надає невідкладну допомогу потерпілим від нещасних випадків, правопорушень, аварій, пожеж та інших надзвичайних ситуацій до прибуття на місце компетентних служб;

3) самостійне виявлення правопорушень

4) припинення правопорушень

5) затримання правопорушників та доставлення їх до підрозділів органів внутрішніх справ.

6) охорону місця події.

7) співпрацю з іншими структурними підрозділами органів внутрішніх справ

8) спілкування і співпрацю із суспільством та ін.

Однією із функцій покладених на поліцію є й інформаційна функція, яка набула особливого значення у воєнний період. Вона стала стратегічним інструментом державної безпеки та політики, адже в результаті належного виконання дозволяє забезпечити громадський спокій, поширювати важливу офіційну інформацію серед населення та спростовувати здійснення діяльності

ворожих інформаційно-психологічних операцій (далі – *ІПСО*), які мають, на жаль в результаті слабкої обізнаності громадян, дуже широкомасштабний вплив на них.

Аналіз законодавства та реалій сьогодення дозволяє виокремити такі основні напрями реалізації інформаційної функції патрульною поліцією:

- оперативне інформування населення щодо надзвичайних подій, змін у режимах пересування, введення обмежень та заходів безпеки;
- попередження інформаційних загроз, зокрема розвінчування фейків, протидія російській пропаганді через офіційні канали зв'язку (Telegram, Facebook, Instagram тощо);
- комунікація з громадянами з метою підтримки довіри, зменшення соціальної напруги, пояснення рішень державних інституцій [5];
- партнерство з медіа та органами місцевої влади для узгодженого донесення інформації;
- залучення до просвітницьких кампаній, зокрема щодо правил поведінки під час повітряної тривоги, евакуації, виявлення підозрілих предметів або осіб [6].

В умовах воєнного стану реалізація інформаційної функції супроводжується низкою викликів:

– навантаження на особовий склад через багатофункціональність виконуваних завдань;

У період воєнного стану патрульна поліція залучається до виконання завдань, які не є типовими для мирного часу. Зокрема, вона співпрацює з військовими адміністраціями, здійснює охорону критичної інфраструктури, забезпечує евакуацію цивільного населення, допомагає в організації обмежень руху в зоні бойових дій або на стратегічно важливих об'єктах. Патрульні підтримують правопорядок під час повітряних тривого, одні із перших приходять на допомогу під час та після обстрілів. Відповідно, необхідно погодитись з, які стверджують, що поліцейські часто працюють в умовах перевантаження, що супроводжується моральним і фізичним виснаженням [7, с. 635].

– високий рівень психологічної напруги у суспільстві, що ускладнює сприйняття навіть офіційної інформації [6];

Постійна загроза життю, великі ризики та високий рівень відповідальності підвищують рівень стресу серед патрульних, що може призводити до психологічного вигорання, зниження ефективності роботи тощо [7, с. 635].

– інформаційне перенасичення — велика кількість повідомлень різного походження знижує здатність до критичного аналізу;

– цілеспрямовані інформаційно-психологічні операції (ІПСО) з боку противника.

Проблемним також є обмеженість технічних та кадрових ресурсів. Підрозділи патрульної поліції не мають належного доступу до професійного SMM-супроводу, належного обладнання в повному обсязі для створення якісного інформаційного контенту та ін.

Успішна реалізація інформаційної функції можлива, на наш погляд, лише за наявності комплексного підходу, який передбачає навчання та підготовку патрульних у сфері кризових комунікацій, публічного виступу, протидії фейкам, цифрової грамотності, розвиток партнерства з медіа, блогерами, громадськими організаціями – для розширення охоплення та посилення впливу. Крім того, слід розуміти, що інформаційна функція патрульної поліції має превентивний потенціал – вона здатна попереджати заворушення, паніку, дезорганізацію. А в умовах війни кожна година стабільності – це зміцнення тилу, економіки, морального стану населення.

В цілому, для підвищення ефективності інформаційної функції патрульної поліції доцільно:

- запровадити регулярне навчання працівників поліції з питань стратегічних комунікацій [5];
- поглибити співпрацю з Центром стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики України;
- створити мобільні інформаційні групи в складі патрульної поліції для оперативного реагування на інциденти інформаційного характеру;
- інтенсифікувати використання мультимедійних каналів для поширення офіційної інформації (наприклад, відеоролики).

Підсумовуючи вищевикладене, можна сказати, що інформаційна функція патрульної поліції в умовах воєнного стану є не лише інструментом забезпечення громадської безпеки, а й важливою складовою національної стійкості. Ефективна комунікація з населенням, протидія фейкам, участь у формуванні соціального капіталу – це завдання, що мають стратегічне значення в умовах гібридної війни. Саме тому необхідно інституціоналізувати інформаційну діяльність поліції як пріоритетну та забезпечити її належними ресурсами й підготовкою персоналу.

Список використаних джерел

1. Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389-VIII URL: https://zakon.rada.gov.ua/laws/show/389-19
2. Корольова В. Функції поліції України як юридична категорія. *Legal Bulletin*, 2022. № 4. С. 69–73. URL: https://lbku.krok.edu.ua/index.php/legal-bulletin/article/view/348/287
3. Про Національну поліцію України: Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19
4. Положення про патрульну службу МВС: Наказ Міністерства внутрішніх справ України від 02.07.2015 № 796. URL: https://zakon.rada.gov.ua/laws/show/z0777-15/conv#Text
5. Рудик С.В. Превентивна діяльність поліції: комунікаційний аспект. *Юридичний вісник України*. 2022. № 11. С. 22–27.
6. Литвин В.М., Вдовиченко М.С. Інформаційна безпека в умовах гібридної війни: виклики та загрози. *Інформаційне право України*. 2023. № 2. С. 45–51.

7. Молокова А.Р., Бухтіярова І.Г. Особливості діяльності патрульної поліції в період воєнного стану. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2024. № 6. С. 632-637. URL: https://app-journal.in.ua/wp-content/uploads/2024/12/105.pdf

Лось Дар'я Ігорівна,
студент факультету фінансів Київського національного економічного університету імені Вадима Гетьмана

ІНФОРМАЦІЙНА БЕЗПЕКА СУСПІЛЬСТВА В УМОВАХ ДІЇ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ ТА ПОВОЄННИЙ ПЕРІОД

Інформаційна безпека у сучасному світі є ключовою складовою національної безпеки, особливо в умовах збройного конфлікту. З початком повномасштабної агресії рф проти України у 2022 році, питання захисту інформаційного простору стало життєво важливим [5, с. 52–58]. Війна XXI століття ведеться не лише на полі бою, але й у кіберпросторі, на телебаченні, в соціальних мережах, у месенджерах. Саме тому ефективне забезпечення інформаційної безпеки у період воєнного стану та в післявоєнній відбудові є пріоритетом державної політики [6, с. 18-24].

Воєнний стан в Україні запроваджується згідно із Законом України «Про правовий режим воєнного стану» [1]. Цей правовий режим передбачає тимчасове обмеження низки прав і свобод, включаючи свободу слова, з метою захисту інтересів держави. Відповідно до ст. 22 Закону, в умовах воєнного стану можуть запроваджуватися: цензура інформації; обмеження роботи ЗМІ; заборона на поширення певної інформації, що може завдати шкоди обороноздатності [1].

Серед ключових загроз можна виділити: дезінформацію та фейки, кіберзагрози, психологічні операції (PSYOPS), витік конфіденційної інформації [7, с. 44-49]. Для протидії цим загрозам Україна активізувала діяльність Центру протидії дезінформації при РНБО [4], Служби безпеки України, а також волонтерських ініціатив.

Інформаційна політика в період війни має подвійне завдання: захист державної таємниці і національних інтересів, а також забезпечення прозорості, інформування громадян і формування стійкості суспільства [6, с. 18-24]. Успішною практикою є щоденні брифінги, робота офіційних каналів, оперативна реакція на фейки.

Після завершення активної фази війни Україна зіткнеться з такими викликами: реінтеграція деокупованих територій, поствоєнна реабілітація суспільства, відновлення національного медіапростору, протидія гібридним впливам. Особливої уваги потребуватимуть: медіаграмотність, удосконалення законодавства, розвиток аналітичної інфраструктури.

Інформаційна безпека в умовах війни та після неї є фундаментом для стійкості, виживання та відновлення держави. Ефективне законодавче

регулювання, стратегічна комунікація, розвиток інформаційної культури та технологічної інфраструктури мають бути основою державної політики [3].

Додатково варто наголосити на важливості співпраці з міжнародними партнерами у сфері інформаційної безпеки. Україна активно інтегрується в європейський інформаційний простір, бере участь у спільних ініціативах з ЄС та НАТО щодо кіберзахисту, обміну розвідувальною інформацією та протидії дезінформації [5, с. 52-58].

Окрему увагу слід приділити ролі освіти, зокрема розвитку медіаосвітніх програм у школах, університетах, а також для дорослого населення. Формування критичного мислення та навичок розпізнавання інформаційних впливів є запорукою стійкості суспільства до пропаганди.

Не менш важливим є удосконалення національного законодавства в частині кібербезпеки, захисту персональних даних, регулювання діяльності соціальних мереж та платформ онлайн-комунікації. Потрібно забезпечити баланс між безпекою та свободою слова, не допустивши зловживання владними повноваженнями [2]. Пропонуємо внести зміни до Закону України «Про основні засади забезпечення кібербезпеки України», доповнивши його обов'язковими галузевими стандартами та національною сертифікацією критичних інформаційних систем, жорсткими строками повідомлення про інциденти, ризик-орієнтованим підходом та державним резервом експертів; водночас оновити Закон України «Про захист персональних даних», запровадивши право переносу, видалення й обмеження обробки даних, закріпивши принцип захисту даних «з проєктування» й «за замовчуванням», наділивши контролюючий орган правом планових і позапланових перевірок із значними санкціями та публічним реєстром витоків і строком інформування до 72 годин; а в частині онлайн-платформ доповнити Закон України «Про інформацію» та Закон України «Про електронні комунікації» визначенням категорій великих сервісів за розміром аудиторії, вимогами до модерації й звітності, прозорістю алгоритмів та незалежними аудитами, забороною реклами для користувачів до 16 років, чіткими строками реагування на скарги й судовим контролем доступу до даних, координуючи все через спеціальну міжвідомчу раду з урахуванням міжнародного досвіду та обов'язкових навчальних програм для фахівців.

У повоєнний період держава повинна підтримувати розвиток незалежних медіа, які дотримуються журналістських стандартів, та сприяти зміцненню громадянського суспільства як активного учасника інформаційного захисту країни.

Висновок. Інформаційна безпека в умовах воєнного стану та у повоєнний період є не лише елементом національної безпеки, а й інструментом збереження державності, суверенітету та суспільної єдності. Успішна протидія ворожим інформаційним впливам потребує поєднання правових, технологічних, освітніх і комунікаційних заходів [5, 6].

Забезпечення інформаційної безпеки суспільства в умовах війни та в повоєнний час вимагає комплексного підходу, який поєднує правове регулювання, технологічні рішення й культивування медіаграмотності громадян. По-перше, необхідно адаптувати законодавчі норми до реалій воєнного стану –

передбачити пріоритетність захисту критичної інфраструктури, оперативний обмін розвідувальною інформацією та чіткі механізми протидії дезінформації. По-друге, у повоєнний період варто закріпити набуті зусилля через довгострокові програми модернізації систем кібербезпеки, підвищення кваліфікації державних службовців і фахівців ІТ-галузі та формування в суспільстві критичного сприйняття джерел інформації. Лише синергія жорстких норм, інноваційних технологій і просвітницьких ініціатив може створити стійку систему інформаційної безпеки, здатну захистити державу й громадян як під час загрози, так і на етапі відновлення.

Список використаних джерел

1. Про правовий режим воєнного стану : Закон України від 12.05.2015 р. № 389-VIII. URL:https://zakon.rada.gov.ua/laws/show/389-19#Text\.
2. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL:https://zakon.rada.gov.ua/laws/show/2469-19#Text.
3. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 14.02.2017 р. № 47/2017 URL:https://zakon.rada.gov.ua/laws/show/47/2017#Text
4. Центр протидії дезінформації при РНБО України – Офіційний сайт, URL:https://cpd.gov.ua/
5. Ситник І.І. Інформаційна безпека в умовах гібридної війни: національний і міжнародний виміри. *Вісник НАДУ при Президентові України*. 2022. № 1. С. 52–58.
6. Костюченко О.В. Інформаційна політика держави в умовах воєнного стану. *Національна безпека і оборона*. 2023. № 2(158). С. 18–24.
7. StopFake.org. Платформа протидії дезінформації: URL:https://www.stopfake.org/.

Майсук Романа Романівна,
студент навчально-наукового інституту права та психології Національної академії внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА СУСПІЛЬСТВА В УМОВАХ ВОЄННОГО СТАНУ: ПРАВОВІ ВИКЛИКИ ТА ПРАВОЗАСТОСУВАННЯ

В наш час, в умовах воєнного стану, ще більш актуального значення набуває безпека, особливо коли відбувається не лише фізична, але й інформаційна агресія. Забезпечення інформаційної безпеки набуває критичної важливості та запобігає спробам посіяти паніку серед населення. Широке використання цифрових технологій зумовлює появу нових форм загроз, таких як кібератаки, дезінформація та маніпулювання інформацією. Однією з основних правових проблем є необхідність розробки нормативно-правових актів, які б ефективно регулювали захист від кібератак, забезпечували прозорість у використанні

інформаційних технологій державними органами, а також захищали права громадян в умовах надзвичайних ситуацій. Такі заходи допомагають не лише у протидії зовнішнім загрозам, але й у захисті від внутрішніх дестабілізуючих чинників, таких як фальсифікація інформації у медіапросторі [1, с. 289].

Науковці звертають увагу на багатовекторність цієї загрози. Так, Лизанчук В.В. у своїй праці зазначає, що ключовим елементом має стати не лише репресивна, а й превентивна стратегія: навчання населення медіаграмотності, розвиток критичного мислення та створення національних платформ перевірки фактів. Водночас Кудінов В.А., підкреслює, що варто врегулювати відповідальність за поширення фальшивої інформації, забезпечити можливість оперативного спростування фейків, а також надати правоохоронним органам необхідні інструменти для протидії інформаційним диверсіям.

Одним із ключових правових викликів у період воєнного стану є гарантування цифрової безпеки – як на рівні держави, так і на рівні кожного громадянина. Особливої уваги потребує кіберзахист об’єктів критичної інфраструктури: енергетичних, комунікаційних, банківських систем. Для цього важливо вдосконалити національне законодавство щодо кібербезпеки, розробити ефективні механізми моніторингу інформаційних потоків та забезпечити міжнародну взаємодію для протидії кіберзагрозам. Скоординована співпраця з іншими країнами допоможе своєчасно реагувати на атаки та поширювати успішні практики цифрового захисту [2, с. 88].

У часи воєнних конфліктів зростає значення боротьби з дезінформацією, яка може посилювати паніку, підривати моральний дух громадян і загалом ставити під загрозу національну безпеку. Протидія інформаційній агресії включає розробку правових норм для боротьби з маніпуляціями в ЗМІ та соціальних мережах. Це включає встановлення законодавчих обмежень щодо поширення фальшивих новин, інструкцій для правоохоронних органів щодо протидії інформаційним операціям супротивника, а також механізми швидкої перевірки і спростування фейкових повідомлень. Водночас важливо забезпечити баланс між безпекою і свободою вираження думок, що є одним із найбільших правових викликів у цьому напрямку.

Варто зазначити, що порушення інформаційної безпеки у часи війни можуть мати особливо тяжкі наслідки. Тому правова система має передбачати посилену відповідальність за дії, які підривають інформаційну стабільність держави. Це стосується не лише кібератак, а й поширення пропаганди, інформаційного шпигунства чи технічного саботажу. Також необхідно впровадити ефективний контроль за діяльністю цифрових платформ, через які може поширюватися шкідливий контент. Посилення покарань, чітке визначення диспозиції кримінального правопорушення у сфері інформаційної безпеки та правозастосування у реальному часі – критично важливі для захисту держави [3].

В умовах воєнного стану, зокрема під час цифрової війни, постає проблема захисту основних прав людини, таких як право на приватність і право на свободу вираження думок. Законодавство повинно чітко регулювати, як збирається, обробляється та використовується інформація про громадян, особливо в умовах надзвичайних ситуацій. Законодавство має чітко окреслювати межі допустимого

збору та використання інформації, а контроль з боку незалежних інституцій допоможе запобігти зловживанням. Таким чином, дотримання прав людини в умовах цифрової війни має залишатись невід'ємною частиною правової стратегії держави.

Список використаних джерел

1. Лизанчук В.В. Інформаційна безпека України: теорія і практика: підручник. Львів: ЛНУ ім. Івана Франка, 2017. 725 с.

2. Кудінов В.А., Яровий К.В. Інформаційне забезпечення правоохоронної діяльності: навч.-практ. посіб. Київ: Нац. акад. внутр. справ, 2024. 120 с.

3. Крайнов В.О., Маланчук М.Ф., Грозовський Р.І. Методика оцінки ефективності комплексної системи захисту інформації автоматизованих інформаційних систем органів військового управління. К.: НУОУ, *Сучасні інформаційні технології у сфері безпеки та оборони,* 2020р. №1(37). С. 103-106.

Марченко Карина Олександрівна,
курсант навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ

ПРАВОВІ АСПЕКТИ ОБМЕЖЕННЯ ДОСТУПУ ДО ІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ

У зв'язку з новими викликами, що постали в умовах воєнного стану є необхідним перманентно враховувати та переглядати інформацію, розповсюдження якої може бути причиною смертельної небезпеки для життя та здоров'я людей, а також становити загрозу територіальній цілісності держави. Відкритість функціонування органів влади підвищує їх ефективність, а систематичний громадський нагляд є гарантією справедливого розподілу ресурсів. Фактично, держава оперує величезним обсягом критично важливої інформації, тому потрібні чіткі норми, що визначатимуть її обіг як у мирний час, так і особливо в умовах воєнних дій, що і зумовлює актуальність теми дослідження.

Внаслідок збройної агресії росії проти України, нашій державі довелося вдатися до обмежень у доступі до певних документів та інформації. Такі заходи було прийнято заради забезпечення захисту національних інтересів та збереження територіальної цілісності країни. Доцільно в даному аспекті зазначають І.І. Голубенко та А.Г. Саградян: «Це дозволяє державі взяти під контроль інформаційний простір та забезпечити захист національних інтересів. Проте, разом з тим, подібні заходи можуть значно обмежити доступ громадян до публічної інформації. Це може відбуватися через обмеження доступу до деяких інформаційних джерел, а також шляхом введення комендантської години» [1, с. 145]. Тому відправною точкою для законного обмеження доступу до інформації є врахування принципу презумпції відкритості публічної інформації.

У ч. 2 ст. 1 ЗУ «Про доступ до публічної інформації» визначено, що публічна інформація є відкритою, за винятком випадків, передбачених законодавством [2].

Відповідно до приписів ч. 2 ст. 64 Конституції України, в умовах воєнного часу допускається обмеження деяких конституційних прав та свобод громадян. Насамперед, це стосується права вільно збирати, зберігати, застосовувати та поширювати інформацію у будь-який спосіб [3]. Як вже було сказано вище, можливість доступу до інформації може бути обмежена в період воєнного стану, насамперед для гарантування національної безпеки та цілісності території країни. Наприклад, прямо заборонено розповсюдження відомостей щодо поставок, транспортування зброї, озброєння та боєприпасів в Україну. Аналогічно під забороною знаходиться поширення даних про переміщення, дислокацію Сил оборони України та інших військових формувань, які діють відповідно до українського законодавства. При цьому «доступ до відомостей щодо екологічного стану, якості харчів та предметів щоденного вжитку неможливо обмежити, зважаючи на умови воєнного часу. Згідно з положеннями статті 50 Конституції України, відповідна інформація не підлягає засекреченню» [4, с. 298].

Вважаємо потрібним наголосити, що законодавство не містить жодних спеціальних положень щодо обмеження доступу до інформації в сучасних умовах. Так само відсутні норми, які можна було б ігнорувати. Відповідно до ст. 13 ЗУ «Про доступ до публічної інформації», всі розпорядники інформації, незалежно від нормативного акта, на підставі якого вони працюють, при прийнятті рішень стосовно доступу до інформації повинні керуватися цим Законом [2]. Таким чином, правила щодо обмеження доступу до публічної інформації залишаються незмінними, проте зазнали трансформацій обставини, за яких ці правила варто використовувати. Зокрема, існування реєстрів значно полегшує повсякденні операції в мирний час, але у воєнний період зростає ризик неправомірного використання інформації з реєстрів агресором, що ставить під загрозу безпеку країни, бізнесу та громадян [1, с. 146]. Відповідно до обставин розпорядник матиме право відхилити запит на інформацію лише за наявності підстав, чітко визначених чинним законодавством. Зокрема, ст. 22 Закону України «Про доступ до публічної інформації» містить перелік підстав для відмови у задоволенні запиту, а також визначає, що у відмові повинна бути вказана мотивована причина [2]. При цьому строки розгляду запитів залишаються незмінними. Проте, неспроможність оперативно опрацьовувати запити та надавати відповіді в умовах воєнного стану зумовлена тим, що ключова увага державних органів та органів місцевого самоврядування, відповідно до ст. 8 ЗУ «Про правовий режим воєнного стану», має приділятися заходам, що націлені перш за все на упередження загроз, відбиття збройної агресії та гарантування національної безпеки [5].

Таким чином, обмеження доступу до відомостей допускається винятково у випадках, коли це необхідно для державної безпеки, збереження цілісності території або забезпечення громадського спокою. Це робиться з метою недопущення заворушень, а також злочинних діянь. Крім того, обмеження можливе для охорони здоров’я населення, захисту прав, честі та гідності

громадян. Запобігання розголошенню конфіденційної інформації та підтримка авторитету судової влади також є вагомими причинами для обмеження такого права.

Для прикладу доцільно розглянути Постанову Верховного Суду від 14 лютого 2025 року у справі №420/20384/23. У даній ситуації Верховний Суд акцентував увагу на тому, що норми ч. 2 ст. 6 ЗУ «Про доступ до публічної інформації» окреслюють передумови для обмеження доступу до відомостей, а не підстави для їх надання. Цей підхід ґрунтується на положеннях ст. 1 цього Закону, яка закріплює презумпцію відкритості публічної інформації, доступ до якої може бути обмежений виключно тоді, коли розпорядник інформації обґрунтує це, використовуючи «трискладовий тест». Доведення факту можливості обмеження доступу до інформації покладається на розпорядника публічної інформації [6].

Отже, зарахування відомостей до розряду з обмеженим доступом не означає автоматичну відмову у їхньому наданні. Розпорядники повинні керуватися «трискладовим тестом», розглядаючи звернення. Безпідставна відмова у наданні інформації є неправомірною [6]. Аналізуючи рішення судів у справах про оскарження відмов суб'єктів владних повноважень щодо надання відповідей на запити про публічну інформацію, можна зробити висновок, що у рішеннях про відмову у доступі до конкретної публічної інформації недостатньо просто послатися на законодавство, оскільки така відповідь буде визнана непереконливою.

Не менш суттєвим є питання обмеження доступу до екологічних відомостей. Зважаючи на російську агресію проти України та її нищівні наслідки, критично важливим є забезпечення доступу до екологічної інформації. Адже це ключова запорука здійснення та охорони прав кожного громадянина на безпечне для життя та здоров'я. Безумовно, враховуючи повномасштабне вторгнення, гарантувати та повною мірою забезпечити цей доступ для всіх громадян на території всієї держави, як це було в мирний час, наразі неможливо. Війна спричинила низку тимчасових обмежень щодо поширення інформації, та на вільний доступ до даних про навколишнє середовище [7, с. 140]. Проте, як уже зазначалося, доступ до такої інформації не може бути обмежений повністю.

Отже, введення воєнного стану не анулює право громадян на доступ до інформації, а обмеження доступу до неї допускається виключно з огляду на інтереси національної безпеки, цілісності території чи громадського порядку, та повинно бути суворо обґрунтованим, відповідно до положень законодавства. Це зумовлено тим, що в умовах воєнних дій, доступ до інформації набуває значення ключового юридичного інструменту, здатного рятувати життя та забезпечувати захист здоров'я особистості.

Список використаних джерел

1. Голубенко І.І. Правові питання реалізації права на доступ до публічної інформації в умовах воєнного стану. *Юридичний науковий електронний журнал.* 2023. № 23. С. 144-147.

2. Про доступ до публічної інформації: Закон України від 13.01.2011, №2939-VI. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2939-17/conv#n40 (дата звернення: 16.05.2025).

3. Конституція України: Закон України від 28.06.1996, №254к/96-ВР. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 16.05.2025).

4. Ярема О.Г., Лазар А.Я. Деякі аспекти обмеження інформаційних прав громадян в умовах воєнного стану. *Конституційні права і свободи людини та громадянина в умовах воєнного стану: матеріали наукового семінару* (23 червня 2022 р.). Львів: ЛьвДУВС, 2022. С. 295-298.

5. Про правовий режим воєнного стану: Закон України від 12.05.2015, №389-VIII. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення: 16.05.2025).

6. Постанова Верховного Суду від 14 лютого 2025 року у справі №420/20384/23. *Єдиний державний реєстр судових рішень.* URL: https://reyestr.court.gov.ua/Review/125173110 (дата звернення: 16.05.2025).

7. Антонюк У. В. Правові аспекти доступу до екологічної інформації в Україні в умовах воєнного стану. *Київський часопис права.* 2023. №1. С. 136-141.

Русанівський Сергій Віталійович,
здобувач кафедри криміналістики та судової медицини Національної академії внутрішніх справ

ПОЧАТКОВИЙ ЕТАП РОЗСЛІДУВАННЯ ПЕРЕВИЩЕННЯ ВЛАДИ АБО СЛУЖБОВИХ ПОВНОВАЖЕНЬ ПРАЦІВНИКОМ ПРАВООХОРОННОГО ОРГАНУ З ЗАСТОСУВАННЯМ ЗБРОЇ ЧИ СПЕЦІАЛЬНИХ ЗАСОБІВ ТА ЙОГО ЗНАЧЕННЯ ДЛЯ ПРИТЯГНЕННЯ ДО КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ

На початковому етапі розслідування важливо орієнтуватися в усіх обставинах події, яку потрібно дослідити. Це включає з’ясування фактів, які повинні бути досліджені, та отримання вихідних даних для планування розслідування. Також необхідно зібрати та зафіксувати докази, які можуть бути втрачені протягом короткого часу, а також встановити, знайти та затримати злочинця по гарячих слідах. На наступному етапі розслідування проводиться збирання, перевірка та оцінка доказів для повного встановлення всіх обставин кримінального провадження.

Основна спрямованість початкового етапу розслідування – інтенсивний пошук, виявлення і закріплення доказів шляхом проведення СРД [1]. На цьому

етапі розслідування важливо забезпечити якісний збір доказів та ідентифікацію підозрюваних у злочині, пов'язаному з незаконним поводженням зі зброєю та вибуховими речовинами. Слідчий повинен зосередитися на точному документуванні матеріальних слідів на місці події, що є ключовим для успішного розкриття справи. Важливо також визначити свідків, які можуть надати цінну інформацію, та призначити необхідні судові експертизи для підтвердження доказів.

Початковий етап розслідування включає організаційні заходи, такі як планування та висунення версій, а також вибір стратегії взаємодії з особами, які можуть сприяти розслідуванню. Процесуальні та організаційні рішення мають бути прийняті з урахуванням типових слідчих ситуацій та криміналістичних характеристик, що сприяють ефективному вирішенню завдань на цьому етапі.

Одним із ключових аспектів успішного розслідування кримінальних проваджень про перевищення влади або службових повноважень працівниками правоохоронних органів є своєчасність. Важливо, щоб ознаки можливого злочину були виявлені якомога швидше, що дозволяє негайно внести інформацію до ЄРДР. Це забезпечує оперативність і ефективність подальших слідчих дій, особливо у випадках застосування зброї чи спеціальних засобів.

Кримінальним процесуальним законодавством (ст. 91 КПК України) закріплено узагальнений перелік обставин, які підлягають доказуванню у кримінальному провадженні: 1) подія кримінального правопорушення (час, місце, спосіб та інші обставини вчинення кримінального правопорушення); 2) винуватість обвинуваченого у вчиненні кримінального правопорушення, форма вини, мотив і мета вчинення протиправного діяння; 3) вид і розмір шкоди, завданої кримінальним правопорушенням, а також розмір процесуальних витрат; 4) обставини, які впливають на ступінь тяжкості вчиненого кримінального правопорушення, характеризують особу обвинуваченого, обтяжують чи пом'якшують покарання, які виключають кримінальну відповідальність або є підставою закриття кримінального провадження; 5) обставини, що є підставою для звільнення від кримінальної відповідальності або покарання; 6) обставини, які підтверджують, що гроші, цінності та інше майно, які підлягають спеціальній конфіскації, одержані внаслідок вчинення кримінального правопорушення та/або є доходами від такого майна, або призначалися (використовувалися) для схиляння особи до вчинення кримінального правопорушення, фінансування та/або матеріального забезпечення кримінального правопорушення чи винагороди за його вчинення, або є предметом кримінального правопорушення, у тому числі пов'язаного з їх незаконним обігом, або підшукані, виготовлені, пристосовані або використані як засоби чи знаряддя вчинення кримінального правопорушення [2].

Розглядаючи питання щодо кримінальної відповідальності службової особи, А.Б. Балонь наголошує на врахуванні низки факторів, які допоможуть визначити ступінь її вини та можливі наслідки. Перш за все, важливо оцінити службовий статус особи, яка підозрюється у вчиненні злочину, оскільки це може

вплинути на кваліфікацію діяння. Не менш важливим є аналіз характеру, умов та особливостей роботи підприємства, установи або організації, де було вчинено злочин. Це дозволяє зрозуміти, наскільки дії службової особи були пов'язані з її професійними обов'язками і чи використовувала вона своє службове становище для досягнення злочинних цілей. Час і місце вчинення злочину також відіграють значну роль у розслідуванні, оскільки можуть свідчити про попередню підготовку або спонтанність дій. Важливо встановити причинний зв'язок між діями особи та шкідливими наслідками, що виникли внаслідок її дій або бездіяльності. Розмір заподіяної шкоди є ключовим фактором, який впливає на міру відповідальності. Форми вини, мотиви і мета злочину допомагають зрозуміти внутрішні спонукання особи, що може вплинути на рішення суду щодо покарання. Кількість злочинів, вчинених з використанням службових повноважень, може свідчити про систематичність або епізодичність протиправної поведінки. Також варто враховувати зв'язок з іншими злочинами або правопорушеннями, особливо якщо вони пов'язані з корупцією. Обтяжуючі або пом'якшуючі обставини можуть змінити характер покарання, а в деяких випадках навіть звільнити особу від кримінальної відповідальності. Останнім, але не менш важливим фактором є характеристика особи підозрюваного чи обвинуваченого, яка включає його соціальний статус, моральні якості та попереднє судове минуле. Врахування всіх цих аспектів дозволяє здійснити об'єктивний аналіз ситуації та прийняти справедливе рішення щодо кримінальної відповідальності службової особи [3].

Виходячи з положень ст. 91 КПК України, початок досудового розслідування перевищення влади або службових повноважень працівником правоохоронного органу з застосуванням зброї чи спеціальних засобів зумовлений особливим режимом досудового розслідування в умовах воєнного стану й переліком обставин, які підлягають встановленню, а саме: (1) загальними:

а) наявністю факту кримінального протиправного діяння передбаченого ч. 2 ст. 365 КК України;

б) способом вчинення, що пов'язаний із застосуванням зброї чи спеціальних засобів;

в) місцем і часом вчинення кримінального протиправного діяння;

г) особою злочинця – працівник правоохоронного органу, який явно перевищив межі наданих повноважень; наявність співучасників. Обставини, що характеризують особистість підозрюваного та його правовий статус, мають важливе значення в процесі розслідування кримінальних правопорушень, особливо коли вони вчинені працівниками правоохоронних органів у сфері їхньої службової діяльності. Слідчий або детектив повинен з'ясувати час і місце прийняття на службу та призначення на посаду підозрюваного, його службові права, обов'язки та функції, а також коло службових повноважень і їх співвідношення з фактичними діями, що містять ознаки кримінального

правопорушення. Важливо також врахувати освіту і кваліфікацію працівника, інформацію з особової справи, включаючи результати психологічних перевірок, а також відомості про фінансове та матеріальне становище підозрюваного і, за потреби, його близьких родичів;

д) незаконністю застосування зброї чи спеціальних засобів; мотивом і метою дій працівника правоохоронного органу;

є) сліди перевищення, застосування зброї чи спеціальних засобів;

е) наявність потерпілого та його дані;

ж) наслідками – вид і розмір шкоди, завданої протиправним діянням.

(2) спеціальними:

а) вид та кількість зброї чи спеціальних засобів, їх характерні ознаки;

б) відомості щодо спеціального статусу особи правопорушника – працівника правоохоронного органу й наявності дозволу на право володіння та користування зброєю.

Аналіз основних завдань, що вирішуються при розслідуванні кримінальних правопорушень, вчинених з використанням службової особи своїх повноважень, є важливим аспектом правозастосування. Ці завдання можна поділити на загальні та специфічні. Загальні завдання стосуються організації розслідування незалежно від його етапу. Вони включають висунення версій залежно від слідчої ситуації, планування розслідування, економічність його організації, забезпечення умов для застосування науково-технічних засобів, використання криміналістичних і інших обліків, а також чітко налагоджену взаємодію учасників розкриття і розслідування злочину. Специфічні завдання стосуються роботи за «гарячими слідами». Вони передбачають широке поєднання типового планування дій з індивідуальністю та конкретністю розслідування, невідкладне залучення всіх сил і засобів у роботу з розкриття злочину, чіткий вибір, високу оперативність запланованих слідчих (розшукових) дій, а також використання технічних засобів для досягнення максимальної повноти фіксації інформації при мінімальній витраті часу.

Важливо також відмітити, що нині актуальним є аналіз проблем, які виникають при правозастосуванні кримінального процесуального законодавства. Це стосується не тільки початку досудового розслідування, а й всього кримінального провадження в цілому. Особливу увагу слід приділити проблемам забезпечення діяльності органів досудового розслідування і шляхам їх вирішення. Це є одним із головних завдань кримінальної процесуальної політики держави, яка повинна враховувати консенсус між правами людини та інтересами держави для встановлення ефективного режиму правозастосування процесуальних норм.

Отже, основна спрямованість початкового етапу розслідування перевищення влади або службових повноважень працівником правоохоронного органу з застосуванням зброї чи спеціальних засобів спрямована на інтенсивний пошук, виявлення і закріплення доказів. Основними завданнями, що постають

перед слідчим на такому етапі є збір і фіксація, як матеріальних так і ідеальних слідів вчинення кримінального правопорушення.

Список використаних джерел

1. Щербаковський М.Г. Використання доказів як етап доказування у кримінальному провадженні. *Вісник Харківського національного університету внутрішніх справ*. 2017. Вип. 2. С. 88–95.

2. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

3. Балонь А.Б. Обставини, що підлягають встановленню за злочинами у сфері службової діяльності, пов'язаної з наданням публічних послуг. *Митна справа*. 2013. № 3. Ч. 2. Кн. 2. С. 55–60.

Сенюк Ольга Петрівна,
слухач навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ
Лапка Оксана Ярославівна,
доцент кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат юридичних наук, доцент

РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

У сучасному світі цифрові технології стали фундаментом функціонування не лише економіки та державного управління, а й усіх сфер суспільного життя. Вони забезпечують швидкий обмін інформацією, зручну комунікацію, дистанційне управління системами та сервісами. Проте у період воєнного стану роль цифрових технологій набуває подвійного значення: з одного боку, вони сприяють оперативному управлінню та координації, а з іншого — стають потенційною ціллю для кібератак, інформаційного впливу та деструктивного втручання.

Сучасні війни дедалі більше набувають гібридного характеру, і кібервиміри конфліктів стають одними з ключових інструментів тиску. Кіберзагрози здатні спричинити колапс критичної інфраструктури, завдати шкоди економіці, паралізувати державне управління та підірвати довіру населення до органів влади. У цьому контексті інформаційна безпека стає визначальним чинником національної стійкості, а цифрові технології — головним засобом її забезпечення [4].

Кіберзагрози під час воєнного стану мають системний характер. Злочинці і ворожі структури здійснюють атаки на державні інформаційні системи з метою

знищення або викривлення важливої інформації, доступу до стратегічних баз даних або поширення деструктивного контенту. Ці атаки спрямовані не лише на технічне порушення роботи об'єктів, а й на створення «інформаційного шуму», що ускладнює громадянам відокремлення правди від маніпуляцій [2, с. 42–49]. Це підриває довіру до державних інституцій, дестабілізує моральний стан громадян і послаблює суспільну єдність.

Найбільш вразливими до таких загроз є об'єкти критичної інфраструктури: енергетичні мережі, банківська система, транспорт, зв'язок, а також системи охорони здоров'я. Саме тому кіберзахист цих елементів має стати пріоритетом державної політики у сфері національної безпеки. До ключових заходів, що забезпечують ефективну протидію кіберзагрозам, належать: впровадження багаторівневої автентифікації, шифрування даних, автоматизовані системи виявлення атак (IDS/IPS), постійний аудит інформаційної безпеки, а також моніторинг інцидентів у режимі реального часу [1].

Агресивні кібердії противника становлять складну комбінацію інформаційного впливу та техногенного втручання. Їх метою є порушення комунікаційної цілісності суспільства, послаблення психологічної стійкості населення та посів недовіри до органів влади. Через цілеспрямоване поширення деструктивного контенту та фальсифікованих повідомлень, противник намагається розмити межу між правдою і вигадкою, що створює ефект «інформаційного шуму». Одночасно здійснюються втручання в роботу військових систем, урядових порталів, логістичних і банківських мереж з метою їхньої тимчасової нейтралізації або виведення з ладу. Ці дії не лише створюють технологічні ризики, а й провокують ланцюгову реакцію суспільної напруги, що в умовах воєнного стану набуває особливої ваги [4, с. 24].

Незважаючи на важливість цифрової безпеки, чинна правова база України у сфері кібербезпеки поки що залишається недостатньо адаптованою до швидко змінюваної природи кіберзагроз. Указ Президента України №447/2021 «Про Стратегію кібербезпеки України» визначає загальні напрями політики, однак у практичному вимірі органи влади часто діють в умовах нормативної невизначеності, що ускладнює своєчасне реагування на складні кіберінциденти [3].

На наш погляд, в умовах збройного конфлікту та після його завершення надзвичайно актуальним є питання відновлення цифрової інфраструктури. Доцільно виділити три ключові етапи цього процесу::

- 1-*й етап* – детальний аудит зруйнованих об'єктів, оцінка рівня пошкоджень та формування черговості відновлення, зокрема, у сферах енергетики, зв'язку та банківської інфраструктури;
- *2-й етап* – впровадження передових технологій захисту, включаючи штучний інтелект для автоматичного виявлення загроз, розширене шифрування, системи резервного збереження;
- *3-й етап* – підготовка кадрів і міжнародне співробітництво — створення кіберрезерву, залучення експертів, інтеграція досвіду партнерів і навчання фахівців для протидії майбутнім загрозам..

Важливим елементом інформаційної безпеки є також формування цифрової грамотності серед населення. Кожен користувач має розуміти базові принципи захисту персональних даних, способи розпізнавання фейкової інформації та шкідливих посилань. Без належної цифрової обізнаності навіть найсучасніші технічні системи можуть виявитися вразливими.

В умовах воєнного стану, коли боротьба відбувається не лише за території, а й за свідомість, саме цифрові технології визначають ефективність державного управління, сталість соціальної системи й перемогу в інформаційному просторі. Цифрова безпека – це не лише технічне завдання, а й стратегічна складова виживання держави у XXI столітті.

Список використаних джерел

1. Ковалів М.В., Єсімов С.С., Ярема О.Г. Інформаційне право України : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2022. 416 с.

2. Кудінов В.А., Яровий К.В. Комплексний підхід щодо створення стійких паролів інформаційних систем спеціального призначення МВС та Національної поліції України (частина 1). *Сучасна спеціальна техніка.* 2023. № 3 (74). С. 42-49.

3. Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серп. 2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

4. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. К.: Вид. НАВС, 2012. 104 с.

Уколов Олексій Леонідович,
аспірант Інститут держави і права імені В.М. Корецького НАН України

ЮРИДИЧНІ ФІКЦІЇ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ: МІЖ НЕОБХІДНІСТЮ ТА МАНІПУЛЯЦІЄЮ

Актуалізація проблематики інформаційної безпеки в умовах воєнного стану зумовила необхідність перегляду низки правових підходів до регулювання інформаційних відносин. Одним із таких підходів є використання юридичних фікцій – особливих правових конструкцій, що дозволяють створювати правову реальність, необхідну для захисту державних інтересів, незалежно від фактичного стану справ.

У загальній теорії права поняття юридичної фікції досліджували такі науковці, як А. Росс, Г. Радбрух, С. Алексі. Зокрема, А. Росс визначав юридичну фікцію як усвідомлену невідповідність між юридичними положеннями та реальними фактами, що, однак, визнається необхідною для ефективного

функціонування правопорядку [1, с. 23]. Густав Радбрух наголошував на тому, що фікції служать мостом між реальною дійсністю та нормативними вимогами права [2, с. 74].

У сфері інформаційної безпеки юридичні фікції в умовах воєнного стану проявляються через нормативне закріплення довіри до офіційної інформації, обмеження свободи вираження поглядів під гаслом захисту національної безпеки, а також через встановлення презумпцій шкідливості або небезпеки певних типів інформації. Наприклад, Закон України «Про правовий режим воєнного стану» передбачає можливість тимчасового обмеження діяльності засобів масової інформації з метою протидії дезінформації та інформаційним атакам.

Однак застосування юридичних фікцій у цій сфері має двоїсту природу. З одного боку, вони є інструментом оперативного реагування на інформаційні загрози та захисту громадян від психологічного впливу ворожої пропаганди. З іншого – юридичні фікції створюють передумови для маніпулювання суспільною свідомістю, що може призводити до порушення основоположних прав і свобод людини.

Проблему балансу між безпекою та правами людини у воєнний час розглядали такі українські дослідники, як О. Скакун і В. Нор. О. Скакун акцентує увагу на необхідності збереження принципу пропорційності обмежень прав людини навіть за умов надзвичайного стану [3, с. 89]. В. Нор підкреслює, що недотримання стандартів верховенства права навіть у кризових умовах може мати довгострокові негативні наслідки для легітимності державної влади [4, с. 105].

Практика свідчить, що надмірне використання юридичних фікцій у сфері інформаційної безпеки може мати низку серйозних негативних наслідків. Передусім це може призводити до легітимації цензури без належного судового контролю. В умовах воєнного стану обмеження на поширення інформації часто запроваджуються адміністративними рішеннями, без належних процедур перевірки їхньої законності та пропорційності, що суперечить принципам верховенства права.

Крім того, систематичне використання юридичних фікцій у сфері інформаційного забезпечення здатне спричинити формування у громадян хибної картини реальності. За відсутності доступу до альтернативних або незалежних джерел інформації суспільство може сприймати нав’язані наративи як об’єктивну істину, що ускладнює процес відновлення демократичних стандартів після завершення надзвичайного стану.

Ще одним наслідком є зниження рівня довіри до державних інститутів після завершення воєнного стану. У разі, якщо громадяни усвідомлять факт маніпуляції інформацією, це може призвести до глибокої кризи легітимності влади, що матиме довгострокові негативні наслідки для стабільності політичної системи та розвитку громадянського суспільства.

Відповідно до позицій С. Алексі, навіть в умовах загрози національній безпеці необхідно забезпечувати діалогову природу права, тобто залишати

можливість для відкритого обговорення правових рішень, нехай і в обмежених формах [5, с. 57].

Для мінімізації ризиків маніпулятивного використання юридичних фікцій у сфері інформаційної безпеки доцільно вживати низку превентивних заходів. Передусім важливо передбачити тимчасовий характер обмежувальних заходів із чіткими процедурами регулярного перегляду їхньої обґрунтованості. Такий підхід дозволить уникнути перетворення тимчасових надзвичайних заходів на постійну практику та забезпечить дотримання принципу пропорційності між обмеженнями прав і завданнями захисту національної безпеки.

Окрім цього, слід встановити незалежний контроль за застосуванням юридичних фікцій у сфері інформаційної безпеки. Ефективним механізмом такого контролю може бути створення спеціалізованих наглядових комісій або залучення уповноважених омбудсменів, які матимуть повноваження оцінювати законність і доцільність відповідних рішень органів державної влади.

Не менш важливо забезпечити громадянам доступ до альтернативних, верифікованих джерел інформації навіть під час дії воєнного стану. Наявність різноманітних перевірених каналів отримання інформації сприятиме збереженню критичного мислення в суспільстві, підвищенню стійкості громадської думки до інформаційних маніпуляцій та зменшенню ризиків виникнення дезорієнтації серед населення.

Таким чином, юридичні фікції виступають необхідним правовим інструментом у сфері забезпечення інформаційної безпеки в умовах воєнного стану, оскільки дозволяють оперативно реагувати на виклики, пов’язані з інформаційною агресією та загрозами державному суверенітету.

Водночас їх застосування потребує суворого дотримання принципів правової держави, верховенства права, об’єктивності та пропорційності. Юридичні фікції мають залишатися винятковим засобом правового регулювання, обмеженим часовими рамками надзвичайного стану та спрямованим виключно на захист національних інтересів без посягання на фундаментальні права і свободи людини. Недотримання цих вимог здатне призвести до небезпечної трансформації тимчасових обмежень у постійну практику пригнічення громадянських прав, що, у свою чергу, підриває демократичні засади суспільного розвитку та ставить під загрозу легітимність державної влади у посткризовий період.

Список використаних джерел

1. Ross A. On Law and Justice. Berkeley: University of California Press, 1959. 387 p.

2. Радбрух Г. Введення у філософію права. Львів: Видавництво УКУ, 2004. 126 с.

3. Скакун О.Ф. Теорія держави і права (енциклопедичний курс): підручник. Харків: Еспада, 2009. 520 с.

4. Нор В. Безпека інформаційного простору України: теоретико-правовий аналіз. Львів: ЛНУ ім. І. Франка, 2022. 312 с.

5. Алексі С. Теорія прав і правосуддя. Харків: Право, 2010. 294 с.

6. Закон України «Про правовий режим воєнного стану» від 12.05.2015 № 389-VIII.

7. Постанова Кабінету Міністрів України «Про деякі питання забезпечення інформаційної безпеки в умовах воєнного стану» від 18.03.2022 № 300.

Шапченко Іван Сергійович,
аспірант Інституту держави і права імені В.М. Корецького НАН України

РОЛЬ СУДОВОЇ ПРАВОТВОРЧОСТІ ПІД ЧАС ПЕРЕХІДНОГО ПРАВОСУДДЯ

Концепція перехідного правосуддя базується на ліберальній теорії прав людини і виникла як реакція на порушення загальних прав людини та гуманітарного права [1, с. 336]. Осмислення перехідного правосуддя неможливе без урахування глибшого контексту теорії прав людини та вивчення його елементів, таких як комісії правди та примирення, судові переслідування, інституційні та міжгалузеві реформи у сфері правосуддя відповідно до правових ідеалів, закладених у теорії справедливого суспільства [2, с. 13].

Втілення ідей зазначеної концепції можливе за умови розслідування та покарання винних у злочинах проти людства, покарання винних у скоєнні воєнних злочинів, забезпечення права знати правду про події минулого, надання відшкодування постраждалим, гарантії неповторення злочинів тощо.

Збройна агресія російської федерації проти України, поставила під серйозну загрозу суверенітет, територіальну цілісність і національну безпеку нашої держави. За таких умов Україна зіштовхнулася з недостатністю комплексних дій, спрямованих на стримування агресора, деокупації та реінтеграції тимчасово окупованих територій, що можливо досягти через перехідне правосуддя, застосування якого в українському контексті має не лише юридичне, а й глибоке суспільне та політичне значення, спрямоване на узагальнення світового досвіду, здобутого в ході постконфліктного врегулювання, практики забезпечення захисту прав жертв агресії, запровадження стандартів прав людини у період після завершення бойових дій, а також подолання безкарності за міжнародні злочини, створення стійких гарантій неповторення насильства, формування нової політичної та правової культури [3, с. 144].

В Концепції державної політики захисту та відновлення прав людини і основоположних свобод в умовах збройного конфлікту на території України та подолання його наслідків (концепція перехідного правосуддя) визначена основна мета, зміст якої полягає у створенні умов для дотримання, захисту та відновлення прав людини і основоположних свобод мешканців України в умовах триваючого збройного конфлікту з російською федерацією та подолання його наслідків в Україні [4]. Відповідно до цієї мети визначено також базові компоненти Концепції, а саме: відшкодування шкоди постраждалим від збройного конфлікту, притягнення винних до відповідальності та заходи із

запобігання безкарності, забезпечення права на правду про збройний конфлікт, заходи з недопущення виникнення збройного конфлікту в майбутньому.

В цілому політичні та правові трансформації в державі, які відбуваються після збройних конфліктів, війн, репресій тощо, обумовлюють становище судової влади, коли – з одного боку, вона повинна забезпечити дотримання і виконання чинного законодавства, а з іншого – відповісти на запит суспільства щодо справедливої відповідальності винних, відновлення справедливості та ін. У такому контексті, на нашу думку, судова правотворчість не лише доповнює перехідне правосуддя, а й стає його ключовим інструментом.

Так, у суспільствах, які проходять етап повоєнної відбудови або перебувають у процесі становлення демократії, верховенства права після повалення антидемократичного режиму, національне законодавство часто не містить норм, які закріплювали б загальні права людини, визначали покарання за порушення прав і свобод людини, гарантували неповторення злочинів минулого. У такому разі судді змушені інтерпретувати загальні положення конституції чи міжнародних договорів, усувати прогалини в законодавстві, використовувати прецеденти міжнародних трибуналів та рішення Європейського суду з прав людини.

Таким чином, судову правотворчість можна сприймати як важливий елемент у механізмі досягнення принципів та мети перехідного правосуддя, що в науковій юридичній літературі тлумачиться як набір правових та інституційних механізмів, які виникли після періоду конфлікту, громадянської війни, репресій тощо і які спрямовані на подолання наслідків порушення загальних прав людини і норм гуманітарного права, притягнення винних до відповідальності, гарантування прав постраждалим, встановлення історичної правди й запобігання повторенню подібного у майбутньому [5, с. 2; 3, с. 130].

Власне суди в перехідному правосудді здійснюють правову реконструкцію, визначаючи межі допустимості амністії (визнаючи неприпустимим амністію щодо злочинів проти людяності), інтерпретуючи поняття «жертва» враховуючи соціальний контекст (потреба соціальної реабілітації, компенсації), імплементуючи норми міжнародного гуманітарного права у національне законодавство, формуючи повагу до права та довіру до держави шляхом винесення обґрунтованих і справедливих рішень у справах, пов’язаних із воєнними злочинами, корупцією, політичними репресіями тощо.

Завдяки судовій правотворчості забезпечується можливість уніфікації практики перехідного правосуддя в державі та правової визначеності, зокрема шляхом єдиної інтерпретації права на відшкодування, встановлення критеріїв визнання політичних переслідувань, правової адаптації міжнародних стандартів доказування, стандартизації люстраційних процедур тощо. Все це сприяє легітимізації перехідного правосуддя всередині країни та інтеграції його до міжнародного права.

Отже, зазначене вище вказує на те, що судову правотворчість у контексті перехідного правосуддя, слід сприймати не тільки як реакцію на відсутність законодавства чи усунення прогалин в ньому, а як динамічний, концептуальний

процес, у якому суд сприймається як творець справедливості, «архітектор» демократичного режиму правової держави.

Список використаних джерел

1. Artur P. How ‘Transitions’ Reshaped Human Rights: A Conceptual History of Transitional Justice. *Human Rights Quarterly*. 2009. Vol. 31. № 2. P. 321-367.

2. Базове дослідження із застосування правосуддя перехідного періоду в Україні : монографія / за заг. ред. А.П. Бущенка, М.М. Гнатовського. Київ : "РУМЕС", 2017. 592 с.

3. Кориневич А., Короткий Т. Перехідне правосуддя для України: Per aspĕra ad astra. *Право України.* 2020. №12 С.129-149.

4. Концепція державної політики захисту та відновлення прав людини і основоположних свобод в умовах збройного конфлікту на території України та подолання його наслідків (концепція перехідного правосуддя). Підготовлена робочою групою з питань реінтеграції тимчасово окупованих територій Комісії з питань правової реформи при Президентові України URL : https://www.ppu.gov.ua/wp-content/uploads/2021/09/Conception.pdf

5. Transitional Justice in the Twenty-First Century: Beyond Truth versus Justice. 1st Edition / ed. by Naomi Roht-Arriaza, Javier Mariezcurrena. Cambridge University Press, 2006. 346 p.

Шип Володимир Володимирович,
курсант навально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ

ПРАВОВА ОСНОВА РЕФОРМУВАННЯ СЕКТОРУ БЕЗПЕКИ УКРАЇНИ

Реформування сектору безпеки України передбачає забезпечення прозорості та відкритості діяльності безпекових та оборонних інститутів для громадянського суспільства. Це необхідно для підвищення довіри населення до сектору безпеки, ефективного контролю з боку громадськості та запобігання неналежного врядування у зазначеній сфері.

В цілому діяльність, спрямована на покращення та зміцнення управління сектором безпеки, визначається як реформування сектору безпеки, що розуміється як безперервний політичний і технічний процес, за допомогою якого країна намагається покращити управління у безпековій сфері [1, с. 32].

Правову основу реформування сектору безпеки України становлять міжнародні нормативні акти як загальної, так і спеціальної дії, зокрема: Статут ООН, Загальна декларація прав людини, Конвенція Ради Європи про захист прав людини і основоположних свобод, Конвенція ООН про ліквідацію всіх форм расової дискримінації, Конвенція ООН про ліквідацію всіх форм дискримінації щодо жінок, Конвенція ООН проти катувань та інших жорстоких, нелюдських або таких, що принижують гідність, видів поводження і покарання, Паризькій

хартії для нової Європи, Брюссельська декларація про закони і звичаї війни, IV Конвенція про закони і звичаї війни на суходолі та додаток до неї: Положення про закони і звичаї війни на суходолі, Конвенція про права і обов'язки нейтральних держав і осіб у випадку сухопутної війни, Конвенція про бомбардування морськими силами під час війни, Женевські конвенції («Про поліпшення долі поранених і хворих у діючих арміях», «Про поліпшення долі поранених, хворих та осіб зі складу збройних сил, які потерпіли корабельну аварію на морі», «Про поводження з військовополоненими», «Про захист цивільного населення під час війни») та ін. [2, с. 536] На національному рівні нормативно-правовими актами, що містять правові засади реформування сектору безпеки є: Конституція України, Закон України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII», Укази Президента України від 14.09.2020 року № 392/2020 «Про Стратегію національної безпеки України», від 25.03.2021 № 121/2021 «Про Стратегію воєнної безпеки України», від 11.05.2023 № 273 «Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки» та ін. Зокрема, Указ Президента України «Про Комплексний стратегічний план реформування органів правопорядку на 2023–2027 роки» передбачає посилення демократичного цивільного контролю, підвищення прозорості та підзвітності органів безпеки, а також активне залучення громадянського суспільства до процесів реформування [3]. Аналогічно, Указ Президента України від 06.01.2025 №16/2025 «Про внесення змін до Стратегії національної безпеки України» вносить зміни до Стратегії національної безпеки України, акцентуючи увагу на інтегрованому управлінні державним кордоном та забезпеченні балансу між безпекою і відкритістю [4]. Згадані вище нормативно-правові акти відображають засади реформування сектору безпеки України, де ключовим є забезпечення національних інтересів, таких як суверенітет, територіальна цілісність, демократичний розвиток та європейська й євроатлантична інтеграція. У 2024 році Україна досягла повного фінансування сектору безпеки та оборони, що становило 38,9% очікуваного ВВП. Це дозволило забезпечити основні пріоритетні напрями діяльності в умовах воєнного стану [5].

Повага до суверенітету інших держав, боротьба з тероризмом, обмеження військових можливостей законними потребами оборони та забезпечення демократичного політичного контролю над збройними силами є основними принципами, що визначені Кодексом поведінки ОБСЄ стосовно військово-політичних аспектів безпеки [6]. Крім того, Рішення Ради міністрів МС 3/11 про елементи конфліктного циклу визнає роль громадянського суспільства у запобіганні та врегулюванні конфліктів та розбудові миру, зокрема шляхом підзвітності, участі, інклюзивності тощо [7].

Водночас, впровадження реформ стикається з регіональними викликами. Зокрема, спостерігається неефективне та нераціональне використання бюджетних коштів, а також недостатнє обґрунтування планування видатків з державного бюджету [5]. Регіональні особливості реалізації реформування сектору безпеки в Україні є важливим фактором, що впливає на його

ефективність та результативність. Врахування специфіки кожного регіону дозволяє адаптувати стратегії та підходи до місцевих умов, забезпечуючи таким чином більш ефективне впровадження реформ.

Воєнні дії на території України, що розпочалися після російської повномасштабної збройної агресії призвели до необхідності організації взаємодії місцевих рад з воєнними адміністраціями, реалізації державних функцій та стабілізації функціонування об'єктів критичної інфраструктури. Такі умови вимагають від місцевих органів влади високої мобільності, здатності до швидкого реагування та ефективної координації з центральними органами влади та військовими структурами [8]. В умовах війни спостерігається інтенсифікація діяльності сепаратистських, терористичних та екстремістських організацій, організованих злочинних угруповань, агентів впливу, спрямованих на дестабілізацію ситуації в окремих регіонах. Ці загрози вимагають від органів правопорядку та місцевих органів влади посиленої уваги до питань безпеки, оперативного реагування та ефективної координації дій.

Отже, реформування сектору безпеки України є складним процесом, сутністю якого слід вважати підвищення прозорості, ефективності та демократичного контролю з боку суспільства. Правовою основою цих змін є Конституція, закони України, укази Президента, а також міжнародні стандарти, що ратифіковані Верховною радою України.

Список використаних джерел

1. Управління та реформування сектору безпеки Рекомендації для співробітників ОБСЄ. Відень. 2022. 264 с. https://www.osce.org/files/f/documents/e/c/557760.pdf
2. Власенко В.П. Міжнародно-правові засади формування та реалізації державної воєнної політики. *Юридичний науковий електронний журнал*. 2024. С. 535-538.
3. Про комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки : Указ Президента України від 11 трав. 2023 р. № 273/2023. URL: https://zakononline.com.ua/documents/show/518213___742181
4. Про внесення змін до Стратегії національної безпеки України : Указ Президента України від 6 січ. 2025 р. № 16/2025. URL: https://www.president.gov.ua/documents/162025-53525
5. Підсумки 2024 року: сектор безпеки і оборони України профінансовано на 100%. Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/ua/Diialnist/7107.html
6. Code of Conduct, (1994). URL: https://www.scribd.com/document/563783148/CODE-OF-CONDUCT-1994
7. Decision No. 3/11 Elements of the Conflict Cycle, Related to Enhancing the OSCE's Capabilities in Early Warning, Early Action, Dialogue Facilitation and Mediation Support, and Post Conflict Rehabilitation, (2012). URL : https://www.osce.org/ministerial-councils/86621

8. Діордіца І.В. Актуальні питання забезпечення державної безпеки України крізь призму муніципальної та освітньої реформи у воєнний та післявоєнний час. *Юридичний науковий електронний журнал*. 2023. № 10. С. 340-343. URL : http://www.lsej.org.ua/index.php/arkhiv-nomeriv?id=167

Яковець Анастасія Юріївна,
курсант навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ
Лапка Оксана Ярославівна,
доцент кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат юридичних наук, доцент

ПРОТИДІЯ ДЕЗІНФОРМАЦІЇ ТА ФЕЙКОВИМ НОВИНАМ В УМОВАХ НАДЗВИЧАЙНИХ ПРАВОВИХ РЕЖИМІВ

Сучасне інформаційне середовище характеризується високою динамікою, доступністю комунікаційних технологій і надзвичайною вразливістю до зовнішніх та внутрішніх деструктивних впливів. В умовах гібридних загроз і повномасштабної війни проти України актуалізується проблема захисту інформаційного простору держави. Однією з найнебезпечніших форм інформаційного впливу є дезінформація та фейкові новини, які у період надзвичайних правових режимів стають засобом інформаційної війни, дестабілізації суспільства та підриву державного суверенітету.

У період надзвичайних правових режимів дезінформація є не просто спотворенням інформації, а свідомим впливом на масову свідомість, що має на меті розхитування суспільної стабільності, поширення паніки, зниження довіри до державних інституцій та легітимності органів влади. Вона виступає як складова гібридної агресії, що поєднує у собі інформаційно-психологічні, правові та технологічні загрози [1, с. 105]. Фейкові новини, як окремий вид дезінформації, виступають засобом маніпулювання масовою свідомістю, підриву довіри до органів державної влади та дестабілізації демократичних інституцій.

У правовому аспекті дезінформація розглядається як явище, що прямо порушує принципи відкритості, об’єктивності та достовірності інформації, закладені у Конституції України (ст. 34) та інших нормативно-правових актах [2].

Протидія дезінформації у період надзвичайного правового режиму може кваліфікуватися як посягання на національну безпеку, громадський порядок або права й свободи інших осіб, тому вона здійснюється та регулюється у певних напрямах:

➢ *нормативно-правове регулювання* – під час якого держава вводить спеціальні законодавчі обмеження (уточнення) щодо поширення інформації. Наприклад, у 2022 році до Кримінального кодексу України внесено зміни, що стосуються відповідальності за поширення неправдивої інформації про діяльність Збройних Сил України. Зокрема, стаття 114-2 передбачає кримінальне покарання за свідоме поширення фейкових відомостей, що можуть зашкодити обороноздатності держави [3].

➢ *адміністративно-примусові заходи* – характеризуються тим, що органи державної влади, в межах наданих повноважень, мають право вживати адміністративно-примусових заходів, зокрема: обмеження доступу до окремих вебресурсів, припинення діяльності засобів масової інформації, які поширюють недостовірну або деструктивну інформацію, а також притягнення винних осіб до адміністративної відповідальності. Так, наприклад, згідно зі статтею 173-1 Кодексу України про адміністративні правопорушення, громадяни, які свідомо поширюють неправдиві чутки, можуть бути притягнуті до відповідальності у формі штрафів або арешту [4].

➢ *інформаційна просвіта та контрпропаганда* – є одним із ключових напрямів протидії дезінформації в умовах надзвичайних правових режимів, направлена на формування критичного мислення громадян та підвищення рівня їхньої медіаграмотності [5, с. 13]. Це дозволяє населенню самостійно розпізнавати маніпулятивні повідомлення, фейкові новини й упереджену інформацію. Даний підхід сприяє запобіганню паніці й соціальній дестабілізації, які можуть виникати внаслідок поширення недостовірної інформації.

➢ *інституційна протидія* – важливу роль відіграють спеціалізовані органи державної влади. Зокрема:

– Центр протидії дезінформації при Раді національної безпеки та оборони України. Цей орган здійснює оперативний моніторинг інформаційного простору, виявлення фейків та їх публічне спростування. Центр також проводить просвітницькі кампанії, формує рекомендації для органів влади та взаємодіє з міжнародними партнерами у сфері інформаційної безпеки;

– Державна служба спеціального зв’язку та захисту інформації. Виконує функції у сфері кіберзахисту, охорони критичної інформаційної інфраструктури, виявлення кіберзагроз, пов’язаних із розповсюдженням дезінформації.

– Міністерство оборони, СБУ, Національна поліція. В умовах воєнного часу правоохоронні органи отримують розширені повноваження щодо виявлення, документування та запобігання деструктивним інформаційним впливам.

➢ *міжнародне співробітництво.* Україна активно співпрацює з міжнародними партнерами у сфері запровадження стандартів кібербезпеки, моніторингу дезінформації, обміну інформацією щодо інформаційних операцій, що мають ознаки ворожих впливів.

Підсумовуючи вищевикладене, можна сказати, що протидія дезінформації в умовах надзвичайних правових режимів є одним із пріоритетів державної політики у сфері національної безпеки. Вона охоплює комплекс заходів — від

кримінального та адміністративного переслідування до інституційного реагування, міжнародної співпраці та превентивної просвіти населення.

Забезпечення інформаційної безпеки потребує балансу між захистом національних інтересів і збереженням фундаментальних прав людини, включаючи свободу слова та доступ до правдивої інформації. Ефективна політика протидії фейкам має ґрунтуватися на принципах правової держави, відкритості та відповідальності.

Список використаних джерел

1. Рудник Л.І. Дезінформація як прояв порушення права на доступ до інформації. *Вісник Національної академії правових наук України. 2024. Т. 31, № 3. С. 103-118.* URL: https://visnyk.kh.ua/web/uploads/pdf/31(3)_2024-103-118.pdf (дата звернення 29.04.2025)

2. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення 29.04.2025)

3. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення 29.04.2025)

4. Кодекс України про адміністративні правопорушення: Закон України від 07.12.1984 р. № 80731-X. URL: https://zakon.rada.gov.ua/laws/show/80731-10#top (дата звернення 29.04.2025)

5. Інформаційна безпека держави: конспект лекцій. Чернігів: НУ «Чернігівська політехніка», 2022. 133 с.

ДЛЯ НОТАТОК

Наукове видання

ІНФОРМАЦІЙНА БЕЗПЕКА СУСПІЛЬСТВА В УМОВАХ ДІЇ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ ТА ПОВОЄННИЙ ПЕРІОД

Збірник матеріалів
Міжвідомчого науково-практичного круглого столу
(Київ, 29 травня 2025 року)