

УДК 351.746.1:007

*Сікорський Олександр Петрович,
кандидат юридичних наук,
доцент кафедри адміністративного та
конституційного права
факультету морського права,
НУК ім. адмірала Макарова
alex.nic.gmail.com*

*Гілецький Максим Вікторович,
студент магістратури
НУК ім. адмірала Макарова
gileckii@gmail.com*

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО МЕХАНІЗМУ РЕАЛІЗАЦІЇ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Одним із ключових секторів національної безпеки будь-якої держави, є інформаційна безпека. Послідовна реалізація чітко сформульованої національної інформаційної стратегії, дозволяє забезпечувати безпеку у політичній, військовій, соціальній, економічній та інших сферах діяльності держави. Стрімкий розвиток інформаційно-комунікативних технологій та швидка глобальна інформатизація населення призвели до появи нових загроз національній безпеці держави. Проведення інформаційно-психологічних операцій спрямованих на ліквідацію суверенітету чи обмеження незалежності держави, для України є не гіпотетичною, а реальною загрозою. Одними із ключових напрямків протидії та мінімізації інформаційно-психологічного впливу, є створення сучасної та ефективної нормативно-правової бази функціонування системи інформаційної безпеки, а також вироблення ефективного механізму її реалізації.

Ключові слова: інформаційна безпека, адміністративно-правовий механізм, національна безпека, інформаційно-психологічні операції, кібербезпека.

Sikorsky O., Giletsky M. MODERN STATUS AND PROSPECTS OF IMPROVING THE ADMINISTRATIVE AND LEGAL MECHANISM OF IMPLEMENTING THE POLICY OF INFORMATION SECURITY OF UKRAINE

Information security is one of the key sectors in national security of any state. The consistent implementation of a well-formulated national information strategy allows to provide security in the political, military, social, economic and other spheres of state activity. The rapid development of information and communication technologies and the rapid global informatization among people have led to new threats in the national security of the state. Conducting information-psychological operations aimed at eliminating sovereignty or limiting the independence of the state is not hypothetical but a real threat for Ukraine. One of the key areas of counteraction and minimization of information and psychological influence is the creation of a modern and effective legal base for the functioning of the information security system, as well as the development of an effective mechanism for its implementation.

Key words: information security, administrative and legal mechanism, national security, information-psychological operations, cyber security.

Постановка проблеми. Проблема формування єдиного інформаційного простору країни, а також активного протистояння впливу зовнішніх чинників, постала в Україні досить давно, однак найгостріше вона проявилась після трагічних подій 2014 року. Лише після прийняття ряду нормативних актів, які дозволили виробити єдиний підхід до розуміння вирішення проблеми, почались масштабні зрушення у реформуванні секторів безпеки держави, у тому числі інформаційного. Однак, незважаючи на вже наявні напрацювання у даній сфері, механізм реалізації політики інформаційної безпеки, є недостатньо ефективним.

Аналіз останніх досліджень і публікацій. Дослідженням питання механізму адміністративно-правового регулювання політики інформаційної безпеки займалось багато вчених-адміністративістів, зокрема: О. Бандурка, Ю. Битяк, С. Алексеев, О. Скакун, В. Галуцько, В. Корельський, Р. Калюжний, Л. Коваль, В. Колпаков, С. Додіна, В. Котюк, В. Перевалов, В. Селіванов та ін. Проте, незважаючи на достатньо об'ємну кількість матеріалів досліджень, питання щодо чіткого визначення механізму адміністративно-правового регулювання та його

структурних елементів не вирішено, а також залишається поза увагою механізм адміністративно-правового регулювання у сфері реалізації політики інформаційної безпеки.

Формулювання цілей статті. Метою статті є загальний аналіз механізму реалізації політики інформаційної безпеки України, як ключової складової функціонування системи національної безпеки нашої держави

Виклад основного матеріалу. Пріоритетними напрямками державної політики будь-якої держави, є збереження суверенітету, незалежності, територіальної цілісності та недоторканості кордонів. Україна, як суверенна та незалежна держава, також не є виключенням. Однак, у 2014 році, Україна вперше в історії своєї незалежності, зіткнулась із новим методом ведення бойових дій – так званою «Гібридною війною». Внаслідок цього, було викрито значні прорахунки вищого політичного та військового керівництва. Так, у державі була частково або повністю відсутня нормативна база для надання оперативної та адекватної відповіді на дії агресора.

Гібридну війну у загальному вигляді розуміють як воєнні дії, що здійснюються шляхом поєднання мілітарних, квазімілітарних, дипломатичних, інформаційних, економічних та інших засобів з метою досягнення стратегічних політичних цілей. Специфіка такого поєднання полягає в тому, що кожний із військових і невійськових способів ведення гібридного конфлікту застосовується у воєнних цілях та використовується як зброя [1, с. 19-20].

З наведеного вище визначення, можна дійти висновку, що невід'ємною складовою такої війни є інформація та способи її використання. Відповідно до Закону України «Про інформацію», *інформація* – це сукупність відомостей про матеріальний і духовний світ, про закономірності й тенденції його розвитку, які можна відтворювати шляхом передачі усним, письмовим або електронним способом [2].

Закон України «Про інформацію», встановлює також принципи державної інформаційної політики, одним з яких є забезпечення інформаційної безпеки України. Однак значний час даний принцип реалізовувався лише формально і лише після безпосереднього початку бойових дій, проблема інформаційної безпеки стала однією з найактуальніших.

Однією з основних причин актуалізації даної проблеми саме у контексті збройного конфлікту, є проведення т.зв. «спеціальних інформаційних операцій» або «інформаційно-психологічних операцій (ІПО)».

Психологічні операції (англ. PSYOP) — комплекс заходів, що передбачає передачу вибраної інформації аудиторії для впливу на емоційний стан і спосіб мислення, а через неї опосередковано на поведінку та рішення урядів, груп чи лідерів. Вони мають ґрунтуватися на реальності, меседжі повинні узгоджуватися між собою, а конструйована «реальність» має бути так чи інакше прийнятною для будь-якої аудиторії. [3].

Історія проведення психологічних операцій сягає своїм корінням час становлення людства та перших битв між людьми. Найбільш масштабний в історії комплекс заходів інформаційно-психологічного впливу (ІПВ) був здійснений за часів «холодної війни». Як писав у 1946 р. один із «архітекторів» американської зовнішньої політики, директор ЦРУ (1953-1961) А. Ф. Даллес, «людський мозок, свідомість людей здатні змінюватися. Посіявши хаос, ми непомітно підмінимо їхні цінності на облудні та змусимо їх вірити у фальшиві цінності. Як? Ми знайдемо своїх однодумців, союзників у самій Росії, Україні, Білорусії, Прибалтиці, Закавказзі, Середній Азії і далі – скрізь» [4, с. 232-233].

Аналіз воєнно-політичної обстановки в Автономній Республіці Крим (далі – АРК) та на південному сході України показав, що проти нашої країни та її Збройних Сил з боку Російської Федерації активно проводяться інформаційно-психологічні операції (ІПО), які складають єдину систему операцій зі взаємопов'язаними цілями, спрямованими на [5]:

- підтримку політичних і воєнних рішень керівництва Російської Федерації на міжнародному рівні, з боку населення РФ та підконтрольних російській владі територій;
- нівелювання та викривлення рішень воєнно-політичного керівництва України, порушення діяльності органів військового управління;
- зниження морально-психологічного стану особового складу Збройних Сил та інших силових структур України;
- деморалізацію населення України.

На думку Г. В. Певцова, для досягнення визначених цілей застосовується майже повний спектр каналів комунікацій – традиційні та електронні засоби масової інформації. Найактивніше використовуються телебачення, Інтернет і соціальні мережі. При цьому застосовуються всі методи інформаційно-психологічної боротьби – від представлення тенденційної інформації та напівправди до неприхованої неправди («фейку») [5].

Квола відповідь України на агресивну політику Росії на початку 2014 р. стала «моментом істини», який засвідчив системну кризу національного сектору безпеки і оборони та показав необхідність негайного здійснення масштабних реформ у цій сфері. Перед Україною постало надскладне завдання – проводити швидкі реформи у секторі безпеки і оборони в умовах протидії широкомасштабній російській агресії. Аналогічний процес у західних країн, навіть за умов мирного часу, не був швидким і тривав роками [1, с. 23-24].

З метою вирішення даного питання на законодавчому рівні протягом 2015-2017 рр. було прийнято ряд нормативних актів, які заклали базові підвалини для реформування системи національної безпеки та створення системи інформаційної безпеки держави.

У травні 2015 року була прийнята Стратегія національної безпеки України. Основним завданням даного документу, стала заміна застарілої Стратегії національної безпеки України «Україна у світі, що змінюється». Стратегія національної безпеки України затверджена Указом Президента України від 26 травня 2015 року № 287/2015 визначає сучасні актуальні виклики національній безпеці України та кроки по ліквідації чи мінімізації таких викликів [6].

Крім основних секторів безпеки та оборони, потребував реформування інформаційний сектор безпеки України.

Прорахунки у системі інформаційної безпеки стали одними з основних, які дозволили північному сусіду налаштувати населення однієї частини суверенної сусідньої держави проти іншого, що в свою чергу дозволило анексувати частину території останньої та створити вогнище напруженості на її території.

З метою урегулювання сфери інформаційної безпеки та можливості вчасного реагування та не допущення чи мінімізування проведення ППО на території країни, була прийнята Доктрина інформаційної безпеки України.

Указом Президента України від 25 лютого 2017 року № 47/2017 введено в дію Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Доктрина інформаційної безпеки України визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері [7].

Для реалізації будь-якого нормативного акту необхідна розробка і впровадження дієвого механізму його реалізації. Під поняттям «механізм правового регулювання» слід розуміти сукупність правових засобів, форм та способів, за допомогою яких забезпечується задоволення інтересів суб'єктів права, впорядкування суспільних відносин, встановлення правопорядку в суспільстві, вирішення конфліктів, досягнення соціального компромісу в правовій сфері [8; с. 373-374].

Ключову роль у реалізації правового регулювання суспільних відносин у сфері адміністративного права займає явище, яке в юридичній науці, теорії права та адміністративному праві носить назву механізму адміністративно-правового регулювання.

На думку низки вітчизняних науковців В. Галунька, В. Олефіра, М. Пихтіна та інших, механізм адміністративно-правового регулювання – це засоби функціонування єдиної системи адміністративно-правового регулювання з метою забезпечення прав, свобод та публічних законних інтересів фізичних та юридичних осіб, нормального функціонування громадянського суспільства і держави. До складових елементів механізму адміністративно-правового регулювання відноситься [9; с. 87-90]:

- 1) норми адміністративного права та їх зовнішнє вираження - джерела права;
- 2) публічна адміністрація;
- 3) принципи діяльності публічної адміністрації;
- 4) індивідуальні акти публічної адміністрації;
- 5) адміністративно-правові відносини та ін..

Первинним елементом правового регулювання є норма права. Адміністративно-правова норма – це загальнообов'язкове правило поведінки, що встановлене державою з метою регулювання суспільних відносин у сфері діяльності публічної адміністрації і забезпечується заходами державного примусу [9, с.12-13].

Досить важливим моментом є те, що потреба здійснення ефективного регулювання політики інформаційної безпеки, вимагає від публічної адміністрації встановлення норм права підзаконного характеру. Це викликане тим, що загальні норми і правила поведінки, сформульовані у законах, не в змозі охопити всі аспекти адміністративно-правового забезпечення політики інформаційної безпеки, врегулювати її в усіх подробицях, тому і виникає необхідність конкретизації та деталізації законодавчих норм до стадії їх застосування. В юридичній літературі є загально визнаним, що основна формула структури адміністративно-правових відносин складається із суб'єктів публічної адміністрації, юридичних фактів та об'єктів охоронного впливу [10, с.94-95].

Виникненню, зміні чи припиненню правовідносин передують юридичні факти, під якими в теорії права розуміються різного роду дії та події, які називають життєвими обставинами. Ці обставини вказуються в гіпотезах правових норм, і коли вони виникають у реальному житті, це призводить до того, що у визначених суб'єктів або з'являються взаємні права й обов'язки, тобто виникають правовідносини; або відбувається зміна цих правовідносин (обсягу чи змісту зазначених прав і обов'язків, складу суб'єктів); або правовідносини припиняються – зазначені права й обов'язки зникають. Залежно від породжуваних ними наслідків юридичні факти можуть бути класифіковані на правоутворюючі, правозмінюючі і правоприпиняючі [11].

Третім основним елементом механізму адміністративно-правового регулювання у сфері адміністративно-правового регулювання інформаційної безпеки України є акти реалізації прав та обов'язків суб'єктів.

В науковій літературі поняття «акт» застосовується у двох значеннях. По-перше, як дія, вчинок громадянина або посадової (службової) особи, по-друге, як документ, який видається державним органом, органом місцевого самоврядування, посадовою особою або громадською організацією у межах їх компетенції: закон, указ, постанова, наказ, розпорядження тощо. Слід погодитись з думкою О.Ф. Скакун, яка розуміє під актами реалізації прав та обов'язків фактичну поведінку суб'єктів правовідносин, пов'язану зі здійсненням (реалізацією) своїх прав та

обов'язків [8, с.501].

Реалізація прав та обов'язків суб'єктів державної політики у сфері інформаційної безпеки здійснюється через наступні форми:

- виконання норм права;
- використання норм права;
- дотримання норм права.

Існуючий механізм реалізації нормативних актів, передбачає наступні елементи: 1) визначення чіткого переліку об'єктів, на які спрямовано вплив реалізації політики інформаційної безпеки; 2) визначення чіткого кола суб'єктів уповноважених на здійснення політики інформаційної безпеки України; 3) визначення повноважень суб'єктів у сфері реалізації політики у даній сфері

Разом з тим, стрімкий розвиток інформаційно-комунікаційних технологій, а також засобів та методів проведення інформаційно-психологічного впливу на широкі верстви населення, призводить до швидкого застаріння нормативної бази у сфері інформаційної безпеки держави. Саме тому, задля своєчасного попередження виникнення нових загроз і протидії існуючому впливу, першочерговим завданням держави, у сфері національної та інформаційної безпеки – є оновлення нормативної бази у цих сферах та створення дієвого адміністративно-правового механізму реалізації політики інформаційної безпеки України.

Список використаних джерел:

1. Горбулін В.П. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. К. : НІСД, 2017. 496 с.
2. Плескач В. Л. Інформаційні системи і технології на підприємствах : підручник / В. Л. Плескач, Т. Г. Затонацька. К.: Знання, 2011. 718 с.
3. Сили спеціальних операцій Збройних сил України. URL: <https://ukrsof.com/psyopsukr/> – Назва з екрана.
4. Остроухой Б. В., Петрик Б. М.. Інформаційна безпека (соціально-правові аспекти): Підручник / Остроухой Б. В., Петрик Б. М., Присяжнюк М. М. та ін. ; за заг- ред. Є. Д. Скулиша. К: КНТ, 2010. 776 с.
5. Певцов Г. В. Інформаційно-психологічні операції Російської Федерації в Україні: моделі впливу та напрями протидії. *Наука і оборона*. - 2015. № 2. С. 28-32.
6. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»» від 26 травня 2015 року № 287/2015 URL: <http://zakon3.rada.gov.ua/laws/show/287/2015>.
7. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»» від 25 лютого 2017 року № 47/2017. URL: <http://zakon3.rada.gov.ua/laws/show/47/2017>.
8. Скакун О.Ф. Теорія держави і права: Підручник / Пер. з рос. Х.: Консум, 2001. 656 с.
9. Галуцько В. В. Теорія держави і права: курс лекцій: навч. посіб. / [авт.-упоряд. В. В. Галуцько, Г. О. Пономаренко, В. К. Шкарупа]; за ред. В. К. Шкарупи. Херсон : Вид-во ВАТ ХМД, 2008. 280 с.
10. Гончарук С. Т. Адміністративне право України. Загальна та Особлива частини : навч. посіб. К. : НАВС, 2000. 240 с.
11. Валькова Є. В. Зміст та структура механізму адміністративно-правового регулювання у сфері охорони права інтелектуальної власності. *Форум права*, 2012. № 3. С. 84-88.

REFERENCES

1. Horbulin V.P. (2017). *Svitova hibrydna viina: ukraïnskyi front: monohrafiia [World hybrid war: Ukrainian front: monograph]*. K. : NISD [in Ukrainian].
2. Pleskach V. L. (2011). *Informatsiini systemy i tekhnologii na pidpriemstvakh [Information systems and technologies at the enterprises]*. K.: Znannia [in Ukrainian].
3. Syly spetsialnykh operatsii Zbroinykh syl Ukrainy [Special Operations Forces of the Armed Forces of Ukraine]. Retrieved from <https://ukrsof.com/psyopsukr/> [in Ukrainian].
4. Ostroukhoi B. V., Petryk B. M. (2010). *Informatsiina bezpeka (sotsialno-pravovi aspekty) [Information security (socio-legal aspects)]*. K: KNT [in Ukrainian].
5. Pievtsov H. V. (2015). Informatsiino-psykholohichni operatsii Rosiiskoi Federatsii v Ukraini: modeli vplyvu ta napriamy protyidii [Information-psychological operations of the Russian Federation in Ukraine: models of influence and directions of counteraction]. *Nauka i oborona – Science and defense*, 2, 28-32 [in Ukrainian].
6. Ukaz Prezydenta Ukrainy «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 6 travnia 2015 roku «Pro Stratehiiu natsionalnoi bezpeky Ukrainy»» vid 26 travnia 2015 roku № 287/2015 [Decree of the President of Ukraine "On the decision of the National Security and Defense Council of Ukraine dated May 6, 2015" On the Strategy of National Security of Ukraine "" dated May 26, 2015 No. 287/2015]. (n.d.). *zakon.rada.gov.ua*. Retrieved from <http://zakon3.rada.gov.ua/laws/show/287/2015>. [in Ukrainian].
7. Ukaz Prezydenta Ukrainy «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy»» vid 25 liutoho 2017 roku № 47/2017 [Decree of the President of

Ukraine "On the decision of the Council of National Security and Defense of Ukraine dated December 29, 2016" On the Doctrine of Information Security of Ukraine "" dated February 25, 2017, No. 47/2017]. (n.d.). zakon.rada.gov.ua. Retrieved from <http://zakon3.rada.gov.ua/laws/show/47/2017>. [in Ukrainian].

8. Skakun O.F. (2001). *Teoriia derzhavy i prava [Theory of state and law]*. Kh. : Konsum [in Ukrainian].

9. Halunko V. V. (2008). *Teoriia derzhavy i prava: kurs lektsii [Theory of state and law: a course of lectures]*. Kherson : Vyd-vo VAT KhMD [in Ukrainian].

10. Honcharuk S. T. (2000). *Administrativne pravo Ukrainy. Zahalna ta Osoblyva chastyny [Administrative Law of Ukraine. General and Special Parts]*. K.: NAVS [in Ukrainian].

11. Valkova Ye. V. (2012). Zmist ta struktura mekhanizmu administratyvno-pravovoho rehuliuвання u sferi okhorony prava intelektualnoi vlasnosti [Content and structure of the mechanism of administrative and legal regulation in the field of intellectual property rights protection]. *Forum prava – Forum of Law*, 3, 84-88 [in Ukrainian].

Стаття надійшла до редакції 20.09.2018

УДК 351.746:007

Сікорський Олександр Петрович,
кандидат юридичних наук,
доцент кафедри адміністративного та
конституційного права
факультету морського права,
НУК ім. адмірала Макарова
alex.nic@gmail.com

Якобчук Микола Юрійович
студент магістратури
НУК ім. адмірала Макарова
alex.nic@gmail.com

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ВІЙНИ: ФОРМИ ТА МЕТОДИ

Стаття присвячена дослідженню сучасного стану розвитку форм та методів ведення інформаційно-психологічних війн, застосування гібридних засобів протистояння, а також аналізується місце України у сучасних інформаційно-психологічних війнах.

Наслідки інформаційно-психологічних війн, які відчуває міжнародна спільнота, у тому числі й Україна, на сьогодні зумовлюють потребу у постійному поглибленому вивченні як теоретичних, так і практичних знань у цій сфері.

Детальний аналіз питань форм та методів проведення інформаційно-психологічних війн має під собою і практичну складову – напрацювання ефективних засобів протидії інформаційно-психологічним загрозам.

Ключові слова: інформаційно-психологічні війни, форми та методи інформаційно-психологічних війн.

Sikorsky O., Yakobchuk M. INFORMATIONAL AND PSYCHOLOGICAL WAR: FORMS AND METHODS

The article is devoted to the research of the current state of the development of forms and methods of conducting information-psychological wars, the use of hybrid means of confrontation, and also analyzes the place of Ukraine in modern information-psychological wars.

The consequences of the information-psychological wars felt by the international community, including Ukraine, today predetermine the need for continuous in-depth study of both theoretical and practical knowledge in this field.

A detailed analysis of the issues of the forms and methods of conducting information-psychological wars has a practical component - the development of effective means of counteracting information and psychological threats.

Key words: information-psychological wars, forms and methods of information-psychological wars.

Постановка проблеми. Формування інформаційного суспільства, зумовлює системні зміни фактично в усіх сферах. Питання інформаційного обміну, взаємини у сфері інформації мають різні сторони. На жаль, людство у ХХІ столітті зіткнулося ще з однією проблемою, яку прийнято називати інформаційно-психологічні війни. Предмет цієї проблематики надзвичайно широкий і наразі потребує ґрунтовних досліджень. Одним із аспектів