УДК/UDC: 351.746.316
DOI: https://doi.org/10.37750/2616-6798.2026.2(57).364412

Микола Андрійович Дмитренко
Національна академія Служби безпеки України
Київ, Україна
ORCID: https://orcid.org/0000-0001-5262-1210

СИСТЕМНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Анотація. *У статті досліджується сучасний стан інституційного забезпечення інформаційної безпеки України в умовах здійснення російськими спецслужбами високо динамічних інформаційних кампаній в інформаційному просторі України, які стали загрозою не лише інформаційній, але й національній безпеці держави.*

Здійснено аналіз нормативно-правових актів з питань державної інформаційної політики щодо системи забезпечення інформаційної безпеки. Зокрема, в контексті антиукраїнської інформаційної кампанії, яка функціонально реалізується російською стороною за низкою напрямків, таких як: забезпечення постійного потоку маніпулятивної дезінформації про події в Україні та на окупованих територіях; внесення розколу в середовище українських політичних та військових еліт, серед іншого й шляхом публікації провокаційних та деструктивних матеріалів, критики центральної влади, компрометації громадсько-політичних діячів, інспірації масових протестів тощо; намагань російських спецслужб вплинути на політичні та соціально-економічні процеси в державі через спеціальні заходи впливу, підірвати авторитет української влади з метою деморалізації суспільства та посилення невдоволення і протестних настроїв.

Проаналізовано системні проблеми інформаційної безпеки держави, які в нинішніх умовах негативно впливають на стан політичної, економічної, оборонної та інших складових національної безпеки України, оскільки найчастіше реалізація інформаційних загроз - це завдання шкоди в усіх сферах національної безпеки. Особливу увагу приділено спеціальним заходам впливу, як ключовому елементу інформаційної безпеки в умовах інформаційного протиборства, а також ризикам спеціальних та інформаційно-психологічних операцій.

Надано пропозиції щодо розроблення цілісної гнучкої динамічної державної системи у сфері забезпечення інформаційної безпеки, яка враховуватиме багатоаспектність цього явища.

Ключові слова: *державна інформаційна політика, інформаційна безпека, система інформаційної безпеки, інформаційне протиборство, спеціальні заходи впливу, спеціальні інформаційні операції.*

Mykola A. Dmytrenko
National Academy of the Security Service of Ukraine
Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-5262-1210

SYSTEMIC PROBLEMS OF ENSURING UKRAINE'S INFORMATION SECURITY

Summary. *The article explores the current state of the institutional framework for Ukraine's information security amid highly dynamic information campaigns carried out by Russian intelligence services. These campaigns involve controlled mass communication tools within Ukraine's information space, posing a threat not only to informational security but also to the national security of Ukraine.*

An analysis of regulatory and legal acts on state information policy regarding the information security system has been conducted. Specifically, this is examined in the context of the anti-Ukrainian information campaign functionally implemented by the Russian side across several directions, such as: ensuring a constant flow of manipulative disinformation about events in Ukraine and its occupied territories; creating divisions among Ukrainian political and military elites, including through the publication of provocative and destructive materials, criticism of the central government, compromising public and political figures, and inspiring mass protests; and attempts by Russian intelligence services to influence political and socio-economic processes in our state, undermining the authority of the Ukrainian government to demoralize society and amplify discontent and protest sentiments.

The article analyzes systemic problems of state information security which, under current conditions, negatively impact the political, economic, defense, and other components of Ukraine's national security, as the realization of information threats most often results in damage across all spheres of national security.

Proposals are provided for the development of a comprehensive, flexible, and dynamic state system in the field of information security that accounts for the multidimensional nature of the information security phenomenon.

Keywords: *information political, information security, information influence, informational psychological influence, information-psychological operation, information confrontation.*

Постановка проблеми. Активне проникнення інформатизації в усі сфери життєво важливих інтересів особистості, суспільства і держави спричинило те, що нині дедалі більшої актуальності набуває завдання забезпечення інформаційної безпеки України як невід'ємного елементу її національної безпеки, а захист інформації стає одним із пріоритетних державних завдань. Інформаційна безпека відіграє одну з провідних ролей у забезпеченні життєво важливих інтересів країни. Оскільки контроль над інформаційною інфраструктурою дає підстави для формування суспільної думки, яка завжди спочатку виявляється в певних переконаннях, а вже потім у конкретних діях. Тож в умовах конкурентної боротьби контроль над інформаційною сферою перетворюється на один із основних ресурсів влади.

На сьогодні загрози інформаційній безпеці мають соціальний характер і зосереджені у внутрішньополітичній, економічній, соціальній, екологічній, інформаційній та духовній сферах суспільства. Актуальність дослідження зумовлена потребою удосконалення системи інформаційної безпеки та внесення відповідних змін до нормативно-правових актів з питань державної інформаційної політики в інформаційній сфері. Особлива роль інформаційної безпеки нині набуває вирішального значення в розробці заходів у зовнішньополітичній сфері для: *удосконалення* інформаційного супроводу державної політики, діяльності українських громадських

організацій та суб'єктів підприємницької діяльності за кордоном; організаційно-технічного, інформаційного та ресурсного *сприяння* держави вітчизняним засобам масової інформації, що формують у світовому інформаційному просторі позитивний імідж України; *гарантування* своєчасного виявлення зовнішніх загроз національному інформаційному суверенітету та їхньої нейтралізації тощо.

Результати аналізу наукових публікацій. Вирішенням проблем забезпечення інформаційної безпеки займалися низка українських вчених і дослідників, Певною мірою проблеми інформаційної безпеки розкриваються у наукових працях, зокрема: В. Бебика, О. Ворони, В. Горбуліна, К. Захаренка, О. Золотар, О. Литвиненка, Є. Макаренко, В. Остроухова, В. Пантелєєва, І. Партоленко, А. Поляруша Г. Почепцова. Т. Савченко, В. Сідака, Є. Скулиша, Л. Смоли, Ю. Шевченко, та багатьох інших науковців. У працях авторів детально проаналізовано методи, форми, засоби інформаційного протиборства та здійснення інформаційних впливів. Однак, сьогодення потребує комплексного дослідження проблем забезпечення інформаційної безпеки, що виникають у процесі протидії воєнній агресії з боку РФ та напрямків їх вирішення, між іншим і з використанням спеціальних сил та засобів.

Метою статті є аналіз системи забезпечення інформаційної безпеки та осмислення проблем інформаційної політики держави для вироблення пропозицій щодо підвищення ефективності протидії заходам впливу в умовах війни, а також організації ефективної системи забезпечення інформаційної безпеки держави.

Виклад основного матеріалу. Україна нині функціонує в умовах надзвичайної ситуації: - повномасштабна війна, кризові явища у сферах економіки, культури, політики, ідеології, в соціальній сфері та сфері управління тощо. Донині на жаль, в протидії спеціальним інформаційним операціям розглядається скоріше технічна сторона, а психологічна здебільшого залишається поза увагою. Це призводить до посилення інформаційної агресії з боку РФ, яка використовує для просування своїх інтересів суспільно-політичну ситуацію в нашій державі та наявні проблеми інформаційної безпеки України. Відкритість національного інформаційного простору в соціальних мережах та Інтернет створює реальну загрозу негативного інформаційно-психологічного впливу на користувачів Інтернету, якими є переважно молодь та освічені люди з активною життєвою позицією, що становить особливу суспільну небезпеку. Безконтрольність електронних засобів масової інформації та соціальних мереж використовуються як майданчик для вербування українців до агентурних мереж, збройних формувань, терористичних організацій тощо, Слід також враховувати, що в українському суспільстві існує низка міжрегіональних, міжетнічних, міжрелігійних розбіжностей, різна шкала цінностей і пріоритетів, а тому складно говорити про єдність інформаційного простору та спільність ціннісних орієнтацій, що також є джерелом різноманітних внутрішніх загроз.

Враховуючи те, що інформаційна безпека є невід'ємною складовою національної безпеки, її регулювання потребує дієвих механізмів у формі політичних рішень або прийнятих нормативно-правових актів. Функціонування відповідного механізму можливе лише за умови належного рівня наукового осмислення теоретичних положень щодо інформаційної безпеки взагалі та сутності загроз, зокрема [1].

Наразі в Україні на законодавчому рівні відсутні достатні гарантії захисту населення від спеціальних та інформаційно-психологічних впливів, наслідком яких може стати руйнація єдиного інформаційно-духовного простору. Тому виникає необхідність формування функціональної, а не декларативної системи забезпечення інформаційної безпеки тепер і зараз, не відкладаючи на потім. Потім може бути запізно.

В науковому середовищі існує думка, що на сучасному етапі формування системи інформаційної безпеки сама система безпеки має безсистемний характер. По-перше, основи нормативної бази не відповідають реаліям, а визначальні поняття неузгоджені між собою. По-друге, у законодавстві визначено велику кількість суб'єктів, котрі повинні здійснювати захист інформаційної безпеки, але взаємодія між ними є складною бюрократичною процедурою. По-третє, вся система законодавства, яке регулює інформаційну безпеку, є громіздким механізмом, котрий вимагає великих витрат ресурсів, часу та фахівців.

Разом із тим інформаційна сфера є надзвичайно динамічною системою і вимагає швидких реакцій. Це зумовлює необхідність створення ефективної системи інформаційної безпеки, котра б адекватно реагувала на виклики та загрози в інформаційній сфері. Інформаційна сфера є комплексним, складним об'єктом, забезпечення захисту якого вимагає спеціальних нормативно-правових, управлінсько-організаційних та техніко-технологічних заходів. Розробка та здійснення цих заходів є пріоритетним обов'язком держави та вимагає створення органів, які здійснюватимуть відповідні функції [2].

Ця система має будуватися на основі реальної взаємодії всіх гілок влади, а також громадських організацій. У процесі реалізації державної політики у сфері безпеки необхідно приділяти увагу, серед іншого, таким питанням: розробці та реалізації комплексних заходів щодо запобігання, нейтралізації і попередження негативних наслідків спеціальних та інформаційно-психологічних впливів на суспільство і державу; підготовці суспільства до активної інформаційної протидії; питанням входження національного інформаційного поля у світовий інформаційний простір; вдосконаленню системи масової інформації та комунікації; формуванню системи підготовки особового складу сектора безпеки до інформаційно-психологічної протидії; духовній консолідації суспільства тощо. У сучасних умовах інформаційну безпеку слід визнати основою інформаційної складової всіх сфер національної безпеки. До основних завдань системи забезпечення інформаційної безпеки мають належати: питання щодо: прогнозування ризиків реалізації державної внутрішньої та зовнішньої політики, міждержавних і державних програм та проектів; визначення внутрішніх і зовнішніх потенційних і реальних загроз; розроблення та впровадження адекватних заходів і засобів реагування на виклики як історичного походження, так і сучасного цивілізаційного розвитку; нейтралізації або послаблення наслідків проявів спеціальних заходів впливу та інших загроз інформаційній безпеці України [3].

З огляду на входження України до сфери впливу одразу декількох найпотужніших світових суб'єктів, успішна реалізація власних інтересів України на міжнародній арені вимагає вдосконалення міжвідомчої взаємодії, чіткої координації та узгодженості дій усіх зацікавлених сторін, у тому числі: розвідувальних органів спецслужб, міністерств, відомств та інших установ України. Зазначене можливе у випадку запровадження єдиного державного механізму відпрацювання скоординованих та злагоджених дій, пов'язаних єдиним задумом, а також постановки завдань, що потребують для реалізації залучення спеціальних засобів і методів спецслужб. Для цього необхідно продовжити *відпрацювання механізму взаємодії* як між самими спецслужбами, так і спецслужб з іншими державними та недержавними суб'єктами, оскільки в ході організації цієї роботи не завжди збігається бачення шляхів вирішення проблемних питань спецслужбами, з баченням відповідних міністерств та відомств держави. Системний і комплексний підхід до вирішення цих проблем має належним чином визначати напрями державної політики у сфері інформаційної безпеки. Тому забезпечення інформаційної

безпеки є визначальним напрямом державної політики, від якого залежатиме існування суверенної та незалежної держави, її національна безпека, соціально-економічний розвиток та належне місце у світовому співтоваристві.

Отже, в Україні має бути вибудована реально скоординована інформаційна політика органів влади щодо реально дієвої системи забезпечення інформаційної безпеки держави. Скоординована інформаційна політика це не лише контроль над інформаційним простором, але й забезпечення за допомогою інформації єдності держави та непорушності державницьких засад. Мова йде про: забезпечення переходу України до нового етапу розвитку інформаційно-комунікаційної структури та інформаційних, телекомунікаційних технологій; ефективне формування та використання національних інформаційних ресурсів і забезпечення широкого доступу до них; забезпечення громадян суспільно значимою інформацією через створення незалежних засобів масової інформації; розробка необхідної правової бази побудови інформаційного суспільства [4].

Забезпечення національної безпеки в інформаційної сфері значною мірою залежить від захисту національних інтересів України у зовнішньополітичній сфері від інформаційних впливів на закордонну аудиторію. Варто зазначити, що дедалі більшої актуальності набуває проблема визначення в державній інформаційній політиці засад протидії зовнішньому впливу на внутрішньополітичну ситуацію в Україні. Сьогодні з'явилася потреба в посиленні державного контролю за діяльністю міжнародних неурядових організацій, що діють завдяки засобам і ресурсам, зокрема фінансовим, які надають уряди іноземних держав чи їхні структури для втручання в інформаційний простір України [5].

Іноземні суб'єкти інформаційних відносин часто чинять потужний негативний інформаційно-психологічний вплив на Україну, поширюючи тенденційну, неповну або упереджену інформацію. Інтенсивність такого впливу значною мірою не залежить від провладних еліт в Україні, а зумовлена насамперед прагненням керівництва іноземних держав впливати на зовнішню та внутрішню політику держави, також має під собою політичне й економічне підґрунтя, продиктоване прагматичними підходами до забезпечення власних національних інтересів. Іноземні держави залежно від їхнього зовнішнього інформаційно-психологічного впливу на Україну можна поділити на дві групи: групу ситуативного впливу та групу постійного впливу. До групи ситуативного впливу можна зарахувати більшість західних держав, інформаційні впливи яких здебільшого стосуються євроінтеграційних перспектив України, внутрішньополітичної та економічної ситуації в нашій державі, російсько-українських відносин, деяких аспектів трактування історії тощо. До країн, що чинять постійний і найінтенсивніший інформаційно-психологічний вплив на Україну, слід віднести насамперед РФ [6].

Саме тому вкрай важливо створити сприятливі умови для вдосконалення вітчизняних систем інформаційного захисту, що набуває особливої актуальності у зв'язку з розширенням інформаційного обміну через мережу Інтернет. Є нагальна потреба у відпрацюванні узгоджених правил і процедур захисту національних інтересів України в процесі інтегрування з міжнародними інформаційними мережами. З огляду на це необхідно запровадити ефективну систему своєчасного виявлення і відвернення небезпеки використання нових інформаційних технологій для створення реальних і потенційних загроз інформаційній безпеці України.

Як бачимо, наразі існує нагальна потреба щодо напрацювання узгоджених правил і процедур захисту національних інтересів України в процесі інтегрування в міжнародні інформаційні мережі. З огляду на те, що державна інформаційна політика здійснює

суттєвий вплив на різні сторони громадського життя, профільні державні органи повинні тісно взаємодіяти з *органами держбезпеки і зовнішньої розвідки, закордонних справ* з метою оцінки як політичних (зовнішні і внутрішні), так і економічних ризиків та вироблення адекватних упереджувальних заходів з мінімізації негативних наслідків. Для розв'язання цих проблем вважається доцільним вжити таких заходів:

– повинна бути створена ефективна багаторівнева *державна система* забезпечення інформаційної безпеки, у якій будуть діяти єдині правові норми і механізми її забезпечення, захисту інформаційних ресурсів, інформаційно-телекомунікаційної інфраструктури й інформаційних прав громадян, здійснюватися ефективна координація діяльності органів державної влади й управління;

– варто на законодавчому рівні розробити механізм узгодження діяльності органів державної і місцевої влади в галузі забезпечення інформаційної безпеки, для чого доцільно було б скористатися досвідом Європарламенту щодо створення спеціального комітету з питань "Європейського щита демократії" з метою протидії інформаційним втручанням [7];

– бажано активізувати діяльність з питань формування державної політики в галузі забезпечення інформаційної безпеки регіонів, створення необхідних для реалізації цієї політики організаційних структур і нормативно-правової бази. Вирішення цієї проблеми зумовлено тим, що органи державної влади та місцевого самоврядування вдаються до закупок імпортного обладнання із залученням іноземних фірм, що підвищує ймовірність несанкціонованого доступу до інформації. Особливо небезпечним у цьому контексті є придбання імпортного програмно-технічного забезпечення з недокументованими функціями [8].

Саме тому надважливим моментом для формування політичної нації, здатної протистояти як інформаційним, так і іншим війнам, а основне – всеохопній корупції як внутрішньому найагресивнішому ворогові держави, має стати визнання того, що жоден прогресивний поступ неможливий, якщо не буде витворено й умотивовано власне ідеологію державотворення України, яку б розуміло і підтримувало суспільство в цілому [9].

Значимість інформаційної безпеки як складової національної безпеки України можна пояснити залежністю від реалізації найважливіших інтересів України в зовнішній та внутрішній інформаційній сфері. Закон України "Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" визначає інформаційну безпеку як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому вдається запобігти завдаванню шкоди через: неповноту, невчасність та невірогідність використовуваної інформації; негативний *інформаційний вплив*; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання, порушення цілісності, конфіденційності та доступності інформації [10].

Ще більший прорив у необхідності формування державної політики інформаційної безпеки визначено в Указі президента України № 449/2014 "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України". У цьому документі акцентувалась увага на: необхідності *удосконалення нормативно-правового забезпечення* інформаційної безпеки, відвернення й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері. Для цього передбачалося розробити і впровадити комплексні заходи організаційного, інформаційного і роз'яснювального характеру, зокрема щодо: посилення контролю за додержанням законодавства *з питань інформаційно-психологічної* та кібернетичної безпеки [11].

Згодом у Стратегії національної безпеки України, затвердженій Указом президента України від 26 травня 2015 р., пріоритетами забезпечення інформаційної безпеки визначено, зокрема: *протидію інформаційним операціям проти України*, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; *розробку і реалізацію скоординованої інформаційної політики органів державної влади; створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку*, з урахуванням практики держав – членів НАТО. Пункт 4.11 Стратегії до основних напрямів державної політики національної безпеки України із забезпечення інформаційної безпеки відносить виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності [12].

На жаль у новій Стратегії національної безпеки України, затвердженій Указом Президента України від 14 вересня 2020 року № 392/2020, про *інформаційну безпеку держави уже не згадується*. Щоправда пункт 45 Стратегії визначає, що: «Пріоритетними завданнями правоохоронних, спеціальних, розвідувальних та інших державних органів відповідно до їх компетенції є: активна та ефективна протидія розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам, російській та іншій підривній пропаганді [13]. Отже ми знову в глухій обороні - зосереджуємося на протидії СІО та кібератакам і залишаємося об'єктом інформаційної війни, і навіть не намагаємося перехопити ініціативу у противника. Тобто стати суб'єктом інформаційного протиборства.

Доктрина інформаційної безпеки України від 29 грудня 2016 року до пріоритетів державної політики в інформаційній сфері (пункт 5.1) додала: "*створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них"*, а також досягнення адекватного рівня спроможності держави відповідати реальним і потенційним загрозам національним інтересам України в інформаційній сфері [14].

У ній визначено, що саме проти України РФ використовує *найновіші інформаційні технології* впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України. Метою документа була - протидія руйнівному *інформаційному впливу* РФ в умовах розв'язаної нею війни.

Проте, у ***цих напрямах практично нічого не було зроблено, зокрема***:

- не було сформовано єдиних підходів, протидії інформаційним впливам;
- не створено інститутів, що відповідають за інформаційно-психологічну безпеку,
- не створено ефективної системи протидії інформаційній агресії та реалізації інтересів держави за кордоном;
- не створено інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них тощо.

Це, зрозуміло, ускладнювало своєчасне проведення заходів протидії акціям інформаційного впливу іноземних держав та нейтралізації їхніх негативних наслідків для України. Ефективно протистояти інформаційним загрозам у сучасних умовах може лише добре організована державна система забезпечення інформаційної безпеки, що може відбутися лише у разі взаємодії всіх державних органів, недержавних структур і громадян.

І нарешті, на заміну Доктрині інформаційної безпеки України від 29 грудня 2016 Указом Президента України 28 грудня 2021 року № 685/2021 була введена в дію Стратегія інформаційної безпеки України (далі Стратегія), термін дії якої закінчився 2025 року. Вона стала черговим кроком у спробі підвищення ефективності інформаційної політики шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України і нейтралізації інформаційної агресії, у тому числі *спеціальних інформаційних операцій* держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством [15].

Цією Стратегією забезпечення інформаційної безпеки України було визначено однією з найважливіших функцій держави. Далі Стратегія визначає актуальні виклики та загрози інформаційній безпеці, стратегічні цілі та напрями реалізації стратегії, механізми реалізації визначеної мети та завдань. [15].

У цьому контексті чи не одним із головних завдань державної політики інформаційної безпеки мало б бути визначення конкретних об’єктів України, на які постійно впливають інші держави, руйнуючи українську державність та її цілісність, а також суб’єктів таких впливів.

Метою цієї Стратегії було посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина. Досягнення мети мало здійснюватися шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі *спеціальних інформаційних операцій* держави-агресора [15].

Мабуть було б доцільним мету, з якою відбуваються впливи, визначати не взагалі, а відповідно до кожного із суб’єктів агресивного інформаційного впливу, що давало б можливість більш цілеспрямовано діяти при проведенні операцій з протидії інформаційним впливам. Зокрема, для визначення засобів протидії інформаційним впливам спочатку варто визначити структурні елементи цього процесу. До структурно-функціональних елементів впливу відносяться об’єкт впливу, суб’єкт впливу та форма їхньої взаємодії. Наприклад, об’єктом інформаційно-психологічного впливу є психіка, а точніше свідомість або підсвідомість людини – нейролінгвіністичне програмування, яке повинно змінити погляд об’єкта на питання щодо ставлення до: політики країни в цілому, уряду, конкретних осіб істеблішменту країни або викликати в нього якесь постійне безперервне почуття: паніки, страху, байдужості тощо. Тому є змога через підсвідомий рівень через маніпуляції впливати на свідомість людей, а в аспекті інформаційної безпеки – на свідому суспільну діяльність людей. Особливістю НЛП є те, що його можна використовувати як для протидії впливам, так і для їх здійснення.

Суб’єктом інформаційного впливу є недружні до України як конкретні особи, організації, так і держави в цілому, що чинять цілеспрямований деструктивний вплив на українську інформаційну сферу з метою досягнення власних, переважно шкідливих для національної безпеки України інтересів. Завдяки особливостям психіки суб’єкт інформаційного впливу може маніпулювати особистістю, через підсвідомість впливати на свідомість членів тієї спільноти, у якій він хоче реалізувати свої інтереси. Такі дії

суб'єкта впливу приводять до того, що ті, хто зазнав впливу, можуть проявляти потрібну суб'єктові поведінку та створювати вигідну для нього ситуацію [16].

Це власне і є джерелом формування суб'єктивного зразка інформаційних загроз та предметом діяльності відповідних спецслужб і завдання державної політики інформаційної безпеки щодо вироблення механізмів протидії таким загрозам.

Форма взаємодії суб'єкта та об'єкта інформаційного впливу визначається через засоби та методи впливу: телерадіомовлення, комп'ютерні мережі, друковані мас-медіа, телефон, телеграф, пошта, кіно і відеопродукція, видавництво і книгарні, бібліотеки та архіви, музеї та експозиції, реклами та листівки, виставки та ярмарки тощо. Методи інформаційного впливу: маніпулювання, пропаганда, дезінформування, шантаж, кризове управління і тому подібні. Середовищем взаємодії суб'єкта та об'єкта впливу є інформаційний простір. Тобто, вплив на свідомість з метою реалізації певних інтересів відбувається через інформацію [16].

Таким чином, державна політика інформаційної безпеки пов'язана з безпекою суспільства і держави та залежить не тільки від боєготовності збройних сил, але й від політичної стабільності суспільства, настроїв населення тощо. Якраз стабільність суспільства та настрої населення і є першочерговими об'єктами інформаційних впливів. Крім цього, *основними загрозами* для держави є дії, вчинені під впливом спеціальних інформаційних чи інформаційно-психологічних операцій, спрямованих на дестабілізацію держави, влади, соціально-політичних інститутів тощо.

Збройні конфлікти кінця XXI ст. переконливо засвідчують, що технології ведення війни, спрямовані на досягнення перемоги, крім засобів ураження та фізичного знищення противника, обов'язково містять спеціальні заходи впливу, зниження морально-психологічної стійкості, паралічу волі до опору, формування депресивних і панічних настроїв серед населення, а отже - створення сприятливої для ініціатора війни соціально-психологічної ситуації. Тому головною метою державної політики інформаційної безпеки є розробка та реалізація її концептуальних засад шляхом прийняття відповідних нормативно-правових актів з питань регулювання інформаційних відносин. Наразі ми можемо констатувати наявність в Україні концепцій, доктрин, стратегій, законів, указів та інших нормативно-правових актів щодо забезпечення інформаційної безпеки. Тобто спроби правового регулювання інформаційної безпеки в Україні відбуваються, що вже є позитивним кроком.

Проте шляхи реалізації прийнятих норм на практиці розвиваються дуже повільно і в більшості випадків є незручним, через невизначеність алгоритму дій, інструментом для практичного застосування і забезпечення ефективності запроваджених механізмів. Тому є нагальна потреба в комплексному та дієвому підході до процесу забезпечення безпеки національного інформаційного простору. У цьому аспекті доцільно було б використати досвід розробки нормативних документів зарубіжних країн, законодавство про інформаційну політику та інформаційну безпеку яких формувалося десятиліттями. Їхня суть полягає у злагодженій діяльності відповідного державно-правового механізму, тобто системі взаємопов'язаних державних органів, організацій, установ щодо розроблення та реалізації комплексу норм і принципів права, які мають регулювати суспільні відносини у сфері інформаційної безпеки [17].

Очікувалося, що Стратегія як основоположний документ, що визначав завдання та напрями діяльності держави до 2025 року з проблем запобігання кризовим явищам у вітчизняному інформаційному просторі, посилення інформаційної безпеки та її складових мала б посилити спроможність держави щодо забезпечення власної інформаційної безпеки та захисту інформаційного простору, а також перенесення

акцентів від оборонного характеру до наступального, стати нарешті не об'єктом, а суб'єктом інформаційного протиборства.

Тим не менше першою головною ціллю Стратегії стала: «Протидія *дезінформації* та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини..» [15, стратегічна ціль 1]. Досягнення цієї цілі має здійснюватися шляхом виконання, якщо коротко, таких завдань: - створення системи раннього виявлення, прогнозування та запобігання *гібридним загрозам*, зокрема, *створення системи протидії дезінформації* та інформаційним операціям, спрямованої на запобігання, максимально швидке виявлення та реагування держави і суспільства на інформаційні загрози; - ужиття заходів щодо запобігання та *протидії поширенню дезінформації* та деструктивної пропаганди стосовно європейської та євроатлантичної інтеграції України і так далі в цьому напрямі [15].

У чому тут проблема? По-перше, виходячи з тексту Стратегії - головною загрозою для України є *дезінформація*, а потім уже інформаційні операції. Але ж дезінформація це лише один із способів психологічного впливу, а інформаційні операції – це комплекс окремих видів/способів впливу таких, наприклад, як маніпулювання, інформаційно-психологічні, спеціальні впливи тощо. Певною мірою у них може бути задіяна й дезінформація, але не обов'язково.

По-друге, у Стратегії нічого не говориться про спеціальні інформаційні операції, інформаційно-психологічні операції тощо і, нарешті про спеціальні заходи впливу, а це набагато серйозніші складові інформаційних воєн ніж дезінформація. Між іншим, *спеціальні заходи впливу* – це багатоешелонований, багатофункціональний, багатовекторний комплекс *заходів держави*, спрямованих на просування власних інтересів за кордоном засобами "м'якої сили", що ґрунтується на методах переконання або "жорсткої сили", яка ґрунтується на військовому і економічному тиску. За своєю суттю вони є багатоаспектними та різноплановими заходами з використанням усього комплексу спеціальних методів із залученням відповідних сил і засобів. Мета цих заходів може бути різною від політичної, економічної чи іншої підтримки союзників до дестабілізації ситуації в країнах-супротивниках, зміни урядів або навіть анексії територій без військового втручання – наприклад анексія Криму. Класичні цілі спеціальних заходів впливу в основному: – це повна або часткова дезінтеграція держави, якісні зміни її внутрішнього та зовнішнього політичного курсу, зміна державного керівництва на лояльні режими, встановлення над країною зовнішнього контролю ідеології та фінансово-економічного стану, хаосу та підпорядкування диктату інших держав [18].

Спеціальні інформаційні операції - це напрям спеціальних заходів впливу зі здійснення вигідного для України впливу в інформаційній сфері. За своєю сутністю це комбінація заходів з використанням спеціальних сил та засобів спеціальних органів для впливу на об'єкт з метою спонукання його до діяльності або бездіяльності, відповідно до заданої лінії поведінки і без можливості встановлення прямого зв'язку їхнього проведення з нашим суб'єктом впливу. За своєю суттю спеціальні інформаційні впливи - це операції спрямовані: проти об'єктів, які ухвалюють рішення; на їх компрометацію, завдання шкоди опонентам (моральної тощо); на політичну (економічну тощо) дестабілізацію [18].

Відмінністю спеціальних інформаційних операцій від спеціальних інформаційно-психологічних операцій є акцент на здійснення змін у свідомості людей не тільки й не стільки через використання психологічних особливостей, а через властивості комунікативних процесів, як процесів соціальних за своєю суттю. Психологічні особливості мають враховуватися, але не вони відіграють провідну роль спеціальних інформаційних операцій.

Далі в розділі "*Національні виклики та загрози"* говориться що спеціальні служби Російської Федерації проводять свої ***спеціальні інформаційні операції***, більшість із яких спрямовані на підрив національної безпеки України, її національних інтересів, ліквідацію української державності та знищення української ідентичності, провокування проявів екстремізму, панічних настроїв у суспільстві, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації в Україні. І тут же в підрозділі "*Обмежені можливості реагувати на дезінформаційні кампанії"* акцентується увага не на спеціальних інформаційних операціях, а на тому, що в Україні досі *не створена ефективна система реагування на* ***виклики*** деструктивної пропаганди, поширення *дезінформації.* А чи потрібна ще одна локальна система протидії окремо дезінформації? Адже дезінформація - це лише один із способів психологічного впливу [19].

То можливо будемо *створювати системи реагування на* ***виклики*** *кожного способу психологічного, інформаційного та інших (понад 20) впливів.* Складається таке враження, що люди, які писали цю Стратегію, не розуміють що таке дезінформація і, що таке інформаційні, інформаційно-психологічні чи спеціальні інформаційні впливи і яка різниця між впливами й операціями.

До речі, незрозуміло, що в Стратегії розуміється під викликами. Якщо інформаційна загроза визначена як 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, то визначення викликів в понятійному апараті відсутнє.

Наразі у нас уже створена система забезпечення інформаційної безпеки держави, в якій ураховані й питання протидії дезінформації як одному із елементів інформаційних впливів, хоча ця система й не досконала, і в ній є певні інституційні проблеми. По-перше, не створена державна структура для розроблення та узгодження міжвідомчих складників системи забезпечення інформаційної безпеки для проведення в єдиному задумі скоординованих інформаційних операцій держави. Особливо це важливо в умовах війни, коли треба зібрати сили і бити по ворогу, образно кажучи, кулаком в конкретне місце, а не просто тицяти кудись розчепіреними пальцями.

По-друге, інформаційні заходи оборони держави згідно зі Стратегією - це сукупність скоординованих дій, які готуються та здійснюються *суб'єктами* забезпечення національної безпеки і оборони України. У нашій державі на інституційному рівні забезпеченням окремих напрямів інформаційної безпеки опікувалися й опікуються наразі низка органів державної влади. Однак донині не визначено (не створено) структуру, спроможну реально координувати: "дії які готуються та здійснюються суб'єктами забезпечення національної безпеки і оборони України" [15].

Далі, згідно зі Стратегією до переліку загроз і *викликів*, які постали перед нашою державою, входять: повноформатна експансивна інформаційна політика Російської Федерації; досить низький рівень медіаграмотності громадян; динамічне зростання

кількості глобальних кампаній *дезінформації*; інформаційне домінування Російської Федерації на тимчасово окупованих територіях; використання технологій для маніпулювання свідомістю пересічних громадян тощо [15]. Звісно, можна погодитися з цим переліком, але незрозуміло, що в ньому віднесено до загроз, а що до викликів.

Потім у розділі "*Механізми реалізації визначеної мети та завдань"* Стратегії сказано, що: "координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері здійснює Рада національної безпеки і оборони України, зокрема *з використанням спроможностей Центру протидії дезінформації"* [15].

Однак, питання протидії інформаційним впливам це не вирішує. Центр можливо й компетентний у питаннях дезінформації, але координувати, наприклад спеціальні заходи впливу або спеціальні інформаційні операції - головні компоненти інформаційного протиборства, центр не в змозі. Тому, що ці заходи, як правило, мають гриф "цілком таємно". До таких операцій навіть в СБУ чи розвідці допускається дуже обмежене коло співробітників.

Також планувалося, що за успішної реалізації Стратегії Україна мала б захищений інформаційний простір, що гарантувало б інформаційну безпеку держави та її суб'єктів; ефективне функціонування системи стратегічних комунікацій; запровадження ефективних заходів протидії поширенню нелегального контенту і тому подібне. На жаль, і цю Стратегію спіткала доля інших нормативно-правових актів державної політики інформаційної безпеки, які мали декларативний характер і нікого ні до чого не зобов'язували.

Ще одна проблема, пов'язана з функціонуванням державної системи інформаційної безпеки – це забезпечення прозорості діяльності державних органів, що беруть участь у формуванні відкритих державних інформаційних ресурсів і забезпеченні доступу до них громадян [15]. Нині відсутність таких ресурсів і доступу до них стає перешкодою для залучення внутрішніх і закордонних інвестицій, оскільки комерційні структури готові вкладати свої гроші в розвиток відкритих державних ресурсів за умови, що ці кошти буде використано за призначенням.

Проблеми забезпечення інформаційної безпеки України багато в чому зумовлені недоліками в правовому регулюванні - правової невизначеності взаємодії суб'єктів інформаційної безпеки в процесі розв'язання завдань безпеки. Як зазначалося вище, метою Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору... і так далі за текстом. А досягнення цієї мети повинно було здійснюватися шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора …далі за текстом [15].

Суть проблеми мабуть у тому, що в таких документах як концепції, доктрини, стратегії не прослідковується взаємозв'язок напрямів державної політики у сфері забезпечення інформаційної безпеки з правовими механізмами, визначеними на законодавчому рівні щодо: взаємодії державних і громадських інституцій з питань реалізації міжвідомчих напрямів державної політики; організації системи інформування суб'єктів, що здійснюють діяльність у сфері інформаційної безпеки, з поточних проблем, виявлення потенційних і реальних загроз та їх джерел, а також відповідних заходів і засобів їх запобігання, нейтралізації та ліквідації можливих наслідків; скоординованих і цілеспрямованих дій суб'єктів, які діють у різних сферах життєдіяльності суспільства і держави, з питань адекватного реагування на виявлені

потенційні та реальні загрози; національне керівництво, координація та контроль у сфері забезпечення інформаційної безпеки [19].

Головна системна проблема інформаційної безпеки та, що в Україні ще не сформовано *дієвої* ***системи*** забезпечення інформаційної безпеки. Проте, навіть за умов успішної протидії всім інформаційним загрозам, нашу державу, якщо вона не знайде можливостей проводити наступальні скоординовані акції (операції) інформаційного впливу в таборі супротивника, й надалі сприйматимуть як постійну державу — жертву інформаційних атак. У цьому контексті постає нагальна потреба у створенні й організації **єдиної державної системи інформаційного протиборства** для розроблення та узгодження міжвідомчих складових забезпечення інформаційної безпеки в єдиному задумі скоординованих інформаційних операцій держави. Для координації та узгодженості дій державних органів, відомств та інших суб'єктів системи інформаційного протиборства, чіткого визначення їхніх конкретних завдань доцільно створити координаційний центр інформаційної безпеки, підпорядкований безпосередньо помічнику президента з національної безпеки (ввести таку посаду як у США, наприклад) або заступнику голови Офісу Президента, який мав би ***відповідні повноваження приймати управлінські рішення з питань протиборства в інформаційній сфері та ніс персональну відповідальність за їх наслідки***. Також надати йому право залучати до участі в розробці загальнодержавних інформаційних операцій відповідні міністерства й відомства, а також аналітичні центри, центри стратегічних комунікацій, зв'язків з громадськістю, ЗМІ як державної, так приватної власності тощо [20].

Саме відсутність дієвої координації, децентралізація управління і відомчість, що характеризували просування національних інтересів і державної політики України за кордоном у довоєнний період, призводили до поразок держави на інформаційному фронті до початку повномасштабної війни. У цьому контексті, розбалансованість системи забезпечення інформаційної безпеки в секторі протидії інформаційній експансії є чи не основною причиною невдач ще до початку воєнних дій. Жодну війну нині не можна виграти, доки не буде перемоги на інформаційному фронті. Можна мати чи отримати надсучасну зброю, виграти бій, але остаточної перемоги у війні без перемоги на інформаційному фронті боротьби за суспільну свідомість здобути неможливо. [21].

Висновки. Системні проблеми інформаційної безпеки України багато в чому зумовлені недоліками в правовому регулюванні взаємодії органів виконавчої влади в процесі розв'язання завдань забезпечення інформаційної безпеки. Наразі жодна сфера життя суспільства чи держави не може функціонувати без розвинутої інформаційної структури. Інформація нині здобуває конкретне політичне, матеріальне і вартісне вираження. І саме через інформаційне середовище здебільшого реалізуються загрози національній безпеці в різних сферах життєдіяльності держави. Ефективно протистояти інформаційним загрозам в сучасних умовах може лише добре організована державна система забезпечення інформаційної безпеки, що потребує взаємодії всіх державних органів, недержавних структур і громадян.

Значимість інформаційної безпеки як складника національної безпеки України можна пояснити залежністю реалізації найважливіших інтересів України в зовнішньополітичній сфері від інформаційних загроз. Інформаційна безпека згідно з чинним законодавством України – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому вдається запобігти завданню шкоди через: неповноту, невчасність та невірогідність використовуваної інформації; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій;

несанкціоноване розповсюдження, використання, порушення цілісності, конфіденційності та доступності інформації.

У цьому контексті надзвичайно важливо створити підґрунтя для формування інституційного забезпечення інформаційної безпеки. Держава повинна проводити заходи із забезпечення безпеки особистості, суспільства й держави, приділяти увагу істотному розширенню переліку вітчизняних інформаційних послуг для населення, забезпеченню правового регулювання відносин у національній інформаційній сфері.

Зрозуміло, що національна безпека пов'язана з безпекою суспільно-політичної системи країни і в сучасних умовах залежить не тільки від боєготовності збройних сил, а й від політичної стабільності суспільства, настроїв населення тощо. Якраз політична стабільність суспільства та настрої населення і є першочерговими об'єктами інформаційно-психологічних впливів. Крім цього основними загрозами для держави можуть бути дії, вчинені під впливом інформаційно-психологічних операцій, різних соціально-політичних суб'єктів (інших держав чи певних зовнішніх структур, партій, рухів, еліт, прошарків суспільства, соціальних груп, особистостей усередині країни тощо), що спрямовані на дестабілізацію політичної системи, підриву довіри до влади, політичного режиму, соціально-політичних інститутів тощо.

В цілому, наведені пропозиції і висновки не є виключними і передусім спрямовані на необхідність серйозного підходу при формуванні правової бази, координації міжвідомчої діяльності в інформаційній сфері, проведенні інформаційних впливів та протидії інформаційній агресії.

ПОДЯКИ: Немає

КОНФЛІКТ ІНТЕРЕСІВ: Немає

Використана література

1. Золотар О.О., Трибун І.О. Класифікація загроз інформаційній безпеці. *Інформація і право.* № 3(9)/2013. 105с.

2. Горбулін В.П. Проблемні питання оборонної політики України в контексті нових викликів національній безпеці. *Стратегічна панорама*. 2003. № 3/4. С. 148-155.

3. Дмитренко Микола, Проблемні питання інформаційної безпеки України: монографія Національна безпека в умовах інформаційних та гібридних війн: / за заг. ред.: В. Куйбіди і В. Бебика. Київ : В-во НАДУ. 2019. С.145-160.

4. Інформаційна політика 2024-2025 н.р. Державний університет «Житомирська політехніка», Освітній портал. URL: https //learn.ztu.edu.ua/course/view.php?ia=6523#section-2

5. Дмитренко. М. Зовнішньополітичні впливи як пріоритети діяльності зовнішньої розвідки. *Збірник наукових праць Інституту СЗРУ.* 2013. № 5. С. 18-32.

6. Партоленко І. Інформаційно-психологічний вплив в контексті інформаційної безпеки держави. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. наук.- практ. конф. (Київ, 30 березня 2018 р.). К. : Нац. акад. СБУ, 2018. С. 249–251

7. Європарламент створив спецкомітет для протидії дезінформації. URL: https://internetua.com/yevroparlament-stvoriv-speckomitet-dlya-protydyi-dezinformaciyi?utm)_source=ukrnet_news

8. Дмитренко Микола, Проблемні питання інформаційної безпеки України: монографія Національна безпека в умовах інформаційних та гібридних війн: / за заг. ред. : В. Куйбіди і В. Бебика. Київ : В-во НАДУ. 2019. С.145-160.

9. Дмитренко М. А. Політична система України: розвиток в умовах глобалізації та інформаційної революції : монографія. 2-ге вид., з доповненнями та змінами. К. : Ун-т "Україна", 2011. 820 с.

10. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 № 537-V. URL: https://zakon.rada.gov.ua/go/537-16

11. Указ Президента України, Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»// Указ Президента України № 449/2014. URL: shttps://president.gov.ua/documents/17588.html

12. Указ Президента України від 26 травня 2015 року №287/2015 «Про Стратегію національної безпеки України». URL: https://www,president.gov.ua/documtnts/2872015

13. Указ Президента України від 14 вересня 2020 року № 392/2029 «Про Стратегію національної безпеки України». URL: https://https://zakon.rada.gov.ua/laws/show/392/2020#Text

13. Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України. URL: https://www.president.gov.ua/documents/472017-21374

14. Указ Президента України від 28 грудня 2021 року № 685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://zakon.rada.gov.ua

15. Захаренко К. Протидія маніпулятивним впливам (засоби, технології, можливості) // Гілея: науковий вісник: зб. наук. пр. 2018. Вип. 137. С. 181-189 .

16. Захаренко К. Міжнародний досвід інформаційної безпеки // Сучасне суспільство: політичні науки, соціологічні, культурологічні науки. Вип. 1 (17). Харків. 2019. С. 95-109.

17. Дмитренко М. А. Спеціальні заходи впливу як механізм протистояння зовнішньополітичним впливам в інформаційних війнах у світлі подій на Донбасі. *Збірник наукових праць Інституту СЗРУ*. 2016. № 12. С. 21-36

18. Дезінформація – спосіб психологічного впливу. URL: https//uk.wikipedia.org

19. Захаренко К. Стратегія формування ефективної системи державної інформаційної безпеки // Гілея: науковий вісник. 2018. Вип. 131. С. 268-272.

20. Національна доповідь. «Політика інтеграції українського суспільства в контексті викликів та загроз подій на Донбасі» // за ред. Е.М.Лібанової. К.: НАН Україні 2015. 363с.

Дмитренко Микола Андрійович
доктор політичних наук, професор, академік Української Академії політичних наук, заслужений діяч науки і техніки України
професор Національної академії Служби безпеки України
03022, Україна, м. Київ, вул. Михайла Максимовича 22
email: mdmytren@gmail.com

Mykola A. Dmytrenko
Dr. hab. of Political Sciences, Professor, Academician of the Ukrainian Political Science, Honored Worker of Science and Technology of Ukraine
Professor of the National Academy Security Service of Ukraine
22 Mikhail Maksimovich Street, Kyiv, 03022, Ukraine
email: mdmytren@gmail.com

Рекомендоване цитування: Дмитренко М. Системні проблеми інформаційної безпеки України. *Інформація і право*. № 2(57)/2026. 2026. С. 141-156. https://doi.org/10.37750/2616-6798.2026.2(57).364412

Suggested Citation: Dmytrenko M. (2026) Systemic Problems of Ensuring Ukraine's Information Security. *Information and Law*. 2(57)/2026. 141-156. https://doi.org/10.37750/2616-6798.2026.2(57).364412

Дата надходження статті до редакції: 14.05.2026 р.
Дата прийняття статті до друку після рецензування: 21.05.2026 р.
Дата публікації (оприлюднення): 26.05.2026 р.

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