УДК 327.5:911.3]:316.776.23] (02)
DOI https://doi.org/10.32782/2524-0374/2024-3/2

РОЗВИТОК НОРМАТИВНО-КОНЦЕПТУАЛЬНИХ ПОГЛЯДІВ НА СУТНІСТЬ І ЗАВДАННЯ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ В ЄВРОАТЛАНТИЧНОМУ ВОЄННО-ПОЛІТИЧНОМУ ПРОСТОРІ

DEVELOPMENT OF NORMATIVE AND CONCEPTUAL VIEWS ON THE ESSENCE AND TASK OF STRATEGIC COMMUNICATIONS IN THE EURO-ATLANTIC MILITARY AND POLITICAL

Вєдєнєєв Д.В., д.і.н.,
провідний науковий співробітник
Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при РНБО України

Семенюк О.Г., д.ю.н.,
перший заступник керівника
Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при РНБО України

У статті проведено аналіз творення доктринальних й -розпорядчих засад системи стратегічних комунікацій як нового якісного етапу розвитку сфери інформаційного протиборства та воєнно-політичної комунікації у діяльності Північноатлантичного співтовариства. Розглядається докорінний перегляд концептуальних поглядів на традиційні способи, форми і методи інформаційно-психологічного протиборства, що знайшло відображення у розробці доктринальних засад й творенні системи «стратегічної пропаганди», або ж стратегічних комунікацій, в основі якої містився перехід від окремішного застосування профільних військових і цивільних структур до їх тісної інтеграції та координації діяльності в інформаційно-когнітивному просторі, у т.ч. – в умовах кризового врегулювання, у конфліктах різного ступеня інтенсивності. У дослідженні простежується розвиток концептуальних поглядів та нормативних настанов щодо визначення складових, функцій та організаційного механізму провадження стратегічних комунікацій на рівні стратегічних документів воєнно-політичного планування США та блоку НАТО. Висвітлюється визначені в НАТО принципи та провідні функціональні складові реалізації стратегічних комунікацій.

На думку авторів, нагальною видається необхідність розробки концептуальних документів у галузі діяльності національної системи стратегічних комунікацій. При цьому потребують визначення її змістовні пріоритети, механізми координації діяльності складових системи СТК, а також виокремлення функцій (напрямів спеціалізації) цих функціональних складових: інструментарію «м'якої сили» у міжнародній діяльності; структур інформаційного протиборства й контрпропаганди військових формувань та спеціальних служб; інститутів зв'язків з громадськістю; системи захисту інформаційно-когнітивної безпеки держави і суспільства.

Ключові слова: стратегічні комунікації, нормативні засади військової політики, безпекові концепції, інформаційне протиборство, іноземний досвід забезпечення безпеки.

The article analyzes the creation of the doctrinal and regulatory foundations of the strategic communications system as a new qualitative stage in the development of the sphere of information warfare and military-political communication in the activities of the North Atlantic Community. A fundamental revision of conceptual views on traditional methods, forms and methods of informational and psychological warfare is considered, which was reflected in the development of doctrinal foundations and the creation of a system of «strategic propaganda», or strategic communications, which was based on the transition from the separate application of specialized military and civilian structures to their close integration and coordination of activities in the information-cognitive space, including – in the conditions of crisis settlement, in conflicts of varying degrees of intensity. The study observes the development of conceptual views and normative guidelines for defining the components, functions, and organizational mechanism of strategic communications at the level of strategic documents of the military-political planning of the United States and the NATO bloc. The principles defined in NATO and the leading functional components of the implementation of strategic communications are highlighted.

According to the authors, the need to develop conceptual documents in the field of activity of the national system of strategic communications seems urgent. At the same time, it is necessary to determine its substantive priorities, mechanisms for coordinating the activities of the components of the STC system, as well as distinguishing the functions (directions of specialization) of these functional components: the toolkit of «soft power» in international activities; structures of information struggle and counter-propaganda of military formations and special services; public relations institutes; systems of protection of informational and cognitive security of the state and society.

Key words: strategic communications, normative principles of military policy, security concepts, information confrontation, foreign experience of security.

Творення системи стратегічних комунікацій (СТК) виступає важливою складової реформування сектору безпеки і оборони держави, забезпечення інформаційної безпеки держави та реформування інфраструктури інформаційно-когнітивного протиборства в Україні [про функції СТК в оборонно-безпековій сфері див. докладніше: 1-3]. Цілеспрямований розвиток системи СТК в Україні розпочався з 2014 р. у межах виконання рішень Уельського саміту НАТО та з консультативною й матеріально-технічною допомогою Альянсу, включаючи запровадження загальнодержавного центру стратегічних комунікацій і ситуаційних центрів у складі центральних органів влади. Поширення поняття й заходів, побудова структур, пов'язаних із явищем СТК, прискорилося Указом Президента України № 555/2015 «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року "Про нову редакцію Воєнної доктрини України"». Відповідно, у зміст дефініції «стратегічні комунікації» вкладалося скоординоване й належне використання комунікативних можливостей держави – публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави [4]. У вересні 2015 р. Україна і НАТО підписали Дорожню карту Партнерства у сфері стратегічних комунікацій, котра скеровувала на розбудову внутрішньовідомчих та міжвідомчих систем СТК, реалізацію національної стратегії СТК в Україні, а також *вдосконалення нормативних документів, що регламентують процес комунікації у структурах безпеки та оборони* [5, с. 98-99].

Відповідно, важливим науково-пізнавальним завданням стало вивчення зарубіжного досвіду нормативно-правового й концептуального регулювання розбудови системи стратегічних комунікацій, ініціаторами та розробни-

ками якої виступили провідні держави Північноатлантичного альянсу. Відповідно, в Україні в останнє десятиліття склався помітний міжвідомчий науковий напрям дослідження питань доктринального обґрунтування та практики творення органів СТК, імплементації зарубіжного досвіду до вітчизняної практики оборонно-безпекової діяльності, представлений працями таких провідних науковців як А. Баровська, А. Вербицька, О. Войтко, Т. Дзюба, Д. Дубов, О. Заруба, Л. Капштик, В. Кацалап, В. Панченко, В. Савченко, О. Сальнікова, Т. Сивак та інші [про наукові доробки з проблеми див.: 6-7].

Відбувається структурування дослідницького поля у галузі СТК, на якому виділяється створений у 2018 р. навчально-науковий підрозділ Національного університету оборони України (НУОУ), на базі якого створений (у 2023 р.) Інститут стратегічних комунікацій НУОУ, структуру якого утворюють кафедри: інформаційної боротьби; соціальної комунікації та публічної дипломатії; внутрішніх комунікацій; зв'язків з громадськістю, а також науково-дослідний відділ проблем розвитку та впровадження стратегічних комунікацій.

Відтак метою статті є аналіз творення доктринальних й нормативно-розпорядчих засад системи стратегічних комунікацій як нового якісного етапу розвитку сфери інформаційного протиборства та воєнно-політичної комунікації у діяльності Північноатлантичного співтовариства.

На межі XX/XXI століть в євроатлантичному середовищі відбувся докорінний перегляд концептуальних поглядів на традиційні способи, форми і методи інформаційно-психологічного протиборства, що знайшло відображення у розробці доктринальних засад й створенні системи «стратегічної пропаганди», або ж стратегічних комунікацій (Strategic Communications), в основі якої містився *перехід від окремішного застосування профільних військових і цивільних структур до їх тісної інтеграції та координації діяльності в інформаційно-когнітивному просторі*, у т.ч. – в умовах кризового врегулювання, у конфліктах різного ступеня інтенсивності.

Як вважають дослідники, гносеологічні й технологічні коріння стратегічних комунікацій (і перегляду традиційних форм і способів інформаційного протиборства) сягають т.зв. «всеохоплюючого підходу» (Comprehensive Approach) до врегулювання криз, в основі якого – забезпечення тісної узгодженості, синергії воєнних та цивільних інформаційних інструментів для досягнення глобальних цілей. Крім того, СТК стали дальшим розвитком доктрини «непрямих дій», сутність якої полягає у впливі на свідомість тих категорій населення, від яких залежить досягнення ключових суспільно-політичних інтересів, а також у тиску на ті управлінські ланки, зміни у яких породжували б ерозію всієї управлінської системи. Одночасно, сама нова термінологія була покликана камуфлювати застосування інформаційної зброї.

Зауважимо, що поняття «стратегічні комунікації» застосовувалося у дослідницьких документах Військового коледжу Армії США (здійснює навчання старшого офіцерського складу армії США, цивільного персоналу, офіцерів інших видів збройних сил країни, а також іноземних слухачів за програмою підготовки керівного складу) щонайменш від 1966 р. (тоді йшлося про забезпечення стратегічного рівня зв'язку під час масштабних воєнних конфліктів) [8, с. 11].

Властиво, що концептуальні підвалини СТК відпрацьовувалися і в умовах локальних війн та конфліктів за участю США і союзників по НАТО. Один із базових підходів до стратегії інформаційного протиборства США передбачав синергію залучення можливостей у всіх операційних середовищах, максимальну погодженість дій усіх сил і засобів інформаційного впливу, або ж дій в «єдиному інформаційному просторі». Повною мірою це знайшло втілення при розробці (апробуванні у конкретних воєнно-політичних умовах) механізмів творення міжвідомчих (багатовидових) угруповань із здійснення СТК, чия діяльність мала мінімізувати втрати власних військ та місцевого населення, викликати симпатії останнього та підштовхнути противника до відмови від спротиву.

В науковій літературі наводиться, зокрема, досвід пошуку організаційних форм скоординованих інформаційно-комунікаційних заходів як складової кампанії Міжнародних сил сприяння (ISAF) в Афганістані у 2001–2021 рр. Під час її проведення відповідні структури МО США налагодили співробітництво із урядом Афганістану, Управлінням адміністрації президента США з міжрелігійних ініціатив, Державним департаментом та ЦРУ США, Центром ім. Джорджа К. Маршалла, Агентством США з міжнародного розвитку, Радою управляючих з іноземного мовлення, делегацією Конгресу США в Афганістані, оперативним центром ЗМІ НАТО, місією ООН з надання допомоги в Афганістані.

Імовірно, прискорений розвиток теорії Страткому в НАТО розпочався після виявлення суттєвих недоліків у діяльності структур «публічної дипломатії» та воєнно-цивільної взаємодії із місцевим населенням в ході операції в Афганістан (2001–2021 рр.). Хоча під час кампанії в Афганістані вживалися численні заходи «воєнно-цивільної взаємодії», але не приділялося достатньої уваги світовій громадській думці, психологічні операції спрямовувалися, передусім, на підтримку бойових дій, а вплив на традиціоналістське цивільне населення ісламської, багатонаціональної країни недооцінювався [9, с. 151; 10, с. 76].

Як зазначають дослідники, помітну роль у розробці поняття СТК у сучасному змістовному наповненні відіграла Оборонна наукова рада (федеральний консультативний орган з незалежних консультацій) при МО США. Існує думка, що активізація ужитку поняття «стратегічні комунікації» у професійному обігу відбулася після 2001 р. – після оприлюднення доповіді Вінсента Вітто (голови згаданої наукової ради) «Звіт цільової групи Ради з оборонних наук щодо управління поширенням інформації». Йшлося про те, що складні стратегічні комунікації («sophisticated strategic communications») здатні створювати такий контекст, який сприятиме досягненню політичних, економічних та військових цілей. Одночасно вказувалося на ключові невирішені обставини, подолати які могло б запровадження системи стратегічних комунікацій: незадовільна координація інформаційних зусиль уряду США, розпорошеність фінансування та відсутність їх інтеграції в загальну стратегію і плани забезпечення національної безпеки. У 2004 р. згадана Оборонна наукова рада МО США у «Заключному звіті Оперативної групи Оборонної наукової ради зі стратегічних комунікацій» дала визначення Страткому як «багатоманіттю інструментів, що використовуються державою для генерування розуміння глобальних відносин та культур», впливу на свідомість і поведінку людських спільнот «за допомогою комунікативних стратегій» [11, с. 166]. Надалі словник військових та асоційованих термінів МО США потрактував стратегічні комунікації як зосередження скоординованих зусиль уряду та всіх інструментів державної влади на залученні ключових аудиторій задля створення сприятливих умов для просування державних інтересів США [12].

В 2006 р. вийшла директива Пентагону «Дорожня карта стратегічної пропаганди». В цілому концептуальні документи НАТО передбачали розширення можливостей із проведення інформаційно-психологічних операцій та впливу на формування суспільних настроїв як складової вирішення ключових воєнно-політичних завдань. Визначилася і сутність СТК, яка полягала у прагненні *досягти військово-політичні цілі переважно невоєнними способами, що вимагало виведення системи інформаційно-психологічного впливу сил НАТО на новий якісний рівень – у статусі одного із провідних видів забезпечення військових дій* за рахунок запровадження сучасних соціальних технологій та синергії взаємодії усіх військових та цивільних інформаційно-про-

пагандистських структур. Віхою на шляху концептуалізації СТК стала поява 31 жовтня 2007 р. директиви «Удосконалення стратегічних комунікацій НАТО» (Enhancing NATO's Strategic Communications), а у 2008 р. – директиви щодо стратегічних комунікацій Штабу Верховного головнокомандувача ОЗС НАТО в Європі. Тоді ж положення про стратегічні комунікації потрапило до політичного документу Альянсу – Декларації саміту НАТО [10, с. 73-75].

Вважається, що вперше інструментарій стратегічних комунікацій було офіційно окреслено у 2009 р. генеральним секретарем Ради НАТО А. Расмусеном: Стратком це «скоординоване і належне використання комунікативних можливостей і діяльності НАТО – публічної дипломатії, зв'язків із громадськістю, військових зв'язків із громадськістю, інформаційних та психологічних операцій у разі необхідності підтримки політики Альянсу, операцій і заходів та з метою просування цілей НАТО». Таке саме визначення закріпили і у концептуальному документі від вересня 2009 р. – «Політика стратегічних комунікацій НАТО» [13].

У 2011–2012 рр. тема СТК (у сучасній її інтерпретації) стала предметом аналізу низки провідних аналітичних центрів євроатлантичного світу: корпорації RAND (у доповіді «Стаючи кращими у стратегічних комунікаціях») та у документі «Стратегічні комунікації та національна стратегія» Королівського інституту міжнародних відносин (Chattem House). Поступово концептуальне бачення СТК закріплюється і в офіційних документах військового відомства США як от «Доповідь щодо стратегічних комунікацій» департаменту оборони Пентагону та у розробках щодо інформаційної діяльності як засобу врегулювання локальних конфліктів за участю сил НАТО («Виграти війну історій: стратегічні комунікації та конфлікт в Афганістані», «Стратегічні комунікації: більше має бути зроблено») [1, с. 14-16].

Перспективне бачення системи СТК виклали експерти робочої групи з підготовки доповіді щодо впровадження «Стратегічної концепції НАТО–2030»:

Альянс має прискорити трансформацію своїх стратегічних комунікацій для забезпечення ефективнішої конкуренції у сучасному динамічному інформаційному середовищі;

надати пріоритет цифровим технологіям у реалізації зусиль із трансформації комунікацій;

вжити додаткових активних заходів задля інформування своїх громадян та підтримки операцій й діяльності Альянсу;

активізувати співпрацю з країнами-партнерами, міжнародними та неурядовими організаціями, аналітичними центрами і науковими колами у вирішенні проблем протидії дезінформації [14, с. 13].

В євроатлантичному концептуальному просторі утвердилося *тлумачення стратегічних комунікацій* як цілеспрямованих зусиль воєнно-політичного проводу країни (блоків держав) із створення, підтримки або покращання сприятливих умов для просування національних інтересів, проведення політичного курсу шляхом впливу на свідомість визначеної аудиторії на основі використання скоординованих програм, планів, тематики обговорення та інформаційних повідомлень, узгоджених з діями всіх інструментів реалізації національних інтересів (спрямувань) держави» [15].

Планування мало здійснюватися на основі таких *принципів СТК*:

- *кваліфіковане централізоване керівництво* – інтегровану систему управління силами і засобами СТК на основі чіткого розуміння персоналом цілей, завдань та особливостей діяльності;
- *цілеспрямованість*, котра розуміється як підпорядкованість цілей і завдань СТК задуму військової операції, концентрація зусиль на пріоритетних завданнях, цільових аудиторіях, територіях, об'єктах тощо;
- *узгодженість дій*, яка полягає у координації заходів всіх залучених профільних військових й громадянських структур навколо єдиного задуму й загального плану;
- *оперативність*, що вимагає належної спрямованості, обсягу та термінів, високої активності та гнучкості у реагуванні на перебіг подій, виборі аудиторії тощо;
- *неперервність* передбачає постійний та системний вплив на цільові аудиторії, необхідне корегування форм, методів і масштабів застосування сил і засобів інформаційно-психологічного впливу;
- *достовірність інформації* тлумачиться як правдоподібна інтерпретація дій НАТО в інтересах завоювання довіри цільових аудиторій, підтримання сталих зв'язків із громадськістю та конструктивних відносин із медіасферою;
- *переконливість подання*, яка досягається шляхом раціонального добору й використання необхідних засобів переконання й навіювання.

Концептуальні документи НАТО визначили і *комплекс вимог до змісту й результатів стратегічних комунікацій*:

- формування позитивного іміджу Альянсу та підтримання високого авторитету його збройних сил в районах проведення операцій, у т.ч. за рахунок адекватного визначення цільових настанов інформаційної діяльності;
- забезпечення ідентичності змісту власної пропаганди та контенту зовнішніх інформаційних агентств (у т.ч. інформації стосовно операцій та навчань ОЗС НАТО) за рахунок узгодження планів дій та обміну інформацією;
- створення сприятливих умов для ефективного впливу на цільові аудиторії, вивчення й оцінка власних та суспільних інформаційних систем;
- протидія ворожій пропаганді шляхом контролю й нейтралізації дій зовнішніх інформаційних структур;
- оцінювання ефективності інформаційно-психологічних заходів НАТО через постійний аналіз і моніторинг суспільної думки, проведення відповідних досліджень ефективності впливів на цільові аудиторії;
- забезпечення швидкої розробки й своєчасного поширення інформації шляхом вибору найбільш достовірних джерел, розвитку співробітництва з відповідними ЗМІ та громадськими організаціями.

Визначалися і *провідні функціональні складові реалізації стратегічних комунікацій*:

- *проведення психологічних операцій* (Psychological Operations), тобто комплексу спланованих дій з доведення спеціально підготовленої інформації іноземній аудиторії з метою впливу на її свідомість, світобачення, емоції, що має призвести до зміни поведінки урядів, соціальних спільнот та окремих значущих особистостей у необхідному для себе напрямку;
- *введення противника в оману*, або дезінформування (Deception), під яким розуміється керований (випереджувальний) інформаційно-психологічний вплив на політичні, управлінські, командно-штабні структури через системи цілеспрямованого розподілення інформації та шляхом просування завідомо хибної, сфабрикованої інформації;
- застосування по відношенню до адресних аудиторій інформаційно-політичних *механізмів публічної дипломатії* (Public Diplomacy), спрямованих іноземних політичних лідерів, парламентарів, журналістів, неурядові організації, певні соціальні спільноти, науково-експертні кола з метою формування вигідного для блоку ставлення до його воєнно-політичних дій, підтримання лояльного ставлення до контингентів НАТО з боку місцевого населення;
- *зв'язки з громадськістю* (Civil Affairs), спрямовані на суспільно-інформаційний вплив на широкі прошарки населення країн (регіонів) зацікавленості Альянсу. Розрізнялися рівні таких контактів: загальноцивільний, що передбачає вплив через медіа та інші канали на цивільно-адміністративні структури з метою роз'яснення політики НАТО із розв'язання кризових ситуацій, налагодження ділових контактів з місцевими державними органами, громадянським сектором, бізнесом, інтелектуальними колами; воєнний рівень роботи з громадськістю, спрямований на забезпечення антикризових операцій, взаємодію із ЗМІ через інформаційні мережі тощо;

• *воєнно-цивільна взаємодія,* між командуванням ОЗС НАТО і місцевими військовими структурами, цивільними органами влади, населенням, неурядовими організаціями, яка спрямована на досягнення таких завдань: використання ресурсів країни у інтересах контингентів НАТО; надання допомоги національним органам влади у реформуванні системи державного управління, збройних сил та органів безпеки, створенні громадянського суспільства; цілеспрямоване інформування населення та гуманітарно-культурна діяльність тощо;

• *оперативне маскування* (Operations Security) – сукупність інформаційних та організаційно-технічних заходів із дезорієнтації розвідувальних органів противника з метою забезпечення прихованості дій власних сил. Ефективними засобами впливу на цільову аудиторію вважаються при цьому дезінформування, імітація дій власних сил, демонстрування хибних розвідувальних ознак;

• *організація радіоелектронної боротьби* (Electronic Warfare, РЕБ) з метою виявлення та придушення (у т.ч. – із сполученням із вогневими ударами) органів і засобів управління противника, дезорганізації або нейтралізації бойової спроможності противника з ефективного використання радіоелектронних систем управління, захисту власних сил от радіоелектронного ураження. РЕБ включає радіоелектронне придушення, радіоелектронний захист та радіоелектронне забезпечення;

• *ведення контрпропаганди* (Counter-Propaganda), яка розглядається як комплексні коаліційні зусилля з проведення інформаційних та психологічних операцій із зниження ефективності або нейтралізації подібних заходів противника шляхом розкриття планів протилежної сторони із впливу на війська та населення країн НАТО, їх партнерів, організації протидії ворожим пропагандистським акціям;

• сприяння виводу із *ладу об'єктів інформаційної інфраструктури противника* (Physical Destruction), який здійснюється застосуванням апаратно-програмних засобів із метою дезорганізації систем управління противника, та фізичного знищення критично важливих об'єктів його інформаційної інфраструктури;

• реалізація *операцій в комп'ютерних мережах* (Computer Network Operations) шляхом проведення кібероперації, об'єктами яких ставали б комп'ютерні й телекомунікаційні мережі;

• *забезпечення безпеки власних інформаційних систем* (Information Security), значення й технічні можливості якої неухильно зростають. Згідно новітнім поглядам теоретиків СТК, безпека має бути комплексом заходів із захисту інформації та інформаційних систем, при збереженні їх доступності, цілісності, автентичності, конфіденційності та авторизації [див.: 17].

В країнах Європейського Союзу та їх провідних науково-аналітичних центрах з 2015 р. поштовх до визначення концептуальних засад СТК надала розробка «Глобальної стратегії зовнішньої політики і безпеки ЄС». В її рамках у червні 2016 р. побачив світ документ під назвою «Спільне бачення, спільні дії: сильніша Європа», котрий визначив п'ять пріоритетів зовнішньої політики ЄС: безпека ЄС, боротьба з тероризмом, кібербезпека, енергетична безпека та стратегічні комунікації. Як зазначалося у згаданій «Глобальній стратегії», СТК передбачали розвиток публічної дипломатії, активізацію контактів між державними структурами та громадянською спільнотою і соціальними медіа, заходи із оперативного спростування дезінформації, забезпечення відкритості суспільства.

У «Спільній рамочній програмі ЄС щодо протидії гібридним загрозам» (6 квітня 2016 р.) наголошувалося на небезпеці гібридних загроз, серед яких називалися поширення дезінформації та дестабілізаційних кампаній в соціальних мережах, перехоплення змісту основних суспільних наративів, що потребує підвищення рівня поінформованості соціуму про гібридні загрози. Підкреслювалася важливість посилення співробітництва та координації діяльності між ЄС та НАТО у сфері стратегічних комунікацій, кібербезпеки і протидії гібридним загрозам. Держави-члени, щоб викрити гібридні загрози, повинні були розробити координаційні механізми стратегічних комунікацій для відсічі дезінформації. Зазначалося, що Європейська служба зовнішніх зв'язків має енергійно використовувати друковані ЗМІ, візуальні та аудіо медіа, соціальні мережі. 23 листопада 2016 р. Європейський парламент схвалив резолюцію під назвою «Стратегічні комунікації ЄС як протидія пропаганді третіх сторін» [див.: 17, с. 107-108].

Отже, нагальною видається необхідність розробки концептуальних документів у галузі діяльності національної системи стратегічних комунікацій. При цьому потребують визначення її змістовні пріоритети, механізми координації діяльності складових системи СТК, а також виокремлення функцій (напрямів спеціалізації) цих функціональних складових: інструментарію «м'якої сили» у міжнародній діяльності; структур інформаційного протиборства й контрпропаганди військових формувань та спеціальних служб; інститутів зв'язків з громадськістю; системи захисту інформаційно-когнітивної безпеки держави і суспільства.

ЛІТЕРАТУРА

1. Сивак Т.В. Стратегічні комунікації у системі публічного управління України: монографія. Київ: НАДУ, 2019. 338 с.
2. Капштик О. В. Поняття і сутність стратегічних комунікацій як засобу забезпечення національної безпеки. *Інвестиції: практика та досвід.* 2018. № 16. С. 109–113.
3. Кушнір О.В. Поняття та сутність стратегічних комунікацій у сучасному українському державотворенні. *Право і суспільство.* 2015. № 6. С. 27–31.
4. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» від 28 грудня 2021 р. № 685/2021. URL: https://www.president.gov.ua/documents/3922020-35037
5. Капштик О. В. Характеристика державних механізмів стратегічних комунікацій у секторі безпеки і оборони України. *Інвестиції: практика та досвід.* 2018. № 17. С. 97–101.
6. Наукове забезпечення стратегічних комунікацій в секторі безпеки і оборони України : бібліограф. огляд / упоряд. І. М. Жовтенко, Т. В. Дорошенко. Київ : НА СБ України, 2023. 260 с.
7. Вєдєнєєв Д.В., Семенюк О.Г. Розвиток в Україні науково-концептуальних та організаційно-функціональних засад протидії інформаційно-психологічній зброї як знаряддю гібридної конфліктності. Монографія. К.: ДП «Інфотек», 2022. 256 с.
8. Дубов Д.В. Стратегічні комунікації: проблеми концептуалізації та практичної реалізації. *Стратегічні пріоритети.* № 4. 2016. С. 9–23.
9. Баровська А.В. Стратегічні комунікації: досвід НАТО. *Стратегічні пріоритети.* 2015. № 1. С. 147–151.
10. Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп. К. : НІСД, 2016. 109 с.
11. Соловйов С. Г. Основні характеристики стратегічних комунікацій. *Вісник Національного університету цивільного захисту України.* Серія: Державне управління. 2016. Вип. 1. С.165–170.
12. Joint Chief of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, April 12, 2001 (as amended through March 4, 2008). P.230. URL: https://irp.fas.org/doddir/dod/jp1_02.pdf
13. NATO Strategic Communications Policy. URL: http://info.publicintelligence.net/ NATO STRATCOM Policy.pdf.
14. Стратегічні комунікації для безпекових і державних інституцій : практичний посібник / [Л. Компанцева, О. Заруба, С. Череватий, О. Акульшин]. Київ: ТОВ «ВІСТКА», 2022. 278 с.
15. NATO strategic communications. An evolving battle of narratives response URL: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/586600/EPRS_BRI (2016)586600_EN.pdf 24. NATO strategic communications
16. Основи стратегічних комунікацій у сфері забезпечення національної безпеки та оборони: навч. посіб. К.: НУОУ імені Івана Черняховського, 2020. 85 с.
17. Тихомирова Є. Стратегічні комунікації ЄС: інституціональний вимір. *Політичні проблеми міжнародних систем та глобального розвитку.* 2016. № 4. С. 103–109.

УДК 340+35.078.3
DOI https://doi.org/10.32782/2524-0374/2024-3/3

СУТНІСТЬ ПРАВОВОЇ ПРИРОДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

THE ESSENCE OF THE LEGAL NATURE OF INFORMATION SECURITY

Гончаров М.В., доктор філософії

У статті розглянуто сутність правової природи інформаційної безпеки з позицій різних дослідників. Проведений аналіз наукових джерел дозволив виявити, що правова природа інформаційної безпеки в цілому, так і на елементному рівні характеризується науковістю, системністю та має багато аспектів.

Дослідження цілісного поняття «інформаційна безпека» вимагає застосування комплексного підходу до розуміння значення (семасіології) кожного терміну, який його формує («інформація і безпека»). При цьому необхідно зауважити, що термін «інформація» застосовується не як системоутворююча складова, а вживається для означення якісної характеристики базового елемента, тобто категорії «безпека», що розкриває галузеве спрямування і змістовне наповнення заходів, та створює відповідне поле нормативно-правового регулювання.

Для розуміння об'єктивного змісту цілісного поняття «інформаційна безпека» послуговуватимемося можливостями окремих методологічних інструментів (в основному, аналізу, синтезу та ін.), які сприятимуть вивченню глибинних діалектичних зв'язків між визначеними категоріями, що його формують.

Акцентовано увагу на основних завданнях державної інформаційної політики та з'ясована мета політики забезпечення інформаційної безпеки України, це формування відкритого інформаційного суспільства, як простору цілісної держави, інтегрувального в світовий інформаційний простір з урахуванням національних особливостей і інтересів при забезпеченні інформаційної безпеки на внутрішньодержавному та міжнародному рівнях.

Державна політика забезпечення інформаційної безпеки повинна базуватися на наукових і методологічних розробках, систематизованих і об'єднаних в єдину концепцію. Вона може бути представлена як сукупність національних цілей, інтересів і цінностей; стратегії та тактики управлінських рішень і методів їх реалізації, що розробляються та реалізуються державною владою.

Ключові слова: інформаційна безпека України, забезпечення інформаційної безпеки, національна безпека, система, державна інформаційна політика.

The article examines the essence of the legal nature of information security from the standpoint of various researchers. The analysis of scientific sources made it possible to reveal that the legal nature of information security in general, as well as at the elemental level, is characterized by scientificity, systematicity and has many aspects.

The study of the integral concept of «information security» requires the application of a complex approach to understanding the meaning (semasiology) of each term that forms it («information and security»). At the same time, it should be noted that the term «information» is not used as a system-forming component, but is used to denote the qualitative characteristics of the basic element, that is, the category «security», which reveals the industry direction and content of measures, and creates a corresponding field of regulatory and legal regulation.

In order to understand the objective content of the integral concept of «information security», we will use the possibilities of separate methodological tools (mainly, analysis, synthesis, etc.), which will contribute to the study of deep dialectical connections between the defined categories that form it.

Attention is focused on the main tasks of the state information policy and the goal of the policy of ensuring information security of Ukraine is clarified, which is the formation of an open information society as a space of an integral state, integrating into the global information space, taking into account national characteristics and interests while ensuring information security at the domestic and international levels.

The state policy of ensuring information security should be based on scientific and methodological developments, systematized and combined into a single concept. It can be presented as a set of national goals, interests and values; strategies and tactics of management decisions and methods of their implementation, which are developed and implemented by the state authorities.

Key words: information security of Ukraine, provision of information security, national security, system, state information policy.

Постановка проблеми. Актуальність теми дослідження визначається важливим значенням інформаційної сфери для задоволення не тільки потреб суспільства у передаванні і зберіганні відомостей, а й для виконання однієї з найважливіших функцій держави – забезпечення національної безпеки України. На сьогоднішній день забезпечення інформаційної безпеки в Україні полягає у здатності нашої країни захищати національні економічні інтереси від зовнішніх і внутрішніх загроз, також спроможності національної економіки зберігати й поновлювати процес суспільного відтворення.

Необхідною умовою розвитку сучасного суспільства є високий рівень інформаційної безпеки. Саме тому ефективне здійснення правового регулювання інформаційними ресурсами є важливою умовою забезпечення інформаційної безпеки та реалізації виваженої державної політики.

Стан опрацювання цієї проблематики. Вивченню даного питання приділяли увагу багато науковців та дослідників: Біленчук П. Д., Білько С. С., Гнатюк С. Л., Григорчук М. В., Дзьобань О. П., Довгань О. Д., Золотар О. О., Косілова О. І., Кудін С. В., Ліпкан В. А., Логінов О. В., Новицька Н. Б., Ткачук Т. Ю., Тихомиров О. О., Француз А. Й., Цимбалюк В. С., Шевченко А. Є., Ярема О. Г. та інші.

Мета статті – розглянути тенденції наукових поглядів сутності інформаційної безпеки України.

Виклад основного матеріалу. З метою забезпечення комплексного підходу до виконання завдань нашого наукового дослідження звертаємося до джерельної науково-практичної бази у сфері інформаційної безпеки України. Це означає, що емпіричною базою для такого аналізу слугуватимуть опрацьовані нами джерела без градації на галузеву приналежність.

О. Д. Довгань, Т. Ю. Ткачук, досліджуючи історичні аспекти та джерела оприлюднення перших згадувань про інформаційну безпеку, зазначають: «Проблематика інформаційної безпеки та її забезпечення у різних аспектах висвітлювались у наукових працях Плутарха, Сенеки, Платона, Макіавеллі, Гроція, а також інших вітчизняних та зарубіжних дослідників» [1, с. 80].

Як вбачається з наведеної вище цитати, логічним висновком є те, що сфера інформаційної безпеки ще в ранні часи набула дуалістичного характеру. Причиною цьому, на наш погляд, є те, що вказані вчені мали визначні досягнення не тільки в юриспруденції, а й у філософії. Тому виведені ними узагальнення поєднують у собі юридичну і філософську компоненту.

О. О. Золотар, досліджуючи першоджерела інформаційної безпеки, зазначає, що «початок історії захисту

інформації вчені пов'язують з появою можливості фіксації інформаційних повідомлень на твердих носіях, тобто з винаходом писемності, а першим видом інформації, що підлягала захисту, вважають державну таємницю» [2, с. 140].

На думку науковця, майже одночасно з винайденням писемності були відкриті методи і способи захисту інформації, а саме шифрування і приховування. Як приклад О. О. Золотар наводить історичний факт, що засвідчує спосіб захисту інформації від стороннього доступу і поширення. Такий випадок відомий як перший шифрований текст, прихований під рецептом глазурі при нанесенні її на вироби гончарства (Месопотамія, 2000 років до н. е.).

Відомі наукові погляди щодо розуміння та формування парадигми інформаційної безпеки мають в основі широку палітру філософського знання, що сягає своїм корінням глибокої давнини. Філософи минувшини завжди досліджували причини і джерела загроз, намагалися домогтися стабільного миру та процвітання. За таких умов трансформувалися підходи до розуміння інформації. Питання безпеки особи, суспільства, держави та отримання достовірної інформації цікавили мислителів Стародавнього світу. Щоправда, вказана проблема розглядалася переважно в контексті війни й миру [3, с. 40].

О. Курбан, досліджуючи генезу інформаційного впливу в XVIII столітті на прикладі боротьби за незалежність мешканців північноамериканських колоній, зазначає: «У своїй боротьбі колоністи використовували соціальні мережі (товариства «Сини свободи», «Кореспондентські комітети»), застосовували образні символи («дерево свободи», стереотипи та лозунги «Воля або смерть»). Вони дуже активно застосовували дієві акції, тогочасні медіа, чутки, маніпуляцію» [4, с. 30].

О. П. Дзьобань, досліджуючи наукову спадщину Томаса Гоббса та Еммануїла Канта, зазначає, що «наукове обґрунтування проблеми національної безпеки взагалі, й інформаційних її аспектів зокрема, в сучасному розумінні й певні напрямки її вирішення містяться у працях вказаних науковців» [5, с. 41].

О. Павленко, вивчаючи генезу інформаційної безпеки, здійснила аналіз історичних джерел виникнення і розвитку цієї галузі права, і запропонувала його поділ на етапи:

I етап – до 1816 року – характеризується використанням природно виникаючих засобів інформаційних комунікацій. Для цього періоду основним завданням збереження відомостей полягало в недопущенні сторонніх осіб до володіння інформацією про факти, майно, події тощо, які мали для людини чи колективу людей важливе, а в окремих випадках – життєве значення.

II етап – починаючи з 1816 року – пов'язаний з початком використання штучно створюваних технічних засобів електро- і радіозв'язку. Поряд з використання досвіду попереднього періоду застосовувалися такі інструменти захисту інформації, як «перешкодостійке кодування повідомлення (сигналу) з подальшим декодуванням прийнятого повідомлення (сигналу)».

III етап – починаючи з 1935 року – пов'язаний з появою засобів радіолокацій і гідроакустики. У цей період головним напрямком у сфері захисту інформації було забезпечити приймальні пристрої радіолокаційних систем «активними маскуючими і пасивними імітуючими радіоелектронними перешкодами».

IV етап – починаючи з 1946 року – пов'язаний з винаходом і впровадженням у практичну діяльність електронно-обчислювальних машин (комп'ютерів). Для даного етапу характерним виступало фізичне обмеження доступу сторонніх осіб до устаткування, на якому зберігалася інформація.

V етап – починаючи з 1965 року – обумовлений створенням і розвитком локальних інформаційно-комунікаційних мереж. Завданнями інформаційної безпеки зазначеного періоду були забезпечити ефективне збереження інформації шляхом фізичного захисту джерел (носіїв) інформації.

VI етап – починаючи з 1973 року – пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань. З урахуванням технологічних проривів загрози інформаційній безпеці ставали дедалі серйознішими, що вимагало розроблення відповідних систем захисту від несанкціонованого втручання (хакерства) у порядок використання інформаційних ресурсів. У цей час починає формалізуватися інформаційне право як нова галузь міждержавної правової сфери.

VII етап – починаючи з 1985 року – пов'язаний зі створенням і розвитком глобальних інформаційно-комунікаційних мереж з використанням космічних засобів забезпечення [6].

Колектив науковців, серед яких А. Б. Тоцький, О. І. Тимошенко, А. М. Гуз, вважають, що історія охорони і захисту інформації на території сучасної України також сягає ще додержавних часів. Першим видом інформації, яку потрібно було охороняти, була військова інформація. Спочатку охорону такої інформації забезпечував князь, потім особа, яку він призначав особисто. Війна була на той час головним і загальновизнаним способом ведення зовнішньої політики будь-якої держави, тому захист військової інформації був головним у політиці князів Олега, Ігоря, Святослава, Ярослава та княгині Ольги. Князі, йдучи в похід, намагалися приховати інформацію про кількість війська і напрям головного удару. Ворог не міг адекватно реагувати на небезпеку, а заздалегідь розпущені чутки, перебільшення і неправдива інформація ще більше призводили до паніки [7, с. 11].

У контексті сказаного вище доцільно навести озвучений результат наукової розвідки колективу у складі В. М. Петрик, А. М. Кузьменко, В. В. Остроухов, які віднайшли одне з первинних документальних свідчень про застосування інформації з метою обману ворогів при провадженні воєнних дій. Науковці зазначають, що до XIII ст. належить один з перших історичних прикладів масштабного застосування дезінформації у воєнних цілях. Пов'язаний цей приклад із вторгненням монголів до Угорщини у 1241 р. [8, с. 56]. Монголи розбили військо угорців та їх союзників на річці Шайо і при цьому серед трофеїв виявили королівську печатку. Хан Батий наказав підготувати наказ угорською мовою від імені короля Бели про припинення опору, скріпивши його захопленою королівською печаткою. Цей документ розіслали в різні частини ще не завойованої країни, що сприяло введенню в оману угорської армії.

Окремо слід вирізнити напрацювання у цій галузі права закордонних науковців, так, Роберт Оуен уважав, що «тільки звільнення народів від приватновласницького ярма й об'єднання їх в один союз покладе край насильству й уможливить забезпечення безпеки [9, с. 375]. На думку відомого філософа й економіста, справжній безпековий стан як вселюдська гармонія можливий лише за умови організованого виховання населення при застосуванні інформаційних інструментів виховного характеру.

Ю. М. Канигін та В. І. Кушерець вважають, що «суспільство з великим запізненням починає осмислювати політичні, економічні, соціальні, військові, психологічні та інші наслідки глобальної інформатизації» [10, с. 35].

Вважається, що одними з перших проблеми комп'ютерної інформаційної безпеки усвідомили і зробили впевнений крок до їх вирішення державні відомства США в кінці 60-х років XX століття, коли комп'ютери коштували великих грошей, а інтернет зароджувалася з нечисленних, виключно військових і наукових інформаційних мереж.

Українська історія також зберегла свідчення про факти використання інформації як для доведення до відома

ворога неправдивих відомостей, та і для організації протидії внутрішнім загрозам щодо недопущення витоку секретної інформації.

Так, у матеріалах раніше згадуваного доробку авторського колективу за участі А. Б. Тоцького, О. І. Тимошенко, А. М. Гуз, знаходимо відомості про те, що у Запорізькій Січі та державі Богдана Хмельницького вироблені були своєрідні форми захисту військово-політичної інформації. Хмельницький широко використовував дезінформацію. В спогадах польських урядовців та військових часто зустрічається рядки на кшталт «одне думає, про інше пише», «наміри його жодним чином не можна зрозуміти». Хмельницький зазначав у жовтні 1648 р.: «А військова справа така: коли мисль буде йти на війну, щоб тої мислі ніхто не відав і недруг би остерігався» [7, с. 14].

Основною метою зловмисників завжди буває порушення складових інформаційної безпеки – доступності, цілісності або конфіденційності.

С. О. Лисенко: Серед останніх новацій із-за кордону варто зазначити, що 15 липня 2016 року німецький уряд затвердив план «Біла книга» з питань оборонної політики та безпеки, в тому числі інформаційної. В ній чітко вказано, що Російська Федерація стала реальною загрозою, що шкодить існуючому міжнародному порядку та європейській безпеці.

Поточним підсумком до вищесказаного є те, що сучасний стан і розуміння значення інформаційної безпеки нерозривно пов'язані з тими наріжними каміннями, на яких виникла і ґрунтується державна політика у сфері забезпечення як національного, так і міжсуб'єктного спілкування з дотримання межових знаків, встановлених як допустимі норми освідомлення з приватно-державними процесами конкретних національних утворень.

Показовими у цій ситуації є висновки, озвучені С. О. Лисенко за результатами дослідження історичних аспектів інформаційної безпеки як сфери спеціальних правовідносин. Науковець зазначає, що в ситуації, що склалась, правомірно «задекларована необхідність підвищення загальної інформаційної захищеності всього блоку НАТО… [11, с. 23–25]. При цьому науковець відзначає надзвичайну потребу у створенні Європейської ПРО, а також висловлюється про необхідність удосконалення механізмів захисту інформаційного поля. Такий підхід можна пояснити необхідністю створення оновленої системи захисту інформації між країнами НАТО.

Висновки. Як вбачається з вищенаведеного, інформація не існує відособлено від людського середовища і має конкретну мету, з якою впливає на суспільство. Здійснене дослідження підтвердило науково-практичну тезу про те, що на різних етапах розвитку суспільства рівень інформаційного впливу на людей напряму залежав від розвитку інструментів інформаційного впливу. Саме для розв'язання окремих завдань нашого дослідження ми торкнулися генезуальних проблем у підходах до розуміння правової природи інформаційної безпеки. На наш погляд, фундаментальними засадами виникнення у зародковому стані понять, які сьогодні визначені як інформаційна безпека, є звичаєве право, елементи якого у процесах розвитку цивілізації набули загальнообов'язкового характеру для їх учасників на підґрунті запровадження нормативно-правового регулювання цієї сфери.

ЛІТЕРАТУРА

1. Довгань О. Д., Ткачук Т. Ю. Наукова рефлексія інформаційної безпеки України: від позитивізму до метафізики права. *Інформація і право*. 2018. № 4 (27). С. 79–89.
2. Золотар О. О. Генеза суспільних відносин щодо інформаційної безпеки людини. *Інформація і право*. 2018. № 1 (24). С. 139–148.
3. Псалтир. Харків: Фоліо, 2013. 574 с.
4. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі. Київ, 2016. 286 с.
5. Дзьобань О. П. Національна безпека України: концептуальні засади та світоглядний сенс: монографія. Харків: Майдан, 2007. 284 с.
6. Павленко О. Історія виникнення інформаційної безпеки. URL : https://www.sutori.com/en/story/istoriia-vinikniennia-informatsiinoyi-biezpieki-94qRpbMUisHMP2JQSCupsNrN.
7. Організаційно-правові основи захисту інформації з обмеженим доступом : навч. посіб. [А. Б. Тоцький, О. І. Тимошенко, А. М. Гуз та ін.]. Київ : Європейський університет, 2006. 232 с.
8. Соціально-правові основи інформаційної безпеки. [В. М. Петрик, А. М. Кузьменко, В. В. Остроухов та ін.] : навч. посіб. [за ред. В. В. Остроухова]. Київ : Росава, 2007. 496 с.
9. Оуен Р. Організаційна поведінка в освіті: Керівництво учбовими закладами та шкільна реформа. [пер. з англ. О. В. Христенко]. Харків: Каравела, 2003. 488 с.
10. Канигін Ю. М., Кушерець В. І. Біблія та майбутнє науки: орієнтири сучасних знань. Київ: Т-во «Знання України», 2009. 163 с.
11. Гончаров М. В. Теоретико-правові основи регулювання інформаційної безпеки в Україні: дис. … канд. юрид. наук: 12.00.01. Ірпінь, 2023. 215 с.