УДК 323.28:004(045)
DOI https://doi.org/10.32782/2663-6170/2023.33.2

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В ІНФОРМАЦІЙНО БЕЗПЕКОВОМУ ВИМІРІ

THEORETICAL AND METHODOLOGICAL ASPECTS OF THE RESEARCH OF THE INFORMATION SOCIETY IN THE INFORMATION SECURITY DIMENSION

Воробець Н.Р.,
аспірант кафедри політології
Прикарпатського національного університету імені Василя Стефаника

Дана наукова стаття розглядає теоретико-методологічні аспекти дослідження інформаційного суспільства в інформаційно безпековому вимірі. В контексті швидкого розвитку інформаційних технологій актуальність дослідження інформаційної безпеки неоспорима. У статті розглядаються проблеми, пов'язані з поняттям інформаційного суспільства та його структурою, а також проаналізовано загрози, що виникають в інформаційному просторі. У статті розглянуто сучасний стан розвитку інформаційних технологій та їх вплив на розвиток інформаційного суспільства. Зокрема, розглядається взаємозв'язок між інформаційним суспільством та державною політикою в галузі інформаційної безпеки.

Стаття відділяє важливість застосування теорій, які вивчають суспільство з позиції інформаційних технологій та їх взаємодії з людьми. Вона також розглядає методологічні підходи до дослідження інформаційного суспільства в контексті його взаємодії з інформаційною безпекою та розробки стратегій її забезпечення. Також наголошується на важливості розуміння взаємозв'язку між інформаційною безпекою та правами та свободами людини в інформаційному суспільстві.

Розглянуто важливість таких основних компонентів як соціальний та політичний аспект у вивченні та дослідженні інформаційної безпеки в Україні, оскільки інформаційна безпека України не може бути досягнута без забезпечення безпеки суспільства та безпеки політичних процесів. Зокрема розглянуто вплив інформаційних технологій на політичні процеси в країні. Крім того, стаття пропонує ряд рекомендацій щодо подальшого дослідження інформаційного суспільства в інформаційно безпековому вимірі.

Результати цього дослідження можуть бути корисними у подальших дослідженнях з даної проблематики, може використовуватися як методологічна база подальшого опрацювання проблем інформаційної безпеки, а також у навчальному процесі.

Ключові слова: інформаційна безпека, інформаційне суспільство, медіаграмотність, Інтернет, державна політика, теоретико-методологічні аспекти.

This scientific article considers the theoretical and methodological aspects of information society research in the information security dimension. In the context of the rapid development of information technologies, the relevance of information security research is undeniable. The article examines the problems related to the concept of the information society and its structure, and also analyzes the threats arising in the information space. The article examines the current state of the development of information technologies and their impact on the development of the information society. In particular, the relationship between the information society and the state policy in the field of information security is considered.

The article highlights the importance of applying theories that study society from the standpoint of information technologies and their interaction with people. It also considers methodological approaches to the study of the information society in the context of its interaction with information security and the development of strategies for its provision. The importance of understanding the relationship between information security and human rights and freedoms in the information society is also emphasized.

The importance of such basic components as the social and political aspect in the study and research of information security in Ukraine is considered, since the information security of Ukraine cannot be achieved without ensuring the security of society and the security of political processes. In particular, the influence of information technologies on political processes in the country is considered. In addition, the article offers a number of recommendations for further research of the information society in the information security dimension.

The results of this study can be useful in further research on this issue, can be used as a methodological basis for further processing of information security problems, as well as in the educational process.

Key words: information security, information society, media literacy, Internet, state policy, theoretical and methodological aspects.

Постановка проблеми. Інформаційна безпека – одна з ключових сфер державної безпеки, що має стратегічне значення для України. Розвиток та удосконалення технологій та відкритих мереж зв'язку призвели до того, що не лише засоби масової інформації, але й засоби персональної комунікації перестають бути розділені державними кордонами й перетворюються на інформаційний

простір на рівні з державами та міжнародними організаціями, як окремої особистості, так і найрізноманітніших соціальних і політичних груп, громадських рухів та організації. Своєю чергою, це створює серйозні виклики національній безпеці всіх держав, а особливо, таких як Україна, які перебувають на шляху демократичних перетворень, а також розбудови та захисту власної національної держави. Що також ставить перед українським суспільством нові виклики та загрози, які можуть мати далекосяжні наслідки для національної безпеки. Таким чином, дослідження інформаційного суспільства в інформаційно-безпечному вимірі України є дуже важливим і актуальним завданням для забезпечення стабільності та розвитку суспільства в умовах постійно зростаючого впливу інформаційних технологій. А також теоретичне осягнення сучасних тенденцій формування інформаційного суспільства в Україні, їх впливу на трансформацію форм та механізмів громадянської участі у соціально політичних процесах.

Виділення невирішених раніше частин загальної проблеми. Дослідження інформаційного суспільства в інформаційно-безпечному вимірі дозволить виявити та проаналізувати основні виклики та загрози, які ставляться перед Україною в цій сфері. Це дасть змогу розробити ефективні стратегії та механізми захисту інформації, визначити необхідність у підвищенні кваліфікації фахівців з інформаційної безпеки, розвивати національну інфраструктуру в інформаційному просторі України, а також залучати до цих процесів широку громадськість.

Формулювання цілей статті (постановка завдання). Мета даного дослідження полягає в тому, щоб проаналізувати сучасний стан інформаційного суспільства в Україні з точки зору інформаційної безпеки. А також визначити основні напрямки розвитку інформаційного суспільства та основних принципів інформаційної безпеки в контексті сучасних викликів та загроз, що постають перед суспільством.

Зокрема можна виокремити такі завдання:

1) Аналіз сучасного стану інформаційної безпеки України.

2) Дослідження міжнародного досвіду забезпечення інформаційної безпеки та аналіз кращих практик та можливостей їх впровадження в Україні.

3) Визначення основних напрямків розвитку інформаційної безпеки в України.

4) Аналіз ролі та взаємодії різних суб'єктів в системі інформаційної безпеки України виявлення можливих проблем та шляхів їх вирішення.

Аналіз останніх досліджень та публікацій. Особливості формування інформаційного суспільства в Україні, досліджувалися у численних роботах таких вчених як Почепцов Г.Г., Боднар І.Р.; Білоусов О.С.; Твердохліб О.С., Романенко Є.О. та інших. Разом з тим, з огляду на складність та багатоаспектність питань дослідження інформаційного суспільства в інформаційно безпековому вимірі, вказана проблематика потребує подальшого розвитку.

Виклад основного матеріалу дослідження. Інформаційна безпека як наукова категорія з'явилась не так давно, проте вже має значний вплив на розвиток наукових досліджень. Це пов'язано з тим, що інформаційні технології стали важливим елементом більшості сфер життя людей. Тому, інформаційна безпека має широкий спектр аспектів, що включає технічні, соціальні, економічні та політичні питання.

Одним з ключових аспектів дослідження є аналіз соціально-економічних, політичних та технологічних трансформацій, які відбуваються в інформаційному суспільстві. Дослідження показують, що збільшення кількості інформації та її доступності, а також розвиток інформаційно-комунікаційних технологій, є неоднозначними факторами, які можуть одночасно впливати як на позитивні, так і на негативні аспекти інформаційного суспільства.

Дослідники звертають увагу на необхідність розуміння основних принципів та проблем інформаційної безпеки, таких як конфіденційність, цілісність та доступність інформації. Згідно з дослідженнями, забезпечення інформаційної безпеки потребує комплексного підходу, який включає технічні, організаційні та правові заходи.

Для вивчення інформаційної безпеки в Україні використовуються різні наукові підходи. Один з них – комплексний підхід, який передбачає розгляд інформаційної безпеки як складової загальної безпеки держави. Цей підхід дає можливість оцінювати рівень інформаційної безпеки з точки зору не тільки технічних параметрів, але і соціально-економічних та політичних факторів.

Одне з перших комплексних досліджень та висвітлення сутності основних аспектів інформаційної безпеки провів Г.Г. Почепцов. Автор приділяє особливу увагу питанням побудови інформаційного суспільства, проблемам правового регулювання інформаційної сфери, а також становленню та впровадженню системи електронного урядування з урахуванням зарубіжного та вітчизняного досвіду. Автор зумів глибоко розкрити технології використання інформаційних стратегій та проведення сучасних інформаційних війн. На думку вченого, інформаційна політика є аналізом організації інформаційного простору, способів споживання інформаційних продуктів на певних територіях, інформаційних уподобань населення, та може бути корисною у вирішенні економічних, соціальних та військових завдань, оскільки сучасні суспільства значною мірою побудовані на інформаційній складовій [6, с. 10].

Для дослідження інформаційної безпеки України необхідно враховувати не лише загальні засади теорії інформаційної безпеки, а й специфіку внутрішніх та зовнішніх загроз, що становлять потенційну небезпеку для держави. Особливу увагу слід звернути на діяльність російської держави, яка веде інформаційну війну проти України, використовуючи різноманітні методи та технології, що включають дезінформацію, кібератаки, вплив на медіа та соціальні мережі, та інші.

Одним із ключових підходів у дослідженні інформаційної безпеки є системний підхід. Він передбачає розгляд інформаційної безпеки як складової системи, яка включає різноманітні субсистеми, елементи та взаємозв'язки між ними. При цьому, важливо враховувати взаємодію інформаційної безпеки з іншими складовими системи держави, такими як політична, економічна, соціальна та інші.

Також, для дослідження інформаційної безпеки необхідно використовувати інтердисциплінарний підхід, що передбачає взаємодію різних наукових дисциплін. Зокрема, в рамках дослідження інформаційної безпеки можуть бути використані знання та методи з інформатики, кібербезпеки, соціології, політології, економіки та інших галузей.

Загалом дослідники наголошують на важливості розуміння взаємозв'язку між інформаційною безпекою та правами та свободами людини в інформаційному суспільстві. Наприклад, необхідність забезпечення конфіденційності даних може конфліктувати з потребою у дотриманні принципів свободи слова та доступу до інформації [7, с. 29].

У процесі дослідження інформаційної безпеки України важливо враховувати різноманітні методологічні підходи, що можуть бути застосовані. Одним із ключових методологічних підходів є експертний аналіз, що передбачає залучення експертів з різних галузей та аналіз їхніх думок та оцінок щодо потенційних загроз інформаційній безпеці України.

Також, важливо враховувати аналітичні методи, такі як кібераналіз, соціально-політичний аналіз, моніторинг інформаційного простору тощо. Наприклад, кібераналіз передбачає аналіз кіберзагроз та кібератак, що можуть стати потенційними загрозами для інформаційної безпеки. Соціально-політичний аналіз дозволяє визначити, які соціальні, політичні та економічні процеси можуть впливати на інформаційну безпеку.

Крім того, не менш важливо використовувати кілька підходів до дослідження інформаційної безпеки, зокрема технічний та соціальний. Технічний підхід передбачає вивчення технічних аспектів забезпечення інформаційної безпеки, таких як шифрування, аутентифікація, захист від кібератак тощо. Соціальний підхід передбачає вивчення соціальних аспектів інформаційної безпеки, таких як поведінка користувачів, соціальні мережі, медіа та інші фактори, які можуть впливати на інформаційну безпеку [2, с. 70-71].

Зокрема вивчення соціального та політичних аспектів є важливими компонентами дослідження інформаційної безпеки в Україні. Саме ці два аспекти є найбільш взаємопов'язані та взаємозалежні, оскільки інформаційна безпека України не може бути досягнута без забезпечення безпеки суспільства та безпеки політичних процесів.

Соціальні аспекти дослідження інформаційної безпеки України пов'язані з дослідженням взаємодії між інформаційною безпекою та суспільством. Основною метою дослідження соціальних аспектів інформаційної безпеки є з'ясування способів впливу інформації на поведінку людей та на суспільство в цілому. Для досягнення цієї мети дослідники проводять соціально-психологічні дослідження, аналізуючи вплив інформаційних повідомлень на формування суспільних настроїв та ставлення до певних подій [2, с. 73].

Політичні аспекти дослідження інформаційної безпеки України пов'язані з дослідженням впливу інформаційних технологій на політичні процеси в країні. Дослідження політичних аспектів інформаційної безпеки має на меті з'ясування впливу інформації на формування політичної волі та рішень владних структур. Дослідники аналізують вплив інформації на процеси взаємодії між владними структурами та громадськістю, а також на формування політичної конкуренції та політичної ідентичності громадян [3, с. 162-163].

Окрім того, коли країна стикається зі складними політичними процесами, такими як вибори або конфлікти, важливо досліджувати вплив інформації на формування громадської думки та прийняття рішень. Для цього досліджувачі використовують методи аналізу політичних та інформаційних процесів, а також досліджують роль різних медіаплатформ у формуванні громадської думки та розповсюдженні інформації.

Політичні аспекти інформаційної безпеки також пов'язані з аналізом кіберзагроз та кібератак, які можуть мати серйозний вплив на політичну ситуацію в країні. Такі атаки можуть бути спрямовані на порушення виборчого процесу, дестабілізацію влади, розповсюдження фейкових новин тощо [2, с. 70]. Тому дослідження політичних аспектів інформаційної безпеки також повинні включати аналіз кібербезпеки та заходи щодо її забезпечення.

Соціальні та політичні аспекти дослідження інформаційної безпеки України є важливими складовими дослідження в цій області. Вони взаємопов'язані та взаємозалежні, оскільки забезпечення інформаційної безпеки в країні неможливе без забезпечення безпеки суспільства та

безпеки політичних процесів. Дослідження соціальних та політичних аспектів інформаційної безпеки України дозволяє розуміти взаємодію між інформацією та суспільством, розробляти стратегії захисту від кіберзагроз та кібератак, а також покращувати регулювання медіа-платформ та їх ролі в формуванні громадської думки. Саме це допоможе країні забезпечити стійку та ефективну інформаційну безпеку в умовах сучасного інформаційного суспільства [5, с. 21-22]

Для того, щоб зменшити негативний вплив ворожої брехні на наше суспільство, необхідно активно боротися з усіма фейками та неправдивою інформацією, які намагаються проникнути в український інформаційний простір. Це дасть громадянам можливість отримувати достовірну інформацію та відчувати підтримку влади, яка завжди на зв'язку з громадянами.

Медіакультура суспільства у вітчизняній науковій літературі визначається як "культура сприймання і виробництва соціальними групами та соціумом у цілому сукупності інформаційно-комунікаційних засобів, що функціонують у суспільстві, знакових систем, технологій комунікації, пошуку, збирання, виробництва і передавання інформації. На особистісному рівні медіакультура означає здатність людини ефективно взаємодіяти з мас-медіа, адекватно поводитися в інформаційному середовищі, здійснювати ціннісно-вольову рефлексивну регуляцію інформаційної поведінки" [3, с. 107]

Окрім того, важливим аспектом дослідження інформаційної безпеки в Україні є забезпечення прав людини та свободи слова в інтернеті. Важливо забезпечити свободу доступу до інформації та заборонити будь-які спроби обмеження свободи слова в мережі. Однак, водночас, необхідно дотримуватися законів, що стосуються захисту від клевети, вільного доступу до інформації та інших прав людини. Відсутність або порушення таких прав може стати причиною конфліктів та загроз для безпеки в інтернеті.

Водночас далеко не всі країни дотримуються даного аспекту в забезпеченні прав людини та свободи слова в інтернеті. Тому, цілком природно, що для того, щоб заповнити правовий вакуум на глобальному рівні висуваються відповідні ініціативи з боку перш за все провідних геополітичних гравців: США, а також країн Європейського Союзу та блоку НАТО.

До прикладу, головна зовнішньополітична ініціатива США щодо перспектив розвитку медіа та кіберпростору, яка була оприлюднена в травні 2011 р. під назвою Міжнародна стратегія кіберпростору, визначає принципові положення, якими будуть керуватися США при формуванні власної політики в інтернетпросторі. Так, "базовими принципами", що мають бути забезпечені при формуванні політики щодо інтернет простору є:

1) Можливість шукати, одержувати й передавати інформацію та ідеї через будь які засоби зв'язку незважаючи на кордони.

2) Люди мають бути обізнані з загрозами їхній персональній інформації та про можливість здійснення проти них кіберзлочинів.

3) Рух інформації не має обмежуватися фільтрами, оскільки вони створюють видимість безпек, інтернет простір має бути місцем інновацій та співпраці держави й бізнесу задля більшої безпеки [9].

Натомість медіаграмотність та забезпечення прав і свобод людини в інтернет просторі є дуже важливими питаннями в умовах російської агресії проти України. Одним з ключових аспектів забезпечення прав і свобод людини в інтернеті є свобода слова. Український законодавчий акт "Про захист персональних даних" забезпечує захист приватної інформації, включаючи особисту інформацію в інтернеті. Однак, на практиці, російська агресія може призвести до обмеження свободи слова та інших прав людини в інтернеті.

До механізмів протидії дезінформації можна віднести нормативно-правовий та інституційний. Починаючи з 2014 року в українському законодавстві відбулось багато позитивних змін, які направлені на вдосконалення інформаційного простору України. Прийняті закони «Про захист інформації» (2014), «Про інформаційні агентства» (2015), «Про інформацію» (2016), «Про друковані засоби масової інформації (пресу) в Україні» (2016). Одним з найважливіших законодавчих документів, що стосуються інформаційної безпеки країни є Доктрина інформаційної безпеки України [7, с. 76].

До підтримки зусиль, спрямованих на розширення доступу до новин, Україна також обмежила доступ до російських державних мас медіа, намагаючись зменшити їхній вплив. Українські медіа, як державні, так і приватні, історично перебувають у прямій конкуренції з російськомовними мас медіа.

На додаток, завдяки злагодженим зусиллям української влади та Указу Президента № 152/2022, яким ввів в дію Рішення Ради національної безпеки і оборони України "Щодо реалізації єдиної інформаційної політики в умовах воєнного стану". Реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення проблеми становлення правової демократичної держави якої реалізується шляхом об'єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач, на єдиній інформаційній платформі стратегічної комунікації – цілодобовому інформаційному марафоні "Єдині новини #UAразом" [8].

Таким чином, головним засобом, яким Україна може боротися з російською дезінформацією під час воєнного стану, є правда. Важливо не лише доносити її до внутрішньої аудиторії, але і до закордонної. Крім того, успіх у боротьбі з дезінформацією залежить від медіакультури та рівня медіаграмотності суспільства.

Щоб підвищити медіаграмотність в українському суспільстві, необхідно проводити освітні кампанії та навчальні заходи, які допоможуть людям зрозуміти, як розпізнавати фейкові новини, маніпуляції та пропаганду. Крім того, необхідно розвивати критичне мислення та навички критичної оцінки інформації. Щоб забезпечити права та свободи людини в інтернеті в умовах російської агресії, необхідно забезпечити безпеку в мережі, включаючи захист від кібератак та спроб злому. Також необхідно забезпечити свободу доступу до інформації та інтернет-ресурсів.

Українське суспільство повинно працювати разом, щоб забезпечити медіаграмотність та захист прав і свобод Водночас необхідна постійна підтримка незалежних ЗМІ та журналістів. Важливо, щоб українські ЗМІ були незалежними від політичних та економічних впливів та мали можливість досліджувати та публікувати об'єктивну інформацію.

Важливо забезпечити розвиток та підтримку соціальних мереж та інших інтернет-платформ, що дозволять українському суспільству зберігати зв'язки зі світом та обмінюватися інформацією.

Україна повинна продовжувати боротьбу з пропагандою та маніпуляціями в інформаційному просторі та підтримувати діалог та відкритість в інтернеті. Таким чином, можна забезпечити медіаграмотність та свободу слова в Україні в умовах російської агресії.

Висновки. Дослідження інформаційної безпеки України має бути зорієнтоване на вивчення різних аспектів інформаційної безпеки, включаючи технічні, соціальні та політичні аспекти. Для досягнення цієї мети важливо використовувати різні методи та інструменти дослідження, зокрема кібераналіз, соціально-політичний аналіз, моніторинг інформаційного простору та аналітику даних.

Водночас дослідження інформаційної безпеки має бути постійним процесом, оскільки загрози та ризики постійно змінюються та еволюціонують. Тому дослідники повинні бути готові до швидкого реагування на нові загрози та ризики. Також дослідження інформаційної безпеки має бути міждисциплінарним. Це означає, що дослідники повинні мати різні компетенції та знання в різних галузях, таких як кібербезпека, соціологія, політичні науки, інформаційні технології та ін. Тільки такий підхід дозволить забезпечити повні і глибокі дослідження інформаційної безпеки України.

Отже, дослідження інформаційної безпеки України має велике значення для забезпечення національної безпеки, захисту інформаційних ресурсів та забезпечення стійкого розвитку країни в умовах інформаційного суспільства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Білоусов О. С. Інформаційне суспільство в сучасній Україні: тенденції розвитку : монографія. О. С. Білоусов ; Одес. нац. політехн. ун-т. – Одеса : Гельветика, 2015. – 359 с.

2. Боднар І. Р. Інформаційна безпека як основа національної безпеки. І. Р. Боднар. Механізм регулювання економіки. – 2014. – № 1. – С. 68–75.

3. Донбас у системі інформаційної безпеки держави: регіональні особливості, зовнішні виклики, інструменти боротьби з антиукраїнською пропагандою: аналіт. доп. Бевз Т. А. та ін. ; НАН України, Ін-т політ. і етнонац. дослідж. ім. І. Ф. Кураса. – Київ : ІПіЕНД ім. І. Ф. Кураса НАН України, 2015. – 191 с.

4. Дунаєва Л. М. Дезінформаційні виклики під час російсько-української війни: політологічний аналіз. Л. М. Дунаєва. Politicus. – 2022. – №5. – С. 73–78.

5. Залєвська І. І. Інформаційна безпека України в умовах російської військової агресії. І. І. Залєвська, Г. І. Удренас. Південноукраїнський правничий часопис. – 2022. – №1. – С. 20–26.

6. Почепцов Г. Г. Інформаційна політика (навчальний посібник). Г. Г. Почепцов., 2008. – 663 с.

7. Твердохліб О. С. Теоретико-прикладні засади дослідження державної інформаційної політики у вітчизняному науковому дискурсі. Держава та регіони. Серія Державне управління, 2016 – № 1. – С. 26–30.

8. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» від 19 березня 2022 р. № 152/2022. URL: https://www.president.gov.ua/documents/1522022-41761.

9. International Strategy for Cyberspace. – 2011. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.