

DOI 10.34132/pard2024.25.03

Отримано: 2 квітня 2024

Змінено: 22 травня 2024

Прийнято: 3 червня 2024

Опубліковано:

25 вересня 2024

Received: 2 April 2024

Revised: 22 May 2024

Accepted: 3 June 2024

Published:

25 September 2024

Nazar Diakiv

STATE POLICY ON THE PROTECTION OF NATIONAL INTERESTS OF UKRAINE IN THE INTERNET ENVIRONMENT

The article deals with the problem of protecting Ukraine's national interests in the context of the Russian-Ukrainian war. The Internet is seen as a space for free expression of opinions, but often turns into a battlefield in the information war. The article analyses the processes of informatisation of society and the increase in the number of Internet users. The impact of the Russian-Ukrainian war on the leading Internet providers and their political position is analysed. Today, Ukraine enjoys great support from leading campaigns in this area, but the aggressor country is heavily funding war propaganda. Attention is drawn to the results of statistics on cyberattacks on state institutions and the public by the Russian Federation. It is emphasised that today state institutions, business and society in Ukraine have united to counteract the negative information influence of Russia. The structure of Ukraine's national interests, priorities and directions of their protection are defined.

Attention is focused on the fact that the Russian Federation attracts teenagers to extremist and radical activities on the Internet. This additionally threatens the national interests of Ukraine. Prevention of extremism is based on raising the legal, political and general culture of citizens, and shaping a positive image of the state. Therefore, it is justified to take effective measures to develop a powerful ideological corpus, a national idea and to adhere to the state's strategy for European integration.

It is important to establish systematic training of specialists in the field of protecting national interests in the Internet space, enhancing the preventive role of the media and institutional support for analytical, educational, propaganda and information work. The author proposes to develop a powerful system of countering manipulations on the Internet, which will include technological developments, methodology, ideological component, legal and educational measures. The author substantiates the necessity of Ukraine's integration into the global and regional European information space; integration into international information and telecommunication systems and organisations; modernisation and certain changes in the information policy; improvement of legislation on harmonisation of national legislation with international standards; introduction of modern information and communication technologies into public administration processes, etc.

Key words: *national interests, national security, state policy, state strategy, Internet threat, disinformation, information security, information warfare.*

Постановка проблеми у загальному вигляді. Захист національних інтересів є вельми важливим в умовах розвитку інформаційного суспільства. Це питання стосується як національної безпеки, так і життєдіяльності конкретного суспільства загалом. Йдеться, з одного боку, про створення державними інституціями сприятливих умов для реалізації та захисту національних інтересів, могутності, процвітання, всебічного розвитку України для максимального задоволення потреб та інтересів українців відповідно до загальновизнаних норм життєдіяльності, які необхідні для їх самозбереження, самовідтворення і самовдосконалення [1]. Інтернет є тим простором, який дозволяє державним інституціям швидко надавати громадянам інформацію, обмінюватись ідеями, дізнаватись думку населення тощо. Іншими словами, сприяє демократизації суспільства та обміну практиками з країнами Європейського Союзу.

З іншого боку, такі можливості інтернету можуть використовувати (й використовують) певні політичні гравці для

маніпуляцій громадською думкою та для проведення інформаційної війни. Такий вплив може мати довгострокові негативні наслідки для національних інтересів та мати певний руйнівний вплив у сфері ідеології та державного устрою.

Тому актуальним є дослідження ризиків та потенціалу інтернет-середовища, яке є платформою для розповсюдження різноманітної інформації, яка може загрожувати національній безпеці. Тут державна політика повинна допомогти сформуванню правильного ставлення як до сутності захисту національних інтересів, так і до практичної реалізації наміченої стратегії. Тому державна політика України у статті буде розглядатись в аспекті забезпечення безпеки саме національних інтересів і досягнення національної мети в інформаційному просторі.

Нині, в умовах розвитку інформаційного суспільства, спостерігається активізація таких двох взаємопов'язаних тенденцій, як необмежені можливості в отриманні інформації, так і у використанні її у протиправних цілях. Особливо в умовах воєнного конфлікту, а саме, широкомасштабної російсько-української війни (в тому числі, інформаційної) питання захисту національних інтересів та, одночасно, дотримання курсу держави на демократизацію відносин і євроінтеграцію є вельми затребуваними.

Аналіз останніх досліджень і публікацій. Питаннями національної безпеки, захисту національних інтересів, аналізу сучасних загроз, пошуком механізмів ефективної державної політики у цьому напрямку, розробкою інформаційно-комунікативних технологій займалися як науковці з різних галузей знань, так і політики, активні громадські діячі. Зокрема, Н. Петрецька, П. Ставичний аналізували категорію «національні інтереси» крізь призму забезпечення прав людини (індивідуальних та колективних); Р. Ковалюк досліджував національні інтереси України в новій геополітичній ситуації; В. Андріяш розглядав цей феномен в умовах глобалізації, а саме, гуманітарний, етнічний аспекти цієї проблематики. Інформаційній безпеці суспільства присвячені праці Г. Ситник, М. Орел, В. Смолянук та роботи багатьох інших науковців.

Сучасні дослідники займаються розробкою різних аспектів державної політики. Проте запропонована тема залишається актуальною як з наукової точки зору, так і у площині державного управління під час російсько-української війни.

Формулювання цілей статті (постановка завдання). Метою статті є визначення сучасних технологій (конструктивного та деструктивного) впливу на національні інтереси України в просторі інтернету, моніторинг інформації в інтернет-просторі, яка може загрожувати (шкодити) національним інтересам України в умовах російсько-української війни та пошук методів протидії у сфері державного управління.

Виклад основного матеріалу дослідження. Почнемо з того, що державна політика та управління щодо захисту національних інтересів України є свідомим цілеспрямованим впливом певного суб'єкта управління на безпеку та загрози (реальні чи потенційні), коли дії інституцій (державних і недержавних), а також окремих громадян створюють сприятливі умови для реалізації таких національних інтересів: існування і стійкий розвиток української нації; територіальна цілісність держави, суверенітет, національна самобутність, прогрес, що містить духовну, матеріальну та фізичні складові; збереження духовного і матеріального потенціалу, соціального капіталу, забезпечення особистої безпеки, конституційних прав та свобод людини і громадянина, науково обґрунтований та гарантований державою мінімум матеріальних і духовних умов існування; забезпечення державного суверенітету, подолання конфронтації в суспільстві, поглиблення консолідації українського суспільства, розв'язання кризових ситуацій у відповідних сферах; підвищення творчої активності населення; політична незалежність, територіальна цілісність, недоторканність державних кордонів; конституційний лад, розвиток цінностей та інтересів народу, законні права й інтереси громадянина; розвиток ефективної системи міжнародних зв'язків на основі партнерства і співробітництва; створення системи забезпечення національної безпеки для ефективної реалізації національних інтересів, участь у системах безпеки різного рівня [2].

Стосовно національних інтересів, то вони являють собою реалізацію природного права народу, нації на гідне життя, є важливими детермінантами та атрибутами національного відродження України. Це питання стає актуальним тоді, коли виникає нагальна потреба задовольнити національні сподівання та ефективно використати всі національні ресурси та соціальний капітал [3].

Проте, як забезпечити безпечну реалізацію та захист національних інтересів в умовах воєнного конфлікту? Інформаційний простір є досить демократичною платформою, де різні політичні актори, групи впливу, громадяни мають можливість оприлюднювати будь-яку інформацію. З іншого боку, потужний масив неперевіреної чи заздалегідь сформованої неправди здатний провокувати і підтримувати масштабні конфлікти та розбрат на національному та міжнародному рівнях.

Звернемось до сутності поняття «інформаційна безпека держави», яку розуміють як стан її захищеності, коли спеціальні інформаційні дії, операції, акти зовнішніх інформаційних агресій, тероризму, комп'ютерні злочини, незаконне зняття інформації за допомоги спеціальних технічних засобів та інший деструктивний інформаційно-комунікативний вплив не завдають істотної шкоди національним інтересам [4].

Тому можна додати, що в інформаційній сфері національні інтереси України містять такі життєво важливі моменти, як недопущення: інформаційної експансії з боку інших держав та різних міжнародних структур; інформаційної залежності; інформаційної блокади України, ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригуванні державної політики в інформаційній сфері; побудова та розвиток інформаційного суспільства; забезпечення економічного та науково-технологічного розвитку України; формування позитивного іміджу України; інтеграція України у світовий інформаційний простір тощо [5].

Зважаючи на той факт, що свідомість, психіка людей, інформаційні системи різного масштабу та призначення є

об'єктами інформаційної безпеки, можна розглядати об'єктами державної політики забезпечення інформаційної безпеки держави в інформаційній сфері: національні цінності; національні інтереси та національні цілі. Можна погодитись з військовими дослідниками Дж. Барбером та Я. Річардом, що в цій системі національні цінності визначають як стабільний елемент системи. Цінності формуються тривалий період часу в процесі історії, розвитку культури суспільства, і, звісно, відповідають геополітичному спрямуванню держави. Національні інтереси є елементом досить динамічним, що формується на ґрунті національних цінностей під впливом суспільного розвитку. Національні цілі є найбільш рухомим елементом [6].

За умов певних загроз, держава відчуває нагальну потребу в отриманні інформаційного суверенітету, але це є неможливим. Зрозуміло, що така ідея, як правило, негативно сприймається представниками ліберальних режимів, адже вона суперечить принципам свободи інформації та зводиться, переважно, до контролю. Зазначимо тут, що свобода інформації є поняттям, що позначає права і свободи людини, включаючи право й на інформацію, свободу вираження власної думки, поглядів і переконань, свободу обміну інформацією [7].

Варто відмітити, що нині державна політика України у сфері захисту національних інтересів в інтернет-середовищі базується на кількох ключових стратегіях та відповідно нормативних актах. Головними такими напрямками є: інформаційна безпека на всіх рівнях, боротьба з дезінформацією, захист критичної інфраструктури та забезпечення кібербезпеки, виявлення загроз з боку держави-агресора (рф). Саме у Стратегії національної безпеки України (затверджена Указом Президента № 392/2020 від 14 вересня 2020 року) визначено пріоритети національних інтересів України, включаючи інформаційну безпеку та захист від кіберзагроз. У Стратегії йдеться про необхідність розвитку технологічної спроможності для протидії інформаційним загрозам [6].

Доктрина інформаційної безпеки України визначає лише національні інтереси в сфері інформації. Логічно, що у цій площині

доцільно виділити такі головні складові національних інтересів України:

Дотримання конституційних прав і свобод людини та громадянина в галузі отримання інформації, її використання, забезпечення розвитку України, збереження і зміцнення моральних цінностей суспільства, традицій патріотизму, культурного і наукового потенціалу держави, гуманізму.

Інформаційне забезпечення державної політики України, яке сприяє поширенню достовірної інформації про суспільно-політичне життя країни, державну політику України, її офіційну позицію на міжнародній арені, коли забезпечується доступ громадян до відкритих державних даних, інформаційних ресурсів.

Розвиток сучасних інформаційних технологій (ІТ), вітчизняної індустрії інформації, в тому числі, засобів інформатизації, телекомунікації і зв'язку, забезпечення потреб внутрішнього ринку цієї продукції та вихід її на світовий ринок, а також забезпеченні накопичення, зберігання й використання вітчизняних інформаційних ресурсів. Нині лише на цій основі можна вирішувати проблеми створення наукомістких технологій, технологічного переозброєння промисловості, збільшення досягнень різних галузей української науки і техніки. Україна повинна зайняти гідне місце серед світових лідерів мікроелектронної і комп'ютерної промисловості.

Захист інформаційних ресурсів від технічних розвідок, несанкціонованого доступу, забезпечення безпеки інформаційних і телекомунікаційних систем.

Потік контенту в інтернет-середовищі є найрізноманітнішим й технологічно насиченим. Сучасні технології дозволяють користувачам поширювати інформацію, використовуючи різні платформи і формати, що надає додаткових труднощів у питаннях контролю над інформаційними потоками та притягнення до відповідальності певних осіб, які розповсюджують незаконний або шкідливий контент [6].

Особливо в умовах російсько-української війни потік пропаганди став дуже потужним. Проте існує розвиток конкретних інституцій та механізмів в Україні, спрямованих на відстеження і

протидію загрозам в інтернеті. Йдеться про моніторинг інформаційного простору, створення аналітичних центрів, а також тісну співпрацю між державними органами, приватними компаніями та закладами освіти. Крім того, сьогодні налагоджується співпраця України з іншими державами у сфері інформаційної безпеки.

Слушно акцентує увагу Стратегія інформаційної безпеки України (прийнята у 2021 р.), яка розроблена на період до 2025 року, що акцентувати увагу потрібно на боротьбі та протидії впливу дезінформації, обмеженні доступу до шкідливого контенту та на взаємодії між різними органами державної влади для захисту національних інтересів, зокрема, в інтернеті. Стратегія передбачає низку заходів, зокрема, видалення незаконного контенту з українського сегменту Інтернету, дотримуючись при цьому міжнародних норм і стандартів [7].

Крім того, головними принципами Стратегії інформаційної безпеки України є верховенство права, захист прав і свобод громадян та своєчасне реагування на інформаційні загрози. Важливим є те, що у забезпеченні інформаційної безпеки визначає роль органів державної влади та громадських організацій. Крім того, державні інституції активно співпрацюють з міжнародними організаціями для оптимізації та знаходження нових механізмів контролю та реагування на різноманітні інформаційні загрози. Наприклад, відбулись підписання міжнародних угод щодо участі України у глобальних ініціативах. Це, безумовно, сприятиме посиленню кібербезпеки та захисту національних інтересів України на світовому рівні [8; 9].

Однак зазначимо, що в умовах російсько-української війни має потужну компоненту інформаційна війна. Як відомо, вперше цей термін з'явився наприкінці 80-х рр. XX ст. і став результатом ефективної роботи аналітиків збройних сил США. Його почали широко використовувати після руйнування СРСР. Нині саме інформаційні війни й стали найбільшою небезпекою функціонуванню органів державного управління [4].

Відомі гуманітарний і технічний підходи щодо трактування поняття «інформаційної війни». У гуманітарному розумінні

інформаційна війна являє собою активні методи нав'язування громадянам таких моделей суспільства, які забезпечують бажані типи поведінки, прийняття рішень. А інформаційна війна, як зброя ведення бойових дій у будь-якій сфері життя, містить такі складові: здійснення впливу на інфраструктуру систем життєзабезпечення; промисловий шпіднаж; хакінг – зламування та використання особистих даних, ідентифікаційних номерів, інформації з обмеженим доступом тощо [18].

Крім того, слід додати до цих складових й ідеологічні маніпуляції. Це заклики рф в інтернеті до знищення українців, розповсюдження брехні про історію України та її культуру, заклики до агресії та окупації України тощо. Тому інформаційні війни, інформаційне протиборство є проявами загрози національним інтересам і національній безпеці в інтернет-просторі.

Зрозуміти масштаби впливу інтернет-ресурсів на національні інтереси можна, опираючись на результати дослідження Data Reportal. Так, на початку 2021 р. рівень проникнення інтернету в Україні був 67,6%. Тоді в Україні налічувалося близько 29,47 млн інтернет-користувачів, а 25,7 млн використовували соціальні мережі.

Безпосередньо перед початком повномасштабної війни кількість інтернет-користувачів зросла до 31,1 млн, а кількість користувачів соціальними мережами – до 28 млн. Рівень проникнення Інтернету зріс до 71,8%. У січні 2023 р. в Україні налічувалося 28,57 млн користувачів інтернетом. Тоді як рівень проникнення Інтернету становив вже 79,2%. До того ж, в Україні було 26,7 млн користувачів соціальних мереж, що становило приблизно 74% від чисельності населення. Для порівняння, на початок 2023 р. соціальними мережами користувалися 22,6 млн українців віком від 18 років (76,8% від загальної чисельності дорослого населення). Загалом, 93,5% інтернет-користувачів в Україні використовували соціальні мережі [10].

Звернемось до витоків існування ресурсів в інтернеті. Так, з кінця 1990-х рр. та ранніх 2000 рр. соціальні сервіси й пошукові машини намагались дотримуватися політики нейтральності. В основі

були однакові для всіх результати пошуку чи політика модерації, неупереджені алгоритми штучного інтелекту тощо. Це був певний ідеал, в якому техногіганти вбачали запоруку своєї незалежності до 24 лютого 2021 року. Втім, російсько-українська війна показала, що в інформаційному світі підтримувати нейтралітет апріорі неможливо. Адже однією і тією ж соціальною мережею користуються обидві сторони війни чи конфлікту, громадяни держав, які воюють між собою. Це призвело до того, що корпорації у 2022 році визначились із тим, яку сторону конфлікту підтримувати. Оскільки очевидним був агресор та жертва у війні, то й більшість техногігантів практично одразу обрали бік України. Зрозуміло, що такий вибір їм немало коштував. Так, Facebook, Instagram, Twitter і Google News заблоковані в рф [11].

Війна стала певним тригером, який стимулював усвідомлення того, що інтернет-платформам прийшлося переосмислити своє місце у цьому світі. Можна стверджувати, що більше не існує такого ідеалу як єдиний для всіх демократичний інтернет. Зокрема, Facebook позиціонував себе як відповідальний сервіс, який контролює дезінформацію та загрози демократії. А у Meta заговорили вимушено, лише після розслідування Конгресу щодо впливу російських тролів, технологій на вибори 2016 р. й після викриття діяльності Cambridge Analytica. Тоді компанія створила документ «Стандарти спільноти», який став основою для певних правил, що обґрунтовують публікацію постів та умови їх видалення [11]. Однак така технологія не уможливлює маніпуляції інформацією в інтернеті.

Зрозуміло, що будь-яка держава не може швидко та ефективно розв'язати комплекс проблем у сфері національної безпеки та зберегти й примножити національні цінності. Адже існує об'єктивна обмеженість наявних у неї ресурсів (матеріальних, політичних, людських, воєнних та інших). Тому завжди визначаються пріоритети, на яких мають бути зосереджені основні зусилля держави в конкретний період часу. Тому практичні завдання щодо забезпечення національної безпеки в державі зумовлюють необхідність визначення ієрархії національних інтересів.

Отже, визначення ієрархії національних інтересів є істотним чинником реалізації політики держави та прийняття управлінських рішень щодо забезпечення національної безпеки. За відсутності такої ієрархії стає неможливим існування певної комбінації управлінських впливів із питань безпеки, а процес вибору ефективного управлінського рішення не може логічно завершитись. Той чи інший варіант ієрархії національних інтересів є результатом використання конкретного критерію щодо її побудови. Пріоритетність національних цінностей можна визначати, враховуючи величину певних витрат (матеріальних, фінансових, людських тощо), які використовуються для захисту зазначених цінностей.

Звичайно, це можуть бути й витрати, спричинені відсутністю захисту національних інтересів. Йдеться про витрати, які є показником для визначення межі необхідного та достатнього з метою захисту національних інтересів, ресурсів та засобів, які необхідно використати в інтернеті. Але побудувати ієрархію національних цінностей досить складно, оскільки апіорі будь-яка національна цінність є безцінною. Тому одним із підходів, який доцільно використати для побудови ієрархії національних інтересів, є такий підхід, в основі якого лежить ступінь їхньої важливості для забезпечення національної безпеки. У такому випадку цей ступінь є критерієм для визначення пріоритетності тих чи інших інтересів стосовно інших із сукупності, яка розглядається [11].

Відомо, що національні цінності гарантують громадянам безпечне існування та прогресивний розвиток особі, суспільству і державі. Саме вони є концептуальними, ідеологічними основами, консолідуючими чинниками, важливими життєвими орієнтирами на шляху ефективного суспільного розвитку. Для людей характерні цінності, як об'єктивні параметри внутрішнього середовища, чітке дотримання яких є домінантою їхнього успішного розвитку.

Проте в інтернеті кожного дня не лише національні інтереси України потерпають від країни-агресора. Спотворення свободи Інтернету стає все більш очевидною, причому Китай і рф придушенні інакомислення та обмежують доступ своїм громадянам

до Інтернету. Оскільки ці авторитарні режими контролюють кіберпростір, то наслідки для демократії, свободи слова, приватного життя та доступу до інформації викликають сумніви.

Сьогодні є досить багато пріоритетних національних інтересів через російську агресію. Визначати їх ієрархію ми не будемо, але права і свободи, життя людини, суверенітет держави знаходяться у небезпеці. Так, відома інформація від команди (CERT-UA) реагування на надзвичайні ситуації, які пов'язані з інтернетом в Україні. Вона зафіксувала у період з січня 2022 року по вересень 2023 року майже 4000 різних кіберінцидентів, що втричі більше, ніж у довоєнний період. Росія координувала численні кібератаки, спрямовані проти України та країн, які є союзники України. Йшлося про проникнення в мережу, шпигунство, а також кібервплив на людей у всьому світі. У цю кількість, звичайно, не увійшли матеріали, які містять маніпулятивну складову, неправдиву інформацію про події в нашій країні [12].

Одразу після повномасштабного вторгнення рф з'явилися поради від Міністерства цифрової трансформації про методи протидії маніпуляціям, механізми боротьби з російською пропагандою в Інтернеті. Зокрема, оприлюднені поради як ідентифікувати неправдиву інформацію та що з нею робити. Упродовж воєнного часу негативний маніпулятивний контент, який публікує рф, виявляють та аналізують такі відомі медійні сайти й антифейкові проєкти, як «StopFake», «Брехунець», «НотаСнота», «Детектор медіа» та «Інститут масової інформації». Антифейковий проєкт «Брехунець» бореться з дезінформацією на Волинщині та Рівненщині. На сайті «Детектор медіа» стартував подкаст, який називається «Русский фейк, іді на...». Автори цього інформаційного ресурсу підбирають та спростовують фейки, вчать самостійно визначати шахрайство, маніпулювання, дезінформацію. Нажаль дотепер ще відсутні комплексні наукові розробки, у яких би досліджували б детально маніпулятивний контент у медіа [13].

Російські засоби пропаганди в інтернеті активно поширюють маніпулятивні новини, які найчастіше стосуються війни та військових, внутрішньо переміщених осіб в Україні. Російські

ЗМІ у своїх текстах намагаються виставити Збройні сили України в негативному світлі та дискредитувати їх в очах громадськості. Якщо ж сприймати інформацію критично й перевіряти дані в офіційних джерелах, то нескладно зрозуміти, що це неправда. Але вплив рф здійснюється й на громадян росії. Тому доцільно в інтернеті публікувати правдиві матеріали про культурне, суспільно-політичне життя українського суспільства російською мовою мовами Європейського Союзу. Це стосується і ресурсів фейсбуку, Instagram тощо, адже найкраще сприймається інформація від пересічних громадян, яким більше довіряють ніж офіційним ЗМІ [11].

Розглядаючи цю проблему з різних сторін, зазначимо, що до загроз національній безпеці в сфері інформації також варто віднести й обмеження свободи слова та доступу громадян до політично-важливої інформації; спотворення, блокування, викривлення фактів, замовчування, упереджене висвітлення конкретної інформації; несанкціоноване її поширення; інформаційну експансію з боку конкретних держав та руйнівне інформаційне вторгнення у національний інформаційний простір (коли держави з потужнішим інформаційним потенціалом отримали можливість розширити свій вплив через ЗМІ на населення і громадськість менш впливової держави); відкрити дезінформацію; функціонування у національному інформаційному просторі держави не підконтрольних інформаційних потоків; поширення жорстокості та насильства; повільність входження України у світовий інформаційний простір тощо [14].

Війна створила певні умови, які потрібно враховувати при розповсюдженні інформації. Окремих особливих професійних, або етичних стандартів, які повинні регламентувати діяльність журналістів та ЗМІ під час воєнних дій, не існує. Зрозуміло, що потрібно отримувати інформацію про факти, перевіряти їх та говорити чи публікувати правду. Звичайно потрібно пам'ятати, що всі ці матеріали отримує і країна-агресор. Будь-яке слово чи відео сюжет може бути використаний з маніпулятивних метою.

Але варто звернути увагу на способи застосування методів отримання інформації та реалії життя. Захищаючи цілісність і незалежність України, потрібно дотримуватись певних вимог, обмежень й особливостей застосування стандартів. Логічно, що діє заборона чи обмеження на поширення важливої інформації, яка може містити елементи таємності. Такі обмеження запроваджені військовим командуванням відповідно до Закону України «Про правовий режим воєнного стану» (2015 р.). Перелік заборон є в додатку № 2 до наказу головнокомандувача Збройних сил України від 3 березня 2022 року № 73 «Про організацію взаємодії між Збройними силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану», який і надалі кілька разів розширювався. Зокрема, заборонено розповсюджувати інформацію про результати ракетних ударів; переміщення озброєння і боєприпасів; розташування підрозділів сил оборони; розташування протиповітряної оборони тощо [16].

Про такі заборони повинні пам'ятати і пересічні громадяни, які публікують інформацію про певні військові дії, події. Для цього, на нашу думку, мають систематично організовуватись курси, семінари з питань медіаграмотності. Сьогодні однією із загроз для національних інтересів є залучення через інтернет підлітків спецслужбами РФ для створення конфліктів в інтернеті, публікацій негативної інформації про українське суспільство. Проте такі дії агресора є передбачуваними та стимулюють створення механізмів протидії.

Важливо займатись профілактикою екстремізму, що потужно фінансується РФ не лише в Україні, але і за кордоном. Тут потрібні спільні зусилля державних органів та громадськості, спрямовані на підвищення правової, політичної і загальної культури громадян, формування позитивного іміджу держави. Враховуючи це, необхідно вжити дієвих заходів для розробки потужного ідеологічного корпусу, національної ідеї та дотримання стратегії держави на євроінтеграцію. Сьогодні у світі загалом почастишали прояви радикалізації й екстремізму, тому важливо налагодити систематичну підготовку фахівців у цій сфері щодо інформаційної

протидії тероризму й екстремізму, підвищення профілактичної ролі медіа та інституційного забезпечення аналітичної, просвітницької, пропагандистської й інформаційної роботи.

Отже, питання забезпечення кібербезпеки, проблеми зовнішньої та внутрішньої загрози і протидії інформації, де пропагують національно-екстремістські та терористичні ідеї, звучать заклики до агресії, є одними з найактуальніших завдань українського суспільства й уряду держави на найближчу перспективу. Нині радикальна ідеологія активніша, ніж будь-коли, і створює серйозну загрозу конституційному ладу України [17].

Можна впевнено стверджувати, що виникнення нових засобів інформації і комунікації та їхнє розповсюдження у світі є одним із ризиків та, одночасно, найвагомішим чинником процесу глобалізації. Стрімке розширення інтернету зблизило людей, надало можливості швидко реагувати на інформацію в різних куточках нашої планети. Щоб уявити всю повноту і глибину інформаційної трансформації, яка нині відбувається, і зрозуміти динаміку цього процесу, необхідно усвідомити головну думку: в умовах глобальної інформатизації географія трансформується, змінюються межі між зовнішньою та внутрішньою політикою, що деформує як «національну», так й «соціальну» ідентичності, що може нести певні ризики. Глобальна інформатизація відкриває широкі можливості для транснаціональної взаємодії людей. Проте це і є ризиком під час воєнних конфліктів. Така ситуація, що містить протиріччя, повинна бути врахована у процесі формування державної політики. Ця проблематика сприяє веденню дискусій на міжнародному рівні, створенню асоціацій між новими акторами, учасниками політичної комунікації [15].

Протистояння України у війні стимулювало розвиток сильних сторін як держави, так і суспільства, що мало відображення й в просторі інтернету. Йдеться про єдність щодо демократичних цінностей та національних інтересів. Це дозволило усунути деякі ризики, передусім, проблеми у сфері інформаційної політики держави й слабкість стратегічної комунікації. Завдяки ефективній координації та об'єднанню зусиль державних інституцій, суспільства та бізнесу

Україна отримала певні переваги в інформаційній війні та забезпечила поширення правдивої інформації про війну та загалом події в країні [9].

Співпраця різних організацій, державних інституцій та громадянського суспільства сприяла консолідації суспільства, але й допомогла на практиці мінімізувати ризики від пропаганди рф. Звичайно, питання забезпечення національних інтересів і національної безпеки в інтернет-просторі продовжує розробляться. Інформаційна безпека забезпечується проведенням лише єдиної державної політики національної безпеки в інформаційній сфері, чітко продуманою системою заходів управлінського, економічного, політичного й організаційного характеру, які адекватно реагують на небезпеки національних інтересів всіх рівнів (особи, суспільства та держави в інформаційній сфері).

Для створення й підтримки належного рівня безпеки в інформаційній сфері розробляється система правових норм, що регулюють відносини в цій сфері, визначаються основні напрями діяльності органів державного управління, створюються або модернізуються органи забезпечення інформаційної безпеки та механізм контролю та нагляду за їх діяльністю. Хоча зауважимо, що функціонування системи забезпечення безпеки національних інтересів не обмежується лише значною кількістю нормативно-правових актів. Так, створення основних елементів системи забезпечення інформаційної безпеки національних інтересів в інтернеті ще не остаточно сформоване. А така недосконалість регулювання цих процесів негативно позначається і на державному управлінні у цій сфері.

Необхідно звернути увагу на те, що має постійно відбуватись моніторинг ризиків та загроз національним інтересам. Можна припустити, що після завершення війни безпекове середовище України буде суттєво змінено. Зазнають змін й пріоритетні потреби у сфері захисту національних інтересів та подальшого розвитку держави. Отже, після війни має бути розроблений новий цикл стратегічного планування, що вплине на зміст Стратегії національної безпеки України.

Висновки. Отже, різноманітність і швидкий розвиток технологій ускладнили контроль за контентом в інтернеті. Російсько-українська війна показала впливовість різних технологій, які можуть нести загрози національним інтересам України. Сьогодні наша держава розробляє та впроваджує комплексні стратегії та механізми для захисту своїх національних інтересів. Поширення дезінформації, кібернапади та інші форми інформаційних атак вимагають від держави високого рівня адаптивності та інноваційності у підходах до інформаційної безпеки.

За останні роки Україна стала прогресивною у питанні швидкого реагування на інциденти дезінформації в інформаційному просторі. Відповідь на виклики сучасного інформаційного середовища стала пріоритетом для держави, що призвело до впровадження ефективних стратегій захисту. Співпраця державних інституцій з громадськістю показала високу ефективність, консолідувала націю та сприяла швидкому реагуванню на ризики в інтернет-середовищі.

Крім того, Україна постійно вдосконалює своє законодавство у сфері інформаційної безпеки, приймаючи нові закони та нормативні акти, що регулюють відповідальність за порушення та визначають механізми захисту інформаційного простору. Міжнародна співпраця також відіграє ключову роль, адже обмін досвідом з іншими країнами та участь у глобальних ініціативах сприяє підвищенню ефективності захисту від інформаційних загроз. Ці заходи дозволяють Україні забезпечити захист своїх національних інтересів у складних умовах сучасного інформаційного середовища, де технології постійно змінюються і розвиваються.

ДЕРЖАВНА ПОЛІТИКА ЩОДО ЗАХИСТУ НАЦІОНАЛЬНИХ ІНТЕРЕСІВ УКРАЇНИ В ІНТЕРНЕТ СЕРЕДОВИЩІ

У статті розглядається проблема захисту національних інтересів України в умовах російсько-української війни. Інтернет розглядається як простір для вільного висловлювання своєї думки, який часто перетворюється на поле бою в інформаційній війні.

Аналізуються процеси інформатизації суспільства, збільшення кількості інтернет користувачів. У дослідженні проаналізовано вплив російсько-української війни на провідних провайдерів в інтернеті та їх політичну позицію. Автором зазначено, що на сьогодні Україна має велику підтримку з боку провідних кампаній в цій галузі, але країна-агресор потужно фінансує пропаганду війни. Звертається увага на результати статистики щодо кібератак з боку рф на державні інституції та громадськість. Акцентується увага на тому, що сьогодні в Україні об'єдналися державні інституції, бізнес і суспільство для протидії негативним інформаційним впливам рф. Визначено структуру національних інтересів України, пріоритетність та напрямків їх захисту.

У роботі також акцентовано увагу на те, що рф залучає підлітків до екстремістської та радикальної діяльності в інтернеті. Це додатково несе загрозу національним інтересам України. Профілактика екстремізму базується на підвищенні правової, політичної і загальної культури громадян, формуванні позитивного іміджу держави. Тому обґрунтовано вживання дієвих заходів для розробки потужного ідеологічного корпусу, національної ідеї та дотримання стратегії держави на євроінтеграцію. Важливо налагодити систематичну підготовку фахівців у сфері захисту національних інтересів в інтернет-просторі, підвищенні профілактичної ролі медіа та інституційного забезпечення аналітичної, просвітницької, пропагандистської й інформаційної роботи. Пропонується розробка потужної системи протидії маніпуляціям в інтернеті, яка включатиме технологічні розробки, методологію, ідеологічну компоненту, правові та просвітницькі заходи. Обґрунтовується необхідність інтеграції України до світового та регіонального європейського інформаційного простору; інтеграція у міжнародні інформаційно-телекомунікаційні системи та організації; модернізація та певні зміни в інформаційній політиці; удосконалення законодавства з питань узгодження національного законодавства з міжнародними стандартами; впровадження сучасних інформаційно-комунікативних технологій у процеси державного управління тощо.

Ключові слова: національні інтереси, національна безпека, державна політика, стратегія держави, інтернет-загроза, дезінформація, інформаційна безпека, інформаційна війна.

Author Contributions: Conceptualization, B.W.A. and L.W.F.; Writing – original draft, B.W.A. and L.W.F.; Writing – review & editing, B.W.A. and L.M.F. Author has read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable as study did not include human subjects.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Medvid, F. (2017). Natsionalna bezpeka i natsionalni interesy Ukrainy v hlobalizovanomu sviti [National security and national interests of Ukraine in the globalized world]. *Visnyk Lvivskoho universytetu. Seriiia istorychna – Bulletin of Lviv University. The series is historical*, (pp. 781-789). [in Ukrainian].
2. Vlasiuk, O., & Kononenko, S. (2017). *Kremlivska ahresiia proty Ukrainy: rozdumy v konteksti viiny* [Kremlin aggression against Ukraine: reflections in the context of the war]. Kyiv: NISD [in Ukrainian].
3. Medvid, F. (2016). Zabezpechennia natsionalnoi bezpeky Ukrainy yak funktsiia suchasnoi derzhavy: filosofsko-pravovi zasady [Ensuring the national security of Ukraine as a function of the modern state: philosophical and legal foundations]. *Proceedings from AIRLS' 16: XIII Mizhnarodna nauково-praktychna konferentsiia «Aktualni pytannia reformuvannia pravovoi systemy» – XIII International scientific and practical conference «Actual issues of reforming the legal system»*. (pp. 46-48) [in Ukrainian].
4. Chudinova, N.V., & Hrytsiuk, Yu.I. Informatsiina bezpeka Ukrainy ta vydy dzherel zahroz i nebezpek [Information security of Ukraine and types of sources of threats and dangers]. (n.d.). moodle.znu.edu.ua. Retrieved from: https://moodle.znu.edu.ua/pluginfile.php/470922/mod_resource/content/1 [in Ukrainian].

5. Dovhan, O.D., & Tkachuk, T.Yu. (2018). Pravove zabezpechennia informatsiinoi bezpeky derzhavy yak pidhaluz informatsiinoho prava: teoretychnyi dyskurs [Legal provision of information security of the state as a sub-branch of information law: theoretical discourse]. *Informatsiia i pravo – Information and law*, 2(25), (pp. 73-86) [in Ukrainian].

6. Yarger, R., & Barber, G. (1997). *The U.S. Army War College Mehtodology for Determining Interests and Levels of Intensity*. Carlisle: Carlisle Barracs, U.S. Army War College. Retrieved from: <http://www.au.af.mil/au/awc/awcgate/army-usawc/natinte.htm> [in English]

7. Solodka, O.M. (2020). Svoboda informatsii yak osnova zabezpechennia informatsiinoho suverenitetu Ukrainy [Freedom of information as a basis for ensuring information sovereignty of Ukraine]. Proceedings from PHRFSSIMC' 20: *Druha naukovo-praktychna konferentsiia «Zakhyst prav, svobod i bezpeky liudyny v informatsiinii sferi v suchasnykh umovakh materialy» – The second scientific and practical conference «Protection of human rights, freedoms and security in the information sphere in modern conditions»*. (pp. 54-58). Kyiv [in Ukrainian].

8. Ukaz Prezidenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy «Pro Stratehiuu natsionalnoi bezpeky Ukrainy» vid 14 veresnia 2020 roku No. 392/2020 [Decree of the President of Ukraine On the decision of the National Security and Defense Council of Ukraine «On the National Security Strategy of Ukraine» dated September 14, 2020 No. 392/2020]. www.president.gov.ua. Retrieved from: <https://www.president.gov.ua/documents/3922020-35037> [in Ukrainian].

9. Stratehiia informatsiinoi bezpeky – 2025: shcho zminytsia u sferi tsyfrovyykh prav [Information security strategy – 2025: what will change in the field of digital rights]. (2021). *dslua.org*. Retrieved from: <https://dslua.org/publications/stratehiia-informatsiynoi-bezpeky-2025-shcho-zminytsia-u-sferi-tsyfrovyykh-prav/> [in Ukrainian].

10. Yak povnomasshtabna viina vidobrazylasia na kilkosti internet-korystuvachiv v Ukraini [How the full-scale war affected the number of Internet users in Ukraine]. (2024). www.slovovidilo.ua. Retrieved from: <https://www.slovovidilo.ua/2024/04/15/infografika/suspilstvo/yak-povnomasshtabna-vijna-vidobrazylasya-kilkosti-internet-korystuvachiv-ukrayini> [in Ukrainian].

11. Balovsiak, N. Yak rosiiska ahresiia zminyla poshukovi servisy ta sotsialni merezhi [How Russian aggression changed search services and social networks]. (2022). *chas.news*. Retrieved from: <https://chas.news/current/viina-v-ukraini-pokazala-scho-neitralitetu-zaraz-ne-mozhe-isnuvati-tehnogigantam-takozh-dovelosya-vibrati-odnu-zi-storin-konfliktu> [in Ukrainian].

12. Svyrydiuk, Yu. (2023). V Ukraini zafiksuvaly maizhe 4 000 kiberatak z boku RF. *suspilne.media*. Retrieved from: <https://suspilne.media/619941-v-ukraini-zafiksuvali-majze-4-000-kiberatak-z-boku-rf/> [in Ukrainian].

13. Shulska, N.M., & Zinchuk, R.S. (2022). Mediamanipuliatsii v umovakh rosiisko-ukrainskoi viiny (na prykladi lokalnykh ZMI) [Media manipulation in the conditions of the Russian-Ukrainian war (on the example of local mass media)]. *Pivdennyi arkhiv – Southern archive*, (pp. 68-77) [in Ukrainian].

14. Ilnytska, U. (2016). Informatsiina bezpeka Ukrainy: suchasni vyklyky, zahrozy ta mekhanizmy protydiv nehatyvnykh informatsiino-psykholohichnykh vplyvam [Information security of Ukraine: modern challenges, threats and countermeasures against negative information and psychological influences]. *Politychni nauky – Political sciences*, 1, (pp. 27-32) [in Ukrainian].

15. Yemelyanov, V., & Bondar, H. (2019). Kiberbezpeka yak skladova natsionalnoi bezpeky ta kiberzakhyst krytychnoi infrastruktury Ukrainy [Cyber security as a component of national security and cyber protection of critical infrastructure of Ukraine]. *Publichne upravlinnia ta rehionalnyi rozvytok – Public administration and regional development*, (5), (pp. 493-523). Retrieved from: <https://doi.org/10.34132/pard2019.05.02> [in Ukrainian].

16. Dombrovska, S., Antonova, L., Shtyrov, O., & Kosse, A. (2023). Sotsialna vidpovidalnist derzhavy yak antykryzova komponenta publichnogo upravlinnia [Social responsibility of the state as an anti-crisis component of public administration]. *Publichne upravlinnia ta rehionalnyi rozvytok – Public administration and regional development*, (21), (pp. 624-641). Retrieved from: <https://doi.org/10.34132/pard2023.21.01> [in Ukrainian].

17. Dovzhenko, O., Yehorova, A., Ivanova, T., Miskyi, V., Potapova, V., & Yurychko, A. (2023). *Mediahramotnist pid chas viiny: teoriia, metodyka, interaktyv* [Media literacy during the war: theory, methodology, interactive]. O. Volosheniuk, V. Ivanova (Eds.). Kyiv: Akademiia ukrainskoi presy, Tsentr vilnoi presy [in Ukrainian].

18. Reznikova, O.O. (2020). Stratehichnyi analiz bezpekovooho seredovyshcha Ukrainy. *niss.gov.ua*. Retrieved from: <https://niss.gov.ua/news/statti/stratehichnyy-analiz-bezpekovooho-seredovyshcha-ukrayiny> [in Ukrainian].

Відомості про автора / Information about the Author

Назар Дяків, аспірант Вінницького державного педагогічного університету імені Михайла Коцюбинського, м. Вінниця, Україна. E-mail: nazard221@gmail.com, orcid: <https://orcid.org/0009-0004-5625-4007>.

Nazar Diakiv, PhD-student of Mykhailo Kotsiubynskyi Vinnytsia State Pedagogical University, Vinnytsia, Ukraine. E-mail: nazard221@gmail.com, orcid: <https://orcid.org/0009-0004-5625-4007>.

Diakiv, N. (2024). State policy on the protection of national interests of Ukraine in the internet environment. Public Administration and Regional Development, 25, 776-797. <https://doi.org/10.34132/pard2024.25.03>