

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

ТАРКІН ВАСИЛЬ ПАВЛОВИЧ

УДК 327.8:316.776.23](100)”19/20” (043.5)

ДИСЕРТАЦІЯ
ІНФОРМАЦІЙНІ ВІЙНИ У СУЧАСНОМУ ПОЛІТИЧНОМУ ПРОСТОРІ ЯК
ФЕНОМЕН ХХ-ХХІ СТОЛІТТЯ

Спеціальність 052 – Політологія

Галузь знань 05 «Соціальні та поведінкові науки»

Подається на здобуття ступеня доктора філософії.

Дисертація містить результати власних досліджень. Використання ідей,
результатів і текстів інших авторів мають посилання на відповідне джерело

_____ В.П.Таркін

Науковий керівник:

ВІТМАН Костянтин Миколайович,

доктор політичних наук, професор, директор
Центру підготовки магістрів публічної служби
і професійних суддів, заступник голови
експертної ради Міністерства освіти і науки
України з питань атестації наукових кадрів
суспільних наук

Одеса – 2023

АНОТАЦІЯ

Таркін В.П. Інформаційні війни у сучасному політичному просторі як феномен ХХ-ХХІ ст. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії з галузі знань 05 «Соціальні та поведінкові науки» за спеціальністю 052 «Політологія». Національний університет «Одеська юридична академія», Одеса, 2023.

Дисертація є одним з перших у вітчизняній політології спеціальним цілісним фундаментальним дослідженням інформаційних війн з позиції інтегрального підходу: феноменальність комплексного розуміння сучасних інформаційних війн полягає у тому, що одне поняття, по суті, акумулює у собі два їх різні види – інформаційно-психологічну та інформаційно-технічну війни. У науковій роботі наведено низку авторських понять, ідей та висновків, які характеризуються науковою новизною.

У дослідженні висвітлено змістовні міркування щодо інформаційних війн у політичній площині: теоретичне підґрунтя, хронологічний розвиток та практичне втілення – зокрема, на прикладі агресії РФ.

Розглянуто стан наукової розробленості проблеми, який характеризується незавершеністю політичної конструкції інформаційних війн. Триває наукова дискусія щодо того, чи є це поняття синтезом двох базових напрямків – інформаційно-психологічного та інформаційно-технічного, чи до нього доцільно відносити лише один із них; які методи та форми доречно відносити до інформаційних війн і яке їх співвідношення.

У сучасній літературі наукова експлікація «інформаційна війна» не має однозначного трактування. Окрім розбіжностей стосовно того, що ж можна вважати «інформаційною війною», так само проблемним є тлумачення окремих її категорій. Популярним є дослідження інформаційних війн у рамках психологічної парадигми. Різні науковці пропонують свої підходи, однак, на нашу думку, найбільш вдалим є комплексне розуміння інформаційних війн.

Шляхом застосування поліпарадигмального підходу, запропоновано визначення поняття: «інформаційна війна» під якою розуміється «комбінація людських або технологічних дій, призначених для присвоєння, видалення чи зміни інформації, що призводить до пошкодження або знищення критичної інфраструктури, порушення сталої роботи органів державної влади, економічних збитків у великих розмірах або порушення адекватного ментального сприйняття явищ і подій шляхом нав'язування певного бачення реальності». Попри об'єднувальне поняття, інформаційна війна має суттєву детермінацію, функціональну спрямованість на отримання різних результатів. Вона – політичний феномен, що слугує різним цілям; не одномоментний, а постійний акт насильства. Невід'ємним атрибутом інформаційних війн є інформаційна зброя.

Визначено, що інформаційна війна є складовою політичної війни – маючи універсальний характер, вона може вестися у економічній, соціальній, оборонній, духовній сферах. У контексті політичної війни, інформаційну війну можна визначити як зовнішню діяльність держави, яка веде до досягнення конкретних політичних цілей, спрямованих на руйнування чи зміну ідей, поглядів, ціннісних орієнтирів та інформаційних систем противника, при цьому захищаючи свої ресурси від аналогічних дій противника.

Акцентовано увагу на тому, що інформаційні війни не бувають поза межами традиційної боротьби – історія більшості конфліктів вказує на нездатність однієї лише військової міці досягнути переваги і перемоги. Зазвичай вони ведуться паралельно із традиційною війною або є складовою «гібридної війни», де слугують для того, щоб зламати головне – волю противника, нанести удар його моральному духу.

Відзначено, що надмірна кількість форм реалізації інформаційної війни ускладнює і без того кризовий, з точки зору наукового світогляду, категоріальний апарат інформаційних війн. У цьому контексті доречніше говорити про три

найчастіше вживані форми: інформаційну атаку, інформаційну операцію, інформаційну кампанію.

Відтворено етапи хронологічної еволюції інформаційних війн. Перший етап розпочинається ще у архаїчні (стародавні часи). Важливе значення у можливості ведення перших форм інформаційно-психологічної війни мало створення писемності (пропагандистські написи на каменях, деревах, будівлях), хоча переважними були вербальні технології впливу (виступи ораторів). Інформаційно-психологічна війна у давні часи була невід'ємною складовою військового конфлікту. Це найбільш тривалий етап, який охоплює і часи Середньовіччя, коли поява друку дозволила розповсюджувати газети, листівки, і Добу Просвітництва. Другий етап простягається із сер. XIX ст., яке охарактеризувалося появою нових способів доставки інформації, що пов'язано із винайденням електрики (фотографії, телеграфу, радіо тощо). Третій етап розпочинається із поч. XX ст., яке охарактеризувалося войовничістю й існуванням біполярного світу холодної війни. Кожна з воєн XX століття мала своє ідеологічне оформлення, мотивацію, яка могла виражатися як в офіційному визначенні війни вищими політичними та ідеологічними інститутами, так і в безпосередніх гаслах, які використовувалися в пропагандистській роботі, особливо під час Другої світової війни. Протягом XX ст. з'являються персональні комп'ютери і перші випадки кібератак. На цьому етапі можна говорити про появу перших форм інформаційно-технічної війни. Активно застосовувалися і теоретично досліджувалися засоби інформаційно-психологічної війни, найчастіше – один з найпоширеніших її методів – пропаганда. Цей етап простягнувся на століття. Четвертий етап розпочався з поч. XXI ст. і триває до теперішнього часу: кібервійна утвердилася як нове деструктивне явище, а методи інформаційно-психологічної війни з огляду на масштабну цифровізацію стали справжньою політичною інфекцією.

Викладено наукову експлікацію інформаційно-психологічної війни, під якою розуміється інструмент впливу політичної, військової, економічної, ідеологічної

дії, логічне застосування якого дозволяє: 1) впливати на формування громадської думки (у т.ч. викликати інакомислення, невдоволення чи навпаки – підтримку у населення); 2) захистити національні інтереси шляхом зниження морального духу, бойової ефективності ворогів; 3) впливати на поведінку іноземних держав, неурядових організацій, окремих груп чи осіб.

Адресантами інформаційно-психологічної війни можуть бути як державні, так і недержавні суб'єкти. Адресатами інформаційно-психологічної війни є маси, оскільки інформаційно-психологічна війна – складова політичних і масових комунікацій.

Об'єктом впливу інформаційно-психологічної війни є психічна діяльність людини чи груп людей. Метою інформаційно-психологічної війни можна вважати виклик певних емоційних реакцій для досягнення конкретних поведінкових результатів. До каналів або засобів інформаційно-психологічної війни можуть відноситися: 1) Інтернет-ресурси: сайти, блоги, соціальні мережі; 2) візуальні і звукові носії: телебачення, радіо, кінотеатр, документальні фільми, пісні, новини, ток-шоу; 3) промови: концерти, особисті зустрічі із великою аудиторією, політичні події; 4) мистецтво: картини, плакати; 5) преса і література: брошури, книги, газети, журнали.

До методів інформаційно-психологічної війни віднесено дезінформацію, яка є більш широким терміном, ніж популярний fake news, пропаганду та теорії змов, хоча теоретичні підходи до розуміння і переліку методів ще підлягатимуть глибокому аналізу, оскільки досі спостерігається семантична плутанина у різних термінах та значеннях.

Визначено пропаганду як основний метод інформаційно-психологічної війни. До її ознак віднесено: 1) односторонність аргументів; 2) виправдання результатами; 3) байдужість до логічних роздумів і доказової бази; 4) емоційну мову і переконливі визначення; 5) «квазіодноголосся»; 6) створення накопичувального повідомлення у ЗМІ.

Сформовано дефініцію інформаційно-технічної війни під якою розуміється будь-який тип інформаційного впливу із застосуванням програмно-математичної інформаційної зброї, метою якого є вплив на функціонування інформаційної системи шляхом незаконного доступу до інформаційної системи, здолаття системи захисту, обмеження доступу законних користувачів з можливістю подальшого несанкціонованого збору, копіювання, перехоплення, блокування або видалення інформації.

Виявлено, що ідейне поле у контексті інформаційно-технічної війни (кібервійни) можна умовно розділити на два табори: 1) кібервійна існує; 2) кібервійна – це певна умовність.

Констатовано, що небезпечної «мілітаризації» кіберпростору ще не досягнуто, а часте використання терміна «кібервійна» для позначення всіх політично-мотивованих кібератак видається дещо перебільшеним, хоча кожен такий випадок, безсумнівно, вказує на вразливість життя суспільства у цифрову епоху.

Встановлено, що до збройного арсеналу інформаційно-технічної зброї, яка націлена на збір конфіденційної інформації, доступ до мережі, може погіршувати роботу мережі, у тому числі призводити до відмови роботи усього сервісу, погіршувати або змінювати роботу одного чи декількох вузлів мережі, активізувати шкідливий код належать чотири основних методи. Першим є атаки, спрямовані на перевантаження ресурсу запитами, аби вичерпати їх фільтрувальну здатність. Такі дії призводять або до сповільнення, або до зупинки роботи інформаційної системи. Другим є метод міжсайтового скриптингу (XXS), пов'язаний із вразливістю веб-сайтів. Третім є метод соціально-технічної інженерії. Четвертий метод – встановлення шкідливого програмного забезпечення без згоди власника.

Викладено бачення особливостей кібервійни: 1) це війна між суверенними державами, яка ведеться за допомогою кіберзброї; 2) кібервійна як становище у кіберпросторі тісно межує із кіберзлочинністю, кібершпигуванням, що робить

розмитим її межі; 3) кібервійна може бути частиною збройного конфлікту, як міжнародного, так і внутрішнього.

Об'єктом кібервійни визначено інформаційно-технічну систему. Суб'єктом є кібервоїн (хакер), який прагне задовольнити своє его або отримати фінансову винагороду; отримати визнання в очах своїх колег, задовольнити цікавість; для нього участь в інформаційно-технічній війні може виступати і як перевірка власного інтелекту, і як виклик державам; або ж, навпаки, це може бути виконання конкретного замовлення окремих компаній, переслідуючи мету грошового прибутку, чи іноземних держав, для досягнення ними конкурентної переваги (наприклад, економічної) тощо.

Відзначено, що інформаційна війна РФ – постійний акт насильства, що слугує різним політичним цілям: ведеться в освітній, соціальній, оборонній, духовній сферах. Стратегія реалізовується сучасними способами – широким простором можливостей інформаційно-психологічної війни та масштабними кібератаками. Наслідки російської кіберактивності все ж менш відчутні, ніж результати традиційних військових дій: реалії російсько-української війни вкотре це підкреслюють, однак, забезпечення національної безпеки держави неможливе без звернення уваги на ризики, пов'язані з можливостями інформаційно-технічної війни.

Пояснено, що український спротив інформаційній агресії РФ зосередився на таких аспектах: 1) невпинне виправлення і встановлення фактів щодо російського вторгнення; 2) роботи спеціальних органів, покликаних спростовувати російські інформаційно-психологічні наративи; 3) розвінчування підступних принижувальних дискурсів щодо історичних фактів; 4) регулярне подання правдивої версії війни і розвінчування російських міфів Президентом України; 5) поступове вирішення питання монументальної пропаганди.

Ключові слова: агресія, дезінформація, інформаційна війна, інформаційний простір, інформаційно-комунікаційні технології, кіберпростір, кіберконфлікт,

м'яка сила, політична комунікація, насильство, сучасна політика, пропаганда, теорія змов, цифровізація, політичні інститути.

SUMMARY

Tarkin V. Information wars in the modern political environment as a phenomenon of the 20th and 21st centuries. – Qualified scientific work as a manuscript.

Dissertation for the of Philosophy Doctor degree with scientific speciality 05 «Social and Behavioral Sciences» for specialty 052 «Political Science». National University «Odesa Law Academy», Odesa, 2023.

The dissertation forms one of the first in domestic political science to be a special holistic fundamental study of informational warfare from the standpoint of an integral approach: the phenomenality of a comprehensive understanding of modern information wars is that one concept, in fact, accumulates two different types of them – informational-psychological and informational-technical warfare. The scientific work contains a number of author's concepts, ideas and conclusions, which are characterized by scientific novelty.

The research highlights meaningful considerations regarding information wars in the political plane: theoretical background, chronological development, and practical implementation – in particular, using the example of the aggression of the Russian Federation.

It was explored the state of scientific development of the problem, which is characterized by the incompleteness of the political construction of informational warfare. There is an ongoing scientific debate as to whether this concept is a synthesis of two basic directions – informational-psychological and informational-technical, or whether it is expedient to refer to it only one of them; what methods and forms should be attributed to information wars and what their ratio is.

The scientific explanation of informational warfare does not have an unambiguous interpretation. In addition to disagreements about what can be considered as informational warfare, the interpretation of its individual categories is equally problematic. The study of

informational warfare within the framework of the psychological paradigm is popular. Different scholars offer their approaches, however, in our opinion, the most successful is a comprehensive understanding of information wars.

By applying a polyparadigmatic approach, the following definition of the concept is proposed: informational warfare is a combination of human or technological actions designed to appropriate, delete or change information, which leads to damage or destruction of critical infrastructure, disruption of the stable work of state authorities, economic losses in large dimensions or violation of adequate mental perception of phenomena and events by imposing a certain vision of reality. Despite the unifying concept, informational warfare has a significant determination, a functional focus on obtaining different results. It is a political phenomenon that serves various purposes which form not a single-time, but a continuous act of violence. An integral attribute of information wars is information weapons.

It was determined that the informational warfare is a component of the political war – having a universal character, it can be waged in the economic, social, defense, and spiritual spheres. In the context of political warfare, information warfare can be defined as the external activity of the state, which leads to the achievement of specific political goals aimed at destroying or changing the ideas, views, value orientations and information systems of the enemy, while protecting its resources from similar actions of the enemy.

It is indicated that information wars do not occur outside the boundaries of traditional struggle – the history of most conflicts indicates the inability of military power alone to achieve superiority and victory. Usually they are conducted in parallel with traditional war or are a component of «hybrid war», where they serve to break the main thing – the will of the enemy, to strike at his morale.

It is noted that the excessive number of forms of implementing informational warfare complicates the already crisis-oriented categorical apparatus of informational warfare from the point of view of the scientific worldview, in this context it is more

appropriate to talk about the three most frequently used forms: information attack, information operation, information campaign.

It was reproduced a chronological evolution of informational warfare. The first stage begins in archaic (ancient times). The creation of writing (propaganda inscriptions on stones, trees, buildings) played an important role in the possibility of conducting the first forms of informational and psychological warfare, although verbal technologies of influence (speech of speakers) were predominant. In ancient times, informational and psychological warfare was an integral part of military conflict. This is the longest stage, which also covers the Middle Ages, when the advent of printing allowed the distribution of newspapers, postcards, and the Age of Enlightenment. The second stage extends from the middle of the 19th century, which was characterized by the emergence of new methods of information delivery, which is connected with the invention of electricity (photography, telegraph, radio, etc.). The third stage begins with the beginning of the 20th century, which was characterized by militancy and the existence of a bipolar Cold War world. Each of the wars of the 20th century had its own ideological design, ideological motivation, which could be expressed both in the official definition of war by higher political and ideological institutions, and in direct slogans used in propaganda work, especially during the Second World War. During the 20th century, personal computers appear and the first cases of cyberattacks have taken its place. At this stage, it is possible to talk about the emergence of the first forms of informational-technical warfare. The means of informational and psychological warfare were actively used and theoretically researched, most often one of its most widespread methods was propaganda. This stage lasted for decades. The fourth stage began at the beginning of the XXI century. and continues to the present: cyber war has established itself as a new destructive phenomenon, and the methods of informational and psychological warfare in view of large-scale digitization have become a real political infection.

It was outlined the scientific explanation of informational and psychological warfare, which is understood as a tool for influencing political, military, economic, and

ideological action, the logical application of which allows: 1) to influence the formation of public opinion (including causing dissent, dissatisfaction or vice versa – support among the population); 2) protect national interests by reducing the morale and combat effectiveness of enemies; 3) influence the behavior of foreign states, non-governmental organizations, individual groups or individuals.

Addressees of informational and psychological warfare can be both state and non-state entities. The addressees of informational and psychological warfare are the masses, since informational and psychological warfare is a component of political communications and mass communications.

The object of informational and psychological warfare is the mental activity of a person or groups of people. The purpose of information and psychological warfare can be considered to be the elicitation of certain emotional reactions to achieve specific behavioral results. Channels or means of information and psychological warfare may include: 1) Internet resources: sites, blogs, social networks; 2) visual and sound media: television, radio, cinema, documentaries, songs, news, talk shows; 3) speeches: concerts, personal meetings with large audiences, political events; 4) art: paintings, posters; 5) press and literature: brochures, books, newspapers, magazines.

The methods of informational and psychological warfare include disinformation, which is a broader term than popular fake news, propaganda and conspiracy theories, although theoretical approaches to the understanding and list of methods will still be subject to in-depth analysis, as there is still semantic confusion in various terms and meanings.

Propaganda is defined as the main method of information and psychological warfare. Its signs include: 1) one-sidedness of arguments; 2) justification by results; 3) indifference to logical thinking and the evidence base; 4) emotional language and convincing definitions; 5) «quasi-unanimous»; 6) creation of cumulative message in mass media.

It was formed the definition of informational and technical warfare, which means any type of information influence with the use of information weapons, the purpose of which is to influence the functioning of the information system through illegal access to the information system, overcoming the protection system, limiting the access of legitimate users with the possibility of further unauthorized collection, copying, interception, blocking or deletion of information.

It was found that the ideological field in the context of information and technical war (cyber war) can be conditionally divided into two camps: 1) cyber war exists; 2) cyber war is a certain convention.

It has been established that the dangerous «militarization» of cyberspace has not yet been achieved, and the frequent use of the term «cyberwar» to denote all politically motivated cyberattacks seems somewhat exaggerated, although each such case undoubtedly points to the vulnerability of society in the digital era.

It has been discovered that the arsenal of information and technical weapons, which are aimed at collecting confidential information, access to the network, can impair the operation of the network, including the failure of the entire service, impair or change the operation of one or more network nodes, activate malicious code there are four main methods. The first are attacks aimed at overloading the resource with requests in order to exhaust its filtering capacity - such actions lead to either slowing down or stopping the operation of the information system. The second is the method of cross-site scripting (XXS) related to the vulnerability of websites. The third is the method of socio-technical engineering. The fourth method is to install malicious software without the owner's consent.

The vision of the features of cyber war is outlined: 1) it is a war between sovereign states, which is waged with the help of cyber weapons; 2) cyberwar as a situation in cyberspace closely borders on cybercrime, cyberespionage, which blurs its boundaries; 3) cyber war can be part of an armed conflict, both international and internal.

The object of cyberwar is defined as an information technology system. The subject is a cyberwarrior (hacker) who seeks to satisfy his ego or receive a financial reward; get recognition in the eyes of your colleagues, satisfy curiosity; for him, participation in the information and technical war can act both as a test of his own intelligence and as a challenge to the states; or, on the contrary, it can be the fulfillment of a specific order of individual companies, pursuing the goal of monetary profit, or of foreign countries, in order to achieve their competitive advantage (for example, economic), etc.

It was noted that the informational warfare of the Russian Federation is a constant act of violence that serves various political goals: it is conducted in the educational, social, defense, and spiritual spheres. The strategy is implemented in modern ways – a wide range of opportunities for information and psychological warfare and large-scale cyberattacks. The consequences of Russian cyber activity are still less tangible than the results of traditional military actions: the realities of the Russian-Ukrainian war once again emphasize this, however, ensuring the national security of the state is impossible without paying attention to the risks associated with the possibilities of information and technical warfare.

It was explained that the Ukrainian resistance to the informational aggression of the Russian Federation focused on the following aspects: 1) relentless correction and establishment of facts regarding the Russian invasion; 2) the work of special bodies designed to refute Russian informational and psychological narratives; 3) debunking insidious derogatory discourses regarding historical facts; 4) regular presentation of the true version of the war and debunking of Russian myths by the President of Ukraine; 5) gradual solution to the issue of monumental propaganda.

Key words: aggression, disinformation, information war, information space, information and communication technologies, cyberspace, cyber conflict, soft power, political communication, violence, modern politics, propaganda, conspiracy theory, digitalization, political institutions.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні результати дисертації

1. Таркін В.П. Інформаційні війни: теоретичний аспект. *Держава і право. Юридичні і політичні науки*. 2020. Випуск 87. С.285-294. DOI: 10.33663/1563-3349-2020-87-285.
2. Таркін В.П. Окремі аспекти використання методів інформаційно-психологічної війни під час пандемії Covid-19. *Актуальні проблеми політики*. 2021. №67. С.112-117. DOI <https://doi.org/10.32837/app.v0i67.1160>.
3. Таркін В.П. Боротьба у кіберпросторі: інформаційні війни і кібертероризм. *European political and law discourse*. 2021. Volume 8. Issue 4. С.97-105. DOI: 10.46340/eppd.2021.8.4.11.
4. Таркін В.П. Особливості інформаційної війни РФ та український спротив. *Актуальні проблеми політики*. 2023. Вип.71. С.204-210. DOI <https://doi.org/10.32782/app.v71.2023.28>.

Наукові праці, які засвідчують апробацію матеріалів дисертації

5. Таркін В.П. Окремі аспекти успішної пропаганди у поглядах С.П. Чахотина. *Українське суспільство в умовах воєнного стану: сучасні виклики та напрямки розвитку* : матеріали Всеукр. наук. конф. молодих вчених, м. Одеса, 6 червня 2022 р. Одеса : Фенікс, 2022. С. 626-630.
6. Таркін В.П. Пропаганда як метод інформаційно-психологічної війни: політичний контекст. *Правове життя сучасної України: у 3 т.: матеріали міжнар. наук.-практ.конф., м.Одеса, 15 трав.2020 р.* Одеса : Видавничий дім «Гельветика», 2020. Т.1. С.251-254.
7. Таркін В.П. Правове забезпечення інформаційної політики. *Нові завдання та напрями розвитку юридичної науки у XXI столітті* : матеріали міжнародної науково-практичної конференції м.Одеса, 26-27 лютого 2021 року, Одеса : Міжнародний гуманітарний університет, 2021. С.42-45.

8. Таркін В.П. Інформаційно-технічна війна у гонитві вакцинації. *Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (за нагоди 30-ти річчя проголошення незалежності України та 25-ти річчя прийняття Конституції України)* : у 2 т. : матеріали міжнар. наук.-практ. конф., м. Одеса, 21 травня 2021 р. Одеса, 2021. Т 1. С.209-212.
9. Таркін В.П. Дезінформація як метод інформаційно-психологічної війни. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права)* : у 2 т. : матеріали Міжнар.наук.-практ. конф. м. Одеса, 17 червня 2022 р. Одеса : Видавничий дім «Гельветика», 2022. Т. 1. С. 267-270.
10. Таркін В.П. Інтернет – платформа інформаційно-психологічної війни. *Сталий розвиток суспільства та держави: сучасні виклики та перспективи розвитку*: матер. Всеукр. наук. конф. молодих вчених, м.Одеса, 18 листопада 2022 р.) [Електронне видання] / уклад. В.С.Кучерявенко, Л.С.Бондарчук, І.С.Радковська [та ін.]; за ред. М.Р.Аракеяна, К.І. Спасової. Одеса, 2022. С.227-230.
11. Таркін В.П. Окремі аспекти конспірологічних теорій. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень*: матеріали міжнародної науково-практичної конференції, м. Одеса, 19 травня 2023 р. Одеса, 2023. Том 1. С.206-209.

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1. ВИЗНАЧЕННЯ ПОНЯТТЯ ІНФОРМАЦІЙНИХ ВІЙН ТА ЇХ РОЛІ У ПОЛІТИЧНОМУ ПРОЦЕСІ.....	11
<i>1.1. Ступінь наукової розробленості проблеми.....</i>	<i>11</i>
<i>1.2. Концептуальні та методологічні підходи до розуміння інформаційних війн. .</i>	<i>28</i>
<i>1.3. Форми реалізації інформаційних війн.</i>	<i>37</i>
<i>1.4. Генеза та розвиток інформаційних війн як політичного інструменту.</i>	<i>44</i>
<i>Висновки до 1 розділу</i>	<i>68</i>
РОЗДІЛ 2. ВИДОВІ ОСОБЛИВОСТІ ІНФОРМАЦІЙНИХ ВІЙН	72
<i>2.1. Комунікаційні та психологічні впливи як підґрунтя інформаційно-психологічної війни.</i>	<i>72</i>
<i>2.2. Інструментарій інформаційно-психологічної війни</i>	<i>96</i>
<i>2.3. Інформаційно-технічна війна: теоретичні засади.</i>	<i>119</i>
<i>2.4. Інструментарій інформаційно-технічної війни.</i>	<i>141</i>
<i>Висновки до 2 розділу</i>	<i>154</i>
РОЗДІЛ 3. СПЕЦИФІКА ІНФОРМАЦІЙНОЇ ВІЙНИ РФ ТА УКРАЇНСЬКІ СПОСОБИ ПРОТИДІЇ	158
<i>Висновки до 3 розділу</i>	<i>171</i>
ВИСНОВКИ.....	175
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	180
ДОДАТКИ	204

ВСТУП

Актуальність теми дослідження. Соціально-економічні, політичні й культурні перетворення нерозривно пов'язані із процесом інформатизації, однак, новий спосіб функціонування суспільства й перехід інформації у розряд цінних ресурсів – це ще й нові виклики, один із яких – інформаційна війна, феномен якої викликає і науковий інтерес.

Питання наповненості багатовимірної категорії «інформаційних війн», її форм та методів належить до дискусійної наукової проблеми. Не дивлячись на існуючі теоретичні міркування, невелика кількість робіт вирізняється інтегральним підходом до розуміння інформаційних війн, що вказує на те, що розуміння їхнього феномена залежить від дослідницької інтерпретації: те, що на думку одних вчених входить до поняття, на думку інших залишається за його межами. Зміст поняття інформаційних війн, на наш погляд, виходить за межі впливу на громадську свідомість, поведінку, почуття та переживання та включає ще й інформаційно-технічне протиборство як окрему підсистему; це не лише про «напад» на людську ментальність, сприйняття та приймання рішень, але й про посягання на інформаційні системи.

Потенціал Інтернету у війнах цифрової епохи складно переоцінити: інноваційні технологічні практики поєдналися із традиційними методами ведення інформаційно-психологічної війни, а кіберполітика як новий спосіб ведення політики нерозривно пов'язана із постійними кіберзагрозами – ці аспекти потребують постійного звернення політичної науки і оновлених теоретичних побудов, адже, теорія володіє найвищим науковим потенціалом тоді, коли знаходиться у логічній близькості із емпірією. У цьому аспекті доцільним видається актуалізація емпіричного і теоретичного рівнів інформаційних війн як складової сучасного політичного простору.

У контексті актуальності теми дисертаційного дослідження, неможливо не звернути увагу і на те, що російсько-українська війна призводить до усвідомленої потреби розробки доктрини інформаційних війн з урахуванням вимог часу, адже інформаційні війни – не лише складова теоретичних розробок, але й глибока соціально-політична проблема сьогодення.

Зв'язок роботи з науковими програмами, планами, темами. Дисертація виконана з урахуванням плану науково-дослідної роботи Національного університету «Одеська юридична академія» «Стратегія інтеграційного розвитку України: правовий та культурний вимір» на 2018-2022 рр. (державний реєстраційний номер 0116U001842); в рамках наукових досліджень Національного університету «Одеська юридична академія» за темою «Правове та соціальне життя України у людиноцентристському вимірі в цифрову еру» на 2021-2025 рр. (державний реєстраційний номер 0122U000266); а також у межах плану науково-дослідницької роботи кафедри політичних теорій факультету психології, політології та соціології Національного університету «Одеська юридична академія» за темою «Людиноцентристський вимір політики в умовах цифрової трансформації».

Тема дисертації затверджена на засіданні Вченої Ради Національного університету «Одеська юридична академія» 17 жовтня 2019 р. (Протокол №1).

Мета і завдання дослідження. Відповідно обраного *об'єкта* – інформаційних війн як політичного явища та *предмета* дослідження – інформаційних війн у сучасному політичному просторі як феномену XX-XXI століття, *метою* написання дисертації є визначення інформаційних війн з позиції теоретичної побудови, історичного підходу та, частково – практичного втілення.

Мета досягається шляхом постановки наступних *завдань*:

- визначити ступінь наукової розробки даної тематики;
- виявити викладені в науковій літературі підходи до розуміння поняття «інформаційні війни»;

- сформулювати власне визначення інформаційних війн;
- відтворити хронологічну еволюцію інформаційних війн на прикладі окремих випадків її втілення на різних історичних етапах;
- визначити особливості, притаманні інформаційно-психологічній війні;
- визначити специфіку інформаційно-технічної війни (кібервійни);
- окреслити напрямки протидії інформаційній агресії РФ, які втілено на фоні повномасштабного вторгнення.

Невід’ємною складовою наукового пізнання політичних категорій є застосування методів, які є частиною раціональної дискусії та забезпечують достовірність емпіричних та теоретичних положень.

Серед основних використаних методів можна виділити загальнонаукові методи: метод аналізу та метод синтезу, індукції та дедукції – для виділення наукових понять, формулювання нових дефініцій та дослідження їх взаємодії.

Особливе місце у роботі займають системно-структурний метод, який дозволив виявити необхідні зв’язки між структурними частинами явища інформаційно-психологічної та інформаційно-технічної війн, зв’язків явища з іншими явищами, розкрити конкретні зв’язки цілого з частинами, частин один з одним; історичний метод, який дав змогу дослідити хронологію інформаційних війн; метод case study (метод окремого випадку) використовувався при ретроспективному аналізі історичних подій та подій на сучасному етапі.

У процесі написання дисертації було використано й інші догматичні та спеціальні методи.

Теоретичну основу дослідження становлять роботи вітчизняних учених, серед них: В.В. Антонюк, І.О. Валюшко, К.М. Вітман Я.М. Жарков, Ю.В.Завгородня, Б.М. Калініченко, Л.І. Кормич, Д.В. Кіслов, Л.Ф. Компанцева, Т.М.Краснопольська, О.В. Литвиненко, Л.П. Макаренко, Е.В. Мамонтова, М.В. Маркова, О.П. Марунченко, І.М.Милосердна, Г.Г. Почепцов, М.А.Польовий, І.І. Проноза, Ю.М.Твердохліб, В.В. Остроухов В.М. Петрик, М.М. Присяжнюк, М.І.

Сенченко, Є.Д. Скулиш, М.О. Туранський, А.О. Фісун, Л.Г. Чистоклетов, В.Й. Шишко та інші.

Наукова новизна полягає у тому, що у вітчизняній політичній науці представлена дисертація є першим цілісним фундаментальним дослідженням інформаційних війн з позиції інтегрального підходу не лише з доктринальної точки зору та історичного підходу, але й з позиції її утілення на тлі російсько-української війни.

У дисертації надано низку авторських понять, ідей та висновків, які характеризуються науковою новизною. Основними з них є такі:

уперше:

викладено визначення теоретичної дефініції «інформаційна війна» як комбінації людських або технологічних дій, призначених для присвоєння, видалення чи зміни інформації, що призводить до пошкодження або знищення критичної інфраструктури, порушення сталої роботи органів державної влади, економічних збитків у великих розмірах або порушення адекватного ментального сприйняття явищ і подій шляхом нав'язування певного бачення реальності;

сформульовано існуючі на фоні російсько-української війни способи протидії інформаційно-психологічній війні, до яких віднесено невпинне виправлення і встановлення фактів щодо російського вторгнення, роботу Центру протидії дезінформації при РНБО України, розвінчування підступних принижувальних дискурсів щодо історичних фактів, поступове вирішення питання монументальної пропаганди;

вказано на недоцільність вживання терміна «теорія змов», адже теорія – це не просто ідея, а висновки або їх сукупність, які виведені шляхом ретельного аналізу фактів, між тим, щодо теорії змови це просто неможливо, оскільки це судження без фактів: в основі конспірології – прихована сторона реальності, це невидимий світ секретних операцій із зловіщою таємною спільнотою, тому, конспіраціонізм – це, швидше, соціальна гіпотеза;

визначено збройний арсенал інформаційно-технічної зброї, яка націлена на збір конфіденційної інформації, доступ до мережі, може погіршувати роботу мережі, у тому числі призводити до відмови роботи усього сервісу, погіршувати або змінювати роботу одного чи декількох вузлів мережі, активізувати шкідливий код. До інформаційно-технічної зброї належить чотири основних методи. Першим є атаки спрямовані на перевантаження ресурсу запитами, аби вичерпати їх фільтрувальну здатність – такі дії призводять або до сповільнення, або до зупинки роботи інформаційної системи. Другим є метод міжсайтового скриптингу (XXS), що пов'язаний із вразливістю веб-сайтів. Третім є метод соціально-технічної інженерії. Четвертий метод – встановлення шкідливого програмного забезпечення без згоди власника.

удосконалено

перелік форм інформаційної війни – у цьому контексті найбільш доречним видається виділення трьох найчастіше вживаних: інформаційна атака (кібератака якщо мова йде про інформаційно-технічну війну), інформаційна операція, інформаційна кампанія;

дефініцію інформаційно-технічної війни під якою розуміється будь-який тип інформаційного впливу із застосуванням програмно-математичної інформаційної зброї, метою якого є вплив на функціонування інформаційної системи шляхом незаконного доступу до інформаційної системи, здолаття системи захисту, обмеження доступу законних користувачів з можливістю подальшого несанкціонованого збору, копіювання, перехоплення, блокування або видалення інформації;

поняття інформаційно-психологічної війни – це інструмент впливу політичної, військової, економічної, ідеологічної дії, логічне застосування якого дозволяє: 1) впливати на формування громадської думки (у т.ч. викликати інакомислення, невдоволення чи навпаки – підтримку у населення); 2) захистити національні інтереси шляхом зниження морального духу, бойової ефективності

ворогів; 3) впливати на поведінку іноземних держав, неурядових організацій, окремих груп чи осіб.

набули подальшого розвитку

у рамках уже існуючих підходів запропоновано стадійний вимір інформаційних війн розділити на чотири етапи;

виділено ознаки пропаганди як основного методу інформаційно-психологічної війни, до яких віднесено односторонність аргументів; виправдання результатами; байдужість до логічних роздумів і доказової бази; емоційна мова і переконливі визначення; «квазіодноголосся»; створення накопичувального повідомлення у ЗМІ;

розвиток вчення щодо наповнення інструментарію інформаційно-психологічної війни, до якого віднесено дезінформацію, яка є більш широким терміном, ніж популярний fake news, пропаганду та теорії змов;

підходи до розуміння інформаційно-психологічної війни з точки зору теорії комунікації, зокрема визначено найчастіше вживані мовностилістичні засоби інформаційно-психологічної війни: риторичні (мовні) фігури; ідеологеми; міфологеми; інфологеми; метафори; пейоративи; неологізми; евфемізми; гіперболізація. В окремих випадках інформаційно-психологічна війна супроводжується наявністю певної символіки, гасел із стилістичними і риторичними властивостями і специфічними способами звернення;

підходи до особливостей інформаційно-технічної війни (кібервійни): 1) це війна між суверенними державами, яка ведеться за допомогою кіберзброї; 2) кібервійна як становище у кіберпросторі тісно межує із кіберзлочинністю, кібершпигуванням, що робить розмитим її межі; 3) кібервійна може бути частиною збройного конфлікту, як міжнародного так і внутрішнього.

Практичне значення одержаних результатів. Дисертаційне дослідження може бути використано у науково-педагогічній діяльності при підготовці матеріалів та удосконаленні тематичних планів дисциплін політичного циклу; у

науково-дослідній роботі дослідження може слугувати джерелом для інших робіт; в практичній діяльності суб'єктів політики може бути складовою політичної комунікації.

Апробація результатів дослідження. Основні аспекти наукового дослідження обговорювалися на засіданнях та фахових семінарах кафедри політичних теорій НУ «ОЮА». Окремі положення дисертаційного дослідження висвітлювалися на міжнародних та всеукраїнських науково-практичних конференціях та круглих столах: «Правове життя сучасної України» (м. Одеса, 2020 р.), «Нові завдання та напрями розвитку юридичної науки у XXI столітті» (м.Одеса, 2021 р.), «Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (за нагоди 30-ти річчя проголошення незалежності України та 25-ти річчя прийняття Конституції України)» (м. Одеса, 2021 р.), «Українське суспільство в умовах воєнного стану: сучасні виклики та напрями розвитку» (м.Одеса, 2022 р.), «Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права)» (м.Одеса, 2022 р.), «Сталий розвиток суспільства та держави: сучасні виклики та напрями розвитку» (м.Одеса, 2022 р.), «Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень» (м.Одеса, 2023 р.).

Публікації. Результати дисертації було висвітлено у 4 фахових виданнях, які розкривають основний зміст дисертації, із яких 1 стаття опублікована у періодичному виданні іноземної держави та 3 статті опубліковано у наукових виданнях, включених до переліку наукових фахових видань України. Крім того, окремі результати дослідження висвітлено у 7 тезах конференцій.

Структура та обсяг дисертації. Дисертація складається із вступу, трьох розділів, висновків, списку використаних джерел (221 найменування) і додатків.

Загальний обсяг дисертації становить – 206 сторінок, з яких основний зміст – 179 сторінок.

РОЗДІЛ 1. ВИЗНАЧЕННЯ ПОНЯТТЯ ІНФОРМАЦІЙНИХ ВІЙН ТА ЇХ РОЛІ У ПОЛІТИЧНОМУ ПРОЦЕСІ

1.1. Ступінь наукової розробленості проблеми.

Теорія інформаційних війн – дослідницька проблема, яка потребує звернення до масиву наукової літератури, адже її складові характеризуються численними інтерпретаційними значеннями.

Теоретичне обґрунтування інформаційно-психологічного впливу з'явилося у роботах давніх часів, наприклад, «Діалогах» Платона, «Риториці» Аристотеля у Артахаштрі (IV ст. до н.е.) – згідно із індійським трактатом, наприклад, «дипломати повинні володіти різнобічними якостями, вони наділені широким колом обов'язків, вирішують складні завдання та застосовують таємні засоби... повинен збирати інформацію... вивчати місця розташування військ, міцність укріплень... У момент переговорів він має відслідковувати психологічну реакцію протилежної сторони на свої слова... Посол повинен налагодити роботу шпигунів, які вивчатимуть внутрішньополітичну ситуацію в державі перебування, її слабкі місця, отримувати відповідну інформацію через моніторинг настроїв найнижчих верств населення...»¹.

У V ст. до н.е. вийшла книга китайського філософа і генерала Сунь-Цзи «Мистецтво війни», яка розповідає про виграну війну без бою: «Всі війни засновані на обмані. Відповідно, коли ми можемо атакувати, ми повинні здаватися недієздатними. Використовуючи наші сили, ми повинні здаватися бездіяльними. Коли ми поруч, ми змушуємо ворога повірити, що ми далеко. Коли ми далеко, ми повинні змусити ворога повірити, що ми поруч»², – пише Сунь-Цзи. Сунь-Цзи наполягав на необхідності знайти компроміс між правдою і брехнею, щоб дезінформація виглядала якомога достовірніше й була ефективною.

¹ Пиріг Р. Дипломатія та зовнішня політика в «Артахаштрі». *Зовнішні справи*. 2013. № 7. С. 52-55.

² Sun T. The art of war: the oldest military treatise in the world. *Project Gutenberg* : веб-сайт. URL: <https://www.gutenberg.org/files/132/132-h/132-h.htm> (дата звернення: 18.09.2020).

Процес невинної трансформації інформаційних війн відбувався паралельно із теоретичним осмисленням: спочатку – їхніх окремих складових. Однак, ґрунтовно пропаганда та інші методи інформаційної війни почали вивчатися у ХХ ст.

Німецький соціолог Й. Пленге у 1922 р. визначив пропаганду як «поширення інтелектуальних імпульсів, які повинні викликати дії»¹. Паралельно із ним в Америці теорію пропаганди створював і У.Ліппман, який сильно вплинув на Е. Бернейза, що був одним із найвідоміших членів комісії Дж.Крила. Е.Бернейз – автор книги «Пропаганда» (1928 р.) вважав, що маніпулювання необхідне для демократії: «Свідоме і розумне маніпулювання звичками і організованою думкою мас є важливим елементом демократичного суспільства. Ті, хто маніпулює... складають невидимий уряд, який є реальним керівником нашої країни. Ми – керовані: наші думки сформовані, наші смаки сформовані, наші ідеї запропоновані... Це логічний результат організації нашого демократичного суспільства... Практично у кожній дії нашої буденності, будь то політична чи економічна сфера, у наших соціальних чи етичних правилах, існує відносно невелика кількість людей... які розуміють психічні процеси і соціальні моделі мас. Саме вони тягнуть ниточки, які контролюють суспільну думку». Е.Бернейз надав наступне визначення пропаганди: «Сучасна пропаганда – це послідовні, стійкі зусилля по створенню або формування подій, щоб вплинути на ставлення суспільства до підприємства, ідеї або групи»². Визначення Е.Бернейза відділяє «сучасну» пропаганду від старих концепцій пропаганди і відповідає широкому значенню пропаганди, яке включає і рекламу.

Гарольд Д. Лассвелл, у рамках американських досліджень пропаганди, визначив дефініцію у «Техніці пропаганди у світовій війні» (1927 р.) як

¹ Plenge J. Deutsche Propaganda. Die Lehre von der Propaganda als praktische Gesellschaftslehre. Bremen, 1922. P. 13.

² Bernays E.L. Propaganda. New York, 1928. P. 25.

«мобілізацію думок» і «управління думками і поглядами за допомогою виразних символів»¹.

Після Другої світової війни велися дослідження не лише нацистського пропагандистського апарату. Паралельно вивчалася, також британська і американська пропаганда в ХХ ст., з'являлися компаративістські дослідження із пропагандистських протистоянь під час двох світових війн. Вивчаючи цей період, слід згадати тритомник Ханнса Бучлі «6000 років реклами. Історія комерційної реклами і пропаганди» і Альфреда Штурмінгера «3000 років політичної пропаганди» – ремейк агітаційного видання епохи нацизму, «Пропаганда і психологічна війна» Теренса Х. Куалтера, написана в 1962 році.

Термін «інформаційна війна» з'явився лише у середині 70-х рр. ХХ ст. На Заході «батьком» інформаційних війн називають ученого-фізика Томаса Рона, який в 1976 р., у розпал «холодної війни», у звіті «Системи зброї й інформаційна війна» назвав інформацію найслабшою ланкою збройних сил і оборони. Офіційно цей термін вперше був ужитий у директиві міністра оборони США №3600 від 21 грудня 1992 р. У жовтні 1998 р. Міністерство оборони США ввело в дію «Об'єднану доктрину інформаційних операцій», у якій інформаційна війна визначалася як «комплексний вплив (сукупність інформаційних операцій) на систему державного і військового управління супротивної сторони, її військово-політичне керівництво, який вже в мирний час призводив би до прийняття сприятливих рішень для сторони-ініціатора інформаційного впливу, а протягом конфлікту повністю паралізував би функціонування інфраструктури управління супротивника»². У науковий обіг дефініцію «інформаційна війна» ввів американський дослідник

¹ Lasswell H.D. The theory of political propaganda. *The American Political Science Review*. 1927. Vol. 21. P. 627-631. URL: <https://www.jstor.org/stable/1945515> (дата звернення: 08.02.2022).

² Погрібна В.Л., Герасіна Л.М. Інформаційна війна як каталізатор геополітичних змін. *eNULAUIR* : веб-сайт. URL: http://dspace.nlu.edu.ua/bitstream/123456789/11320/1/Pogribna_Gerasina_72-75.pdf. (дата звернення: 16.07.2021).

М. Маклюен, який проголосив тезу: «Істинно тотальна війна – це війна за допомогою інформації».

Термін «кібервійна» було уведено у 1993 р. експертами із безпеки Джоном Аркілом та Девідом Ронфельдтом для опису «війн майбутнього» (того ж року сталося масове враження комп'ютерним вірусом, серед них були і комп'ютери Білого дому) у зв'язку із оновленням інформаційних технологій у воєнних технологіях і переосмислення війни. Тоді автори під терміном розуміли перш за все терористичні атаки зі сторони недержавних суб'єктів, по-друге, Аркіла і Ронфельдт намагалися описати зростаючу інтеграцію кіберкомпонентів у систему воєнної безпеки.

У 1995 р. М.Лібікі написав роботу «Що таке інформаційна війна?», яка характеризується комплексним підходом. У роботі автор відзначає: «...є кілька різних форм інформаційної війни... командно-адміністративна війна, війна на основі розвідки, радіоелектронна боротьба (радіоелектронна або криптографічні методи), психологічна війна, «хакерська» війна, економічна інформаційна війна, кібервійна»¹.

Принагідно відмітимо, що приставка «кібер-» відсилає нас до терміна «кібернетика». Термін «кібернетика» насправді не неологізм, попри те, що його активне використання розпочалося із 1947 р. (за декілька десятиліть до початку перших кібератак), воно зустрічається, наприклад, у роботах Платона, де означало «мистецтво керування кораблем», а у переносному сенсі – «мистецтво керування людьми». У 1834 р. французький фізик А.М. Ампер при класифікації наук назвав кібернетикою «науку про керування державою», разом із наукою про права народів (етнодицея), дипломатією і теорією влади вони відносилися до політичних наук, до того ж, кібернетика і теорія влади за Ампером утворювали політику у власному сенсі цього слова².

¹ Libicki M.C. What is information warfare? Washington : National defense university, 1995. P.10.

² Ampere A.M. Essai sur la philosophie des sciences. Paris : Bachelier, 1843. 2nd partie. P. 140–142.

Таким чином, вживання самого прикметника «кібернетична» видається надто широким, однак, оминати приставку «кібер-» з огляду на її входження у словникову, наукову літературу та законодавство неможливо, хоча, на наш погляд, найбільш вдалим видається термін «інформаційно-технічна», він робить вказівку на основну мету інформаційно-технічної війни – інформацію (а саме її цілісність, доступність, конфіденційність), і засоби – технічні.

Осмислення вітчизняної теорії інформаційних війн неможливе без звернення до фундаментальних монографічних досліджень.

У 2007 р. інформаційні війни, переважно у контексті інформаційно-психологічної парадигми досліджувалися В. Брижком, М. Швецем та В. Цимбалюком. Результати дослідження було викладено у монографії «Е-боротьба в інформаційних війнах та інформаційне право». У другому розділі монографії «Інформаційна боротьба в цивільному суспільстві», зокрема, приділяється увагу маніпулюванню, його сутності, видам, ролі ЗМІ у маніпулюванні свідомістю. Брехня, обман та дезінформація визначається як основні чинники маніпулювання.

Г.Г. Почепцов – один із найвідоміших теоретиків інформаційних війн. У його роботі «Сучасні інформаційні війни» викладено історію виникнення інформаційних війн, їх методологію, досліджено її зв'язок із національною безпекою та місце інформаційних війн у структурі сучасних цивілізацій. Проведено паралелі між інформаційними та смисловими війнами.

У монографії «Війни інформаційної епохи: міждисциплінарний дискурс» за редакцією В.А. Кротюка викладено «науково-методологічні підходи до розуміння феномена сучасної війни і авторське бачення даної проблематики в філософському, політологічному, психологічному та правовому вимірах»¹. Зосереджено увагу на природі війн інформаційної епохи, їх стратегіях та технологіях, викладено окремі позиції щодо протидії, у тому числі, методам інформаційно-психологічної війни.

¹ Війни інформаційної епохи: міждисциплінарний дискурс : монографія / за ред. В.А. Кротюка. Харків : ФОП Федорко М. Ю., 2021. С.9.

Науковець Б.М. Калініченко у роботі «Інформаційна війна: чинники ескалації та засоби протидії» серед іншого дійшов висновку, що «інформаційна війна складається з багатьох окремих елементів та аспектів, вона є явищем, утвореним різними видами інформаційного протистояння...Духовна складова цієї війни пов'язана зі стереотипами мислення, світоглядними та ідеологічними засадами індустріальної цивілізації. Технологічна складова послуговується засобами маніпулювання, кібертехнологій інформаційної цивілізації»¹.

Д.В. Дубов у монографії «Кіберпростір як новий вимір геополітичного суперництва» робить спробу категоріально-понятійного осмислення кібербезпекової теорії та робить вказівку на досі існуючу проблему: «Незважаючи на те, що такі поняття, як кіберпростір, кібервійна, кібератака та кібертероризм, широко використовуються в науковій і публіцистичній літературі, дотепер невизначеним є їх зміст, що значно ускладнює наукове осмислення та практичне освоєння проблеми загроз у кіберпросторі»².

У монографії В.Д. Кіслова висвітлено бачення сутності та методів інформаційних війн, крім того, автор торкається проблеми кібертероризму та Інтернету у міжнародних інформаційних війнах.

Зарубіжні учені С.Джаджодіа, П.Шакарян та ін. дослідили воєнні та політичні аспекти кібервійни у роботі: «Кібервійна: створення наукової основи». Багаторівневий підхід, запропонований у роботі дає уявлення про способи протидії кібервійнам.

У роботі Г.В. Певцова, А.М. Гордієнка, С.В. Залкіна, С.О. Сідченка, А.О. Феклістова, К.І. Хударковського «Інформаційно-психологічна боротьба у воєнній сфері» характеризуються конфлікти ХХІ ст. та визначено роль

¹ Калініченко Б.М. Інформаційна війна: чинники ескалації і засоби протидії [Електронний ресурс] / Національний педагогічний університет імені М. П. Драгоманова. Київ, 2020. С.261.

² Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ : НІСД, 2014.С.69.

інформаційно-психологічної боротьби у них. Зосереджено увагу на функціях органів протидії інформаційно-психологічним операціям у зарубіжних країнах та надано рекомендації щодо впровадження позитивного досвіду у вітчизняну систему.

Формування політичної конструкції інформаційних війн відбувається на рівні дисертаційних досліджень.

У 2012 р. вітчизняна політична наука побачила дослідження О.П. Марунченка «Інформаційна війна в сучасному політичному просторі», у якій не лише викладено бачення інформаційної війни як теоретичної дефініції, розкрито її еволюцію та сутність, але яка характеризується глибоким прикладним аспектом: другий розділ дисертації присвячено інформаційній війні у сучасній політичній практиці, а у третьому – зосереджено увагу на інформаційній війні в Україні. Відмітимо, що попри те, що з моменту захисту дисертаційного дослідження пройшло 11 років, ряд проблем, поставлених автором залишаються або невирішеними, як-от: «не секрет, що в Україні серйозні проблеми створює діяльність зарубіжних ЗМІ», «електронне шпигування стало суворою реальністю» або дискусійними, наприклад: «поки що в теорії політичної науки не сформувалося єдине універсальне поняття інформаційної війни»¹.

М.О. Туранський у дисертаційному дослідженні «Інформаційно-психологічне забезпечення операції з анексії Криму Російською Федерацією: історичні передумови та практична реалізація», серед іншого, розробив «періодизацію інформаційного завоювання Росією мешканців Кримського півострова від латентної фази ІПсО, через ескалацію до постанексійного зниження напруги довкола цього питання. Зокрема, латентна фаза включала у себе окремі ІПсО, які здійснювалися за чотирма етапами цієї фази та були спрямовані передусім на ретельно визначені цільові аудиторії. У цей час з громадських організацій та

¹ Марунченко О.П. Інформаційна війна в сучасному політичному просторі : дис. ... канд. політ. наук : 23.00.02. Одеса, 2012. С.173, 175, 177.

партій на півострові була створена проросійська платформа, яка стала основою підтримки пропагандистського впливу російських ЗМІ»¹.

Вагомий внесок у розробку категоріального апарата інформаційно-психологічних війн зробила Ю.М.Твердохліб у дисертації на тему: «Інформаційно-психологічні операції у російсько-українській гібридній війні», робота якої була зосереджена у тому числі і на потребі «виключення двозначності, оскільки значна частина термінів у вітчизняній науці досі не має єдиної та чіткої дефініції попри існування великої кількості праць»². У роботі також наголошено, що «поняття «інформаційної війни» та «інформаційно-психологічної війни» не є тотожними.

І.О. Валушко у дисертаційному дослідженні «Інформаційна безпека України в контексті російсько-українського конфлікту» висловив власне бачення на розуміння мети, методів та інструментів інформаційної агресії проти України, приділив увагу осмисленню ЗМІ як інструменту інформаційної безпеки.

Навчальні посібники дозволяють впорядкувати вчення про інформаційні війни і доступно донести його до усіх зацікавлених осіб. Із досліджуваної тематики одними із таких є навчальні посібники: О.В. Курбана «Сучасні інформаційні війни в мережевому он-лайн просторі». Окрім викладення теорії інформаційних війн, її стратегії та тактики, робота написана із урахуванням історичного підходу – у ній викладено бачення інформаційних війн, починаючи із первісних часів. Особливу увагу приділено ролі он-лайн простору у веденні інформаційних війн; «Гібридна війна і журналістика» (за загальною редакцією В.О. Жадька), у якому розглянуто характерні ознаки інформаційних війн в історії та сучасності, надано авторське розуміння розмежування понять «інформаційна війна» та «сміслова війна».

Міркування щодо інформаційних війн викладалися ученими у наукових виданнях України.

¹ Туранський М.О. Інформаційно-психологічне забезпечення операції з анексії Криму Російською Федерацією: історичні передумови та практична реалізація : дис. ... доктора філософії : 032. Львів, 2020. С.191-192.

² Твердохліб Ю.М. Інформаційно-психологічні операції у російсько-українській гібридній війні : дис...канд.політ.наук : 23.00.04. Чернівці, 2019. С.2.

Закономірності історичного процесу інформаційних війн розкрито у наукових статтях І.О. Валюшка «Еволюція інформаційних війн: минуле та сучасність» присвячена ролі інформації у веденні війн у минулому та на сучасному етапі. Науковець акцентує увагу не лише на окремих аспектах трансформації інформаційного протиборства, але й розмірковує про те, як розвиток інформаційних технологій змінив підходи до самої війни; Л.П. Макаренко «Еволюція форм та методів ведення інформаційної війни». Дослідження Б.В. Довганя, О.В. Мартинюк «Становлення і розвиток поняття інформаційної війни» також присвячено еволюції інформаційних війн. Серед іншого, науковці вказують на певні альтернативи для боротьби з інформаційною агресією. А окремі дослідження зорієнтовані на конкретний вид протидії серед таких робота С.В. Куцепал «Критичне мислення як засіб спротиву в інформаційній війні».

І.І.Проноза у роботі «Інформаційна війна: сутність та особливості прояву» розглядає інформаційні війни крізь призму чотирьох підходів – психологічного, геополітичного, конфліктологічного та системного. П.С.Шпиґа, Р.М.Рудник у праці «Основні технології та закономірності інформаційної війни» надали авторську дефініцію поняттю, визначили основні ознаки та наслідки інформаційних війн. Крім того, у роботі приділено увагу учасникам інформаційних війн, їх формам, напрямам використання інформаційної зброї; визначено ЗМІ як основний інститут інформаційних війн.

В.С.Яковчук, Б.І.Малець, Ю.О.Борзов у науковій статті «Інформаційні війни в сучасному світі» роблять вказівку на інформаційну війну як складову ідеологічної боротьби, а М.Пілат у роботі «Інформаційні впливи та інформаційні війни: сутність понять та їх взаємозв'язок в інформаційну епоху» розглядає змістовне наповнення концепції інформаційної війни, зокрема, з точки зору проблеми протиправного застосування спеціальних засобів впливу на свідомість. Дослідженню інформаційних впливів присвячено і наукову статтю Л.Г.Чистоклетова,

В.Й.Шишко «Інформаційно-психологічні впливи як невід’ємна складова парадигми інформаційної безпеки».

До питання класифікації інформаційних війн звертався Я.Малик у науковій статті «Інформаційна війна і Україна». Серед іншого, автор викладає бачення завдань інформаційних війн, визначає об’єкти та звертається до прикладного аспекту – інформаційної війни проти України.

Ряд досліджень розкривають теоретичний зміст інформаційної зброї: В.О.Хорошко, Ю.Є.Хохлачова, Т.П.Пірцхалава, І.С.Іванченко «Інформаційна зброя як інструмент інформаційної війни»; стаття І.М.Харченка, С.О. Сапогова, В.М.Шамраєвої, Л.В.Новікової «Основні засоби інформаційного протистояння та інформаційної війни як явища сучасного міжнародного процесу» присвячена роботі інформаційної зброї у контексті інформаційно-технічної війни.

Робота В.М.Огаренка, А.Г.Стадник «Засоби масової комунікації в інформаційній війні: соціологічний підхід у визначенні аспектів впливу» присвячена аналізу механізмів впливу ЗМІ на громадську думку.

У науковій статті М.В. Маркової, А.Р. Маркова «Інформаційно-психологічна війна проти населення України як сучасна реальність: стан проблеми і подолання наслідків» розкривається поняття, ознаки та зміст інформаційно-психологічної війни, її завдання, об’єкти та викладено історичне бачення інформаційно-психологічної війни від перших її зародків. Н.О. Марута, М.В. Маркова у роботі «Інформаційно-психологічна війна як новий виклик сучасності: стан проблеми та напрямки її подолання» підходять до розуміння інформаційно-психологічної війни як складової гібридних війн; виокремлюють маніпулятивні впливи на масову та індивідуальну свідомість та приділяють увагу заходам протидії в інформаційно-психологічній війні. Крім того, М.В. Маркова є автором роботи «Інформаційно-психологічна війна: медико-психологічні наслідки та стратегії протидії».

Інформаційно-психологічні війни відображають відтінки національної специфіки, тому окремі дослідження стосуються видів інформаційно-психологічної

зброї: Б.Д. Чорномаз є автором статей «Менталітет та історична пам'ять в інформаційній війні» та «Національна пам'ять як зброя в інформаційній війні», де, зокрема, «наводяться неспростовні докази того, що історичні знання є одним із видів інформаційної зброї...»¹.

Дослідженню окремих методів інформаційно-психологічної війни присвячено роботи таких учених як: Є.Джиджора «Теорія змови як пропагандистська модель комунікації (як вишки 5G пов'язані з коронавірусом та «вакцинами Білла Гейтса»)», де проаналізовано маніпулятивні прийоми окремих теорій змов: «обрізання мультимедійного повідомлення у потрібному місці, зміщення акцентів у дискурсі, безапеляційна констатація припущень, нагнітання ірраціонального (релігійного) страху»²; Г.Г. Почепцов «Пропаганда: основні характеристики», у якій зацентовано увагу на окремих аспектах радянської пропаганди, наведено класифікаційні моделі пропаганди та виділено основні її риси; С.Шпилик «Інформаційна війна, пропаганда та PR: такі схожі й такі різні...», у якій автор відзначає, що «інформаційна війна і зв'язок з громадськістю схожі тільки на етапі реалізації цілей, проте самі цілі принципово різні»³; М.Б. Шевцев, К.А. Гончарук «Пропаганда як соціально-політичне явище: проблеми розуміння», Ж.З. Денисюк «Пропаганда та контрпропаганда в контексті стратегій державної інформаційної політики», А.Гурківська «Концептуалізація поняття «політична пропаганда», В.Е. Гапій «Пропаганда як інструмент впливу на підсвідомість людини в сучасній Україні», М.А. Авдєєва «Фактор м'якої сили у російсько-українських відносинах», Н.Б. Белоусова «М'яка» сила як потенціал зовнішньополітичного впливу держави», А.Гребенюк «Антиукраїнська пропаганда: характерні риси та поняття», В.А.Полторак, А.Г.Стадник «Пропаганда

¹ Чорномаз Б.Д. Національна пам'ять як зброя в інформаційній війні. *Науково-теоретичний альманах «Грані»*. 2019. № 22 (11). С. 69-80.

² Джиджора Є. Теорія змови як пропагандистська модель комунікації (як вишки 5G пов'язані з коронавірусом та «вакцинами Білла Гейтса»). *Діалог: медіа-студії*. 2020. № 26. С.37-51.

³ Шпилик С. Інформаційна війна, пропаганда та PR: такі схожі й такі різні. *Галицький економічний вісник*. 2014. Том 47. № 4. С. 178-188.

та її місце в процесі ведення інформаційних війн. Основні форми пропагандистського впливу: пряма пропаганда, Джинса, пабліситі, пропаганда 2.0», Н.Войтович «Створення фейкових новин: новий шлях інформаційної війни», О.Звоздецька «Дезінформація як загроза національній безпеці Європейського Союзу: проблеми та підходи», М.О. Кіца «Фейкова інформація в українських соціальних медіа: поняття, види, вплив на аудиторію», В.І.Маляренко «Кращі практики зарубіжного досвіду боротьби з фейками та дезінформацією», Р.Ф.Черниш «Фейк як один із інструментів негативного впливу на національну безпеку України в умовах ведення гібридної війни», О.Бойко «Чутка як інструмент політичного маніпулювання», В.В.Воротинський «Чутки як інструмент політичного маніпулювання в Інтернеті», А.Канарська «Пропаганда й маніпуляції в інформаційній сфері», О.І.Ткач «Особливості використання комунікативних властивостей чуток у політичному маніпулюванні», Н.Вітюк «Особливості дискурсу політичної пропаганди в умовах інформаційно-психологічної війни».

Серед зарубіжних учених – дослідників методів інформаційно-психологічної війни: Саманта Сенн (Samantha Senn) «Усіляка пропаганда небезпечна, але деяка – небезпечніша за інші: Джордж Орвелл і використання літератури у якості пропаганди» («All propaganda is dangerous, but some are more dangerous than others: George Orwell and the use of literature as propaganda»), Дуглас Волтон (Douglas Walton) «Що таке пропаганда і що з нею не так» («What Is Propaganda, and What Exactly Is Wrong with It»), [Корі Е. Добер](#), [Керол К. Вінклер](#) ([Cori E. Dauber](#), [Carol K. Winkler](#)) «Радикальна візуальна пропаганда в онлайн-середовищі» («Radical visual propaganda in the online environment: an introduction»), Філіп М.Тейлор (Philip M. Taylor) «Нова пропаганда: психологічні та інформаційні операції» («The new propaganda: psychological and information operations»), [Норман Васу](#), [Бенджамін Анг](#), [Террі-Енн Тео](#), [Шаши Джаякумар](#), [Мухаммад Файзал](#), [Джухи Ахуджа](#) ([Norman Vasu](#), [Benjamin Ang](#), [Terri-Anne Teo](#), [Shashi Jayakumar](#), [Muhammad Faizal](#), [Juhi Ahuja](#)) «Розпаковка фейкових новин» («Unpacking Fake News»), «Методи

розповсюдження в дезінформаційних кампаніях» («Dissemination Techniques in Disinformation Campaigns») [Андреа Черазе](#), [Клаудія Санторо](#) ([Andrea Cerase](#), [Claudia Santoro](#)) «Від расових містифікацій до ажіотажу в ЗМІ: реальні наслідки фейкових новин» («From racial hoaxes to media hypes»), Пітер В. Пол (Peter V. Paul) «Фейкові новини, альтернативні факти, постправда, дезінформація, невірне тлумачення та інші проблеми, пов'язані із генерацією знань» («Fake News, Alternative Facts, Post-Truths, Misinformation, Misinterpretation—and Other Challenges Associated With Knowledge Generation»), Ніл Кумар Катял (Neal Kumar Katyal) «Теорія змови» («Conspiracy Theory»), [Дж. Ерік Олівер](#), [Томас Дж. Вуд](#) ([J. Eric Oliver](#), [Thomas J. Wood](#)) «Теорія змови і параноїдальний стиль громадської думки» («Conspiracy theories and the paranoid style (s) of mass opinion»), Джозеф Е.Усинські, [Кейсі Клофстад](#), [Метью Д. Аткинсон](#) ([Joseph E. Uscinski](#), [Casey Klofstad](#), [Matthew D. Atkinson](#)) «Що рухає конспірологічними переконаннями? Роль інформаційних сигналів і схильностей» («What drives conspiratorial beliefs? The role of informational cues and predispositions») та інші.

Формам інформаційної війни присвячено роботи О.Левченка «Форми ведення інформаційної боротьби: практичний підхід до понятійного апарату», О.П. Сікорського, М.Ю. Якобчука «Інформаційно-психологічні війни: форми та методи», Ю.Мороза, Ю. Твердохліб «Інформаційно-психологічні операції в умовах ведення гібридної війни», Ю.М.Твердохліб «Інформаційно-психологічні операції: процес планування та реалізації»

У науковій статті Є.Тихомирової «Російська інформаційна війна: теоретичні та практично-прикладні аспекти» приділено увагу створеним у Росії підрозділам для ведення інформаційного протиборства в Інтернеті. Натомість, у роботі А.Г. Стадника «Інформаційна війна як комунікативна технологія впливу на масову свідомість та громадську думку» інформаційна війна розглядається «не як допоміжний механізм реальної війни, а як механізм впливу саме на громадську думку... У статті детально обговорюються чотири основні чинники, які визначають

ефективність інформаційного впливу: 1) суб'єкти інформаційних війн, які впливають на населення, масову свідомість, громадську думку; 2) інформаційна зброя війни; 3) сам контент, зміст інформації, що транслюється у ході інформаційної війни; 4) специфіка масової свідомості населення у тих чи інших країнах, формування та функціонування у них громадської думки»¹. І.Мудра, Є.Сінькова у праці «Інструменти інформаційної війни проти України в Інтернет-ЗМІ» приділили увагу інтернет-ЗМІ, які є учасниками інформаційної війни проти України. Г.В.Сасин у науковій статті «Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір)» досліджує інформаційні атаки Росії проти України та аналізує застосування країною-агресором засобів та методів інформаційного впливу. Комарчук О. «Маніпулятивні технології російських ЗМІ в рамках сучасної гібридної війни», В.Лизанчук «Просвітницька та маніпулятивна пропаганда в умовах нинішньої російсько-української війни», А.Іванець «До питання про використання Росією монументальної пропаганди як елементу окупаційної політики на тимчасово окупованій території Криму у 2014-2018 роках».

П.П.Черник, А.В.Шумка у своїй роботі «Інформаційно-психологічні операції у війнах та збройних конфліктах другої половини ХХ-початку ХХІ ст.» приділили увагу використанню методів інформаційно-психологічної війни у зарубіжних країнах.

На необхідності вироблення нових методів інформаційної боротьби на фоні російської агресії проти України наголошували науковці: О.В.Ауліна у науковій статті «Специфіка застосування асиметричних підходів в інформаційному протиборстві», І.М.Сопілко у роботі «Інформаційна війна проти України та правові засоби протидії злочинним діям», І.Мудра, Є.Сінькова у праці «Інструменти інформаційної війни проти України в Інтернет-ЗМІ». Боротьбу з пропагандою як

¹ Стадник А.Г. Інформаційна війна як комунікативна технологія впливу на масову свідомість та громадську думку. *Науково-теоретичний альманах «Грані»*. 2016. № 1. С. 111-115.

основним методом інформаційно-психологічної війни зокрема, у контексті російсько-української війни досліджували: О.В.Безтільна «Боротьба з пропагандою російських ЗМІ», А.Ю.Даценко «Стратегічні напрями боротьби з російською пропагандою і дезінформацією в інформаційному просторі України», Є.А.Макаренко «Протидія російській пропаганді на міжнародній арені: європейський вимір» тощо.

Серед зарубіжних учених – дослідників російської інформаційно-психологічної війни Леон Арон (Leon Aron) «Російська пропаганда: шляхи і засоби» («Russian propaganda: ways and means»), [Кристофер Пол](#), [Міріам Метьюз](#) ([Christopher Paul](#), [Miriam Matthews](#)) «Російська модель пропаганди: чому вона може працювати і як їй протидіяти» («The Russian «Firehose of Falsehood» propaganda model: why it might work and options to counter it»), Стефан Мейстер (Stefan Meister) «Путінська версія м'якої сили» («Putin's version of soft power»), Майкл Дженсен (Michael Jensen) «Російські тролі і фейк-новини: інформація чи логіка ідентичності?» («Russian trolls and fake news: information or identity logics») та інші.

Окремі аспекти інформаційно-технічних війн (кібервійн) розкрито у публікаціях С.Вдовенка, Ю.Даника, С.Фараона «Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення», Р.В. Бараненка, А.Ю. Задорожної «Кібервійна як новий вид протистояння держав», М.В. Камчатного «Основні ознаки поняття «кібервійна» в сучасному міжнародному праві» та «Заборонені засоби ведення кібервійни», А.В.Слободяннюк, К.М.Писаренко «Аналіз небезпеки кібервійни на сучасній світовій арені», Я.В.Дмитрук, Т.О.Гришанович, Л.Я.Глинчук, О.К.Жигаревич «Кібервійна як різновид інформаційних війн. Захист кіберпростору України», Р.В.Бараненка, В.С.Полякова «Кібервійни: основні проблеми забезпечення інформаційної безпеки держави», Т.О.Ткачук, І.В.Гамової «Кібернетична війна як різновид інформаційної війни».

Дослідженню кібернетичної зброї як виду сучасної зброї присвячено наукові праці Р.В.Грищука «Кібернетична зброя: класифікація, базові принципи побудови, методи та засоби застосування захисту від неї» та В.Г. Бабенка «Основні групи кіберзброї та особливості її застосування».

Серед зарубіжних науковців, що вивчали питання російсько-української кібервійни виділимо роботи Гібні Е. (Gibney E.) «Де кібервійна Росії? Дослідники розшифровують його стратегію» («Where is Russia's cyberwar? Researchers decipher its strategy»), Машмайєр Леннарт і Міріам Данн Кавелті (Maschmeyer Lennart, and Myriam Dunn Cavelty) «До побачення, кібервійна: Україна як перевірка реальністю» («Goodbye cyberwar: Ukraine as reality check»), С. Мохі Адмад (C. Mohee Ahmad) «Кібервійна: прихована сторона російсько-української кризи» («Cyber war: the hidden side of the russian-ukrainian crisis»), Соесанто Стефан (Soesanto Stefan) «ІТ-армія України: структура, завдання та екосистема» («The IT Army of Ukraine: structure, tasking, and eco-System»).

Загальні питання кібервійн досліджували Дефібо Стівен і Донна Шеффер (Defibaugh Stephen, and Donna Schaeffer) «Чи може теорія виснаження дати розуміння кібервійни?» («Can attrition theory provide insight for cyber warfare?»), Дузе Фредерік, Од Жері та Франсуа Делерю (Douzet Frédérick, Aude Géry, and François Delerue) «Побудова кібермиру під час підготовки до кібервійни» («Building cyber peace while preparing for cyber war»), Колер Кевін (Kohler Kevin) ««Кібернейтральність: запобігання супутній шкоді»» («Cyberneutrality: discouraging collateral damage»), Малецька Агата (Małecka Agata) «Кібероперації згідно з міжнародним правом» («Cyber-Operations under international law»), Марангіоне М.С. (Marangione M.S.) «Тіньова війна: політика кібервійни в Сполучених Штатах, Росії та Китаї» («Shadow Warfare: cyberwar policy in the United States, Russia and China»), Мур Деніел (Moore Daniel) «Наступальні кібероперації: розуміння нематеріальної війни» («Offensive cyber operations: understanding intangible warfare»), Нін Хуаншен

(Ning Huansheng) «Коротка історія кіберпростору» («A brief history of cyberspace») та багато інших.

Серед інших вітчизняних учених, дослідників інформаційних війн та окремих її методів Я.М.Жарков, Л.Ф.Компанцева, В.В.Остроухов В.М.Петрик, М.М.Присяжнюк, Є.Д.Скулиш, А.О.Фісун, В.В.Антонюк, О.В.Литвиненко, В.П.Горбулін, Д.В.Ланде, О.О.Верголяс, О.Г.Заруба, М.П.Сніцаренко, Л.М.Шутяк, С.І.Гаврилюк, О.О.Гойман, О.Дарморіз, О.Дубас, М.Житарюк, І.Крупський, Т.В.Андрущенко, О.Герасименко та ін.

Чи можна на фоні такої інтенсивної публікаційної діяльності стверджувати про незавершеність політичної конструкції інформаційних війн? На наш погляд, – так, і на рівні розуміння поняття – попри те, що усі науковці визнають самодостатність категорії «інформаційних війн», змістовне наповнення цього динамічного явища відрізняється: «понятійно-категоріальний апарат інформаційних воєн ще не сформований остаточно»¹. Триває дискусія щодо того, чи є це поняття синтезом двох базових напрямків – інформаційно-психологічного та інформаційно-технічного, чи до нього доцільно відносити лише один із них; які методи та форми доречно відносити і яке їх співвідношення до інформаційних війн: «є сенс зауважити, що динаміка розвитку інформаційного інструментарію вимагає розмежування розуміння інформаційної та психологічної, інформаційної та кібернетичної війн»²; чи існує кібервійна... багато питань характеризуються системною складністю, вимагають подальших наукових пошуків і тільки посилюються на фоні тиску складних суспільно-політичних процесів.

¹ Кіслов Д.В. Інформаційні війни : монографія. Київ : Київ. нац. торг.-екон. ун-т, 2013. С.56.

² Антонюк В.В. Інформаційна війна в структурі сучасного геополітичного протистояння: нові контексти та інтерпретації. *Державне управління: удосконалення та розвиток* : електронний журнал. URL: http://www.dy.nayka.com.ua/pdf/7_2021/35.pdf (дата звернення: 04.03.2023).

1.2. Концептуальні та методологічні підходи до розуміння інформаційних війн.

Перехід інформації у розряд цінних ресурсів кличе до життя не лише бажання досягти мети – володіти ним, але й вбачає у ньому засіб – новий вид зброї, який став ефективним засобом впливу на міжнародну політичну арену.

Літературних тлумачень поняття «інформація» дуже багато, її зокрема розглядають, як «знання, що може зберігатися; як дані у певному середовищі; як частину комунікаційного процесу тощо»¹. У Законі України «Про інформацію» теж надано визначення: «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді», однак, такий підхід має мінімум один суттєвий недолік – він фрагментарно окреслює поняття, звужуючи його до «матеріальних носіїв і електронного вигляду», між тим, інформація є нематеріальним благом, а матеріальний носій лише може бути використано для її збереження. Більш вдале визначення поняття інформації міститься у ст.1 Закону України «Про захист економічної конкуренції»: «відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги... бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості».

У наукових роботах дефініція «інформаційна війна» не має однозначного трактування. Окрім розбіжностей стосовно того, що ж можна вважати «інформаційною війною», так само проблемним є тлумачення окремих її категорій. Різні науковці пропонують свої підходи: деякі вбачають більшу доречність у вживанні терміна «інформаційні операції», інші схиляються до суто

¹ McCreadie M., Rice R.E. Trends in analyzing access to information. Part I: cross-disciplinary conceptualizations of access *Information Processing and Management*. 1999. Vol.35. P. 45-76. URL: bit.ly/4852AMr (дата звернення: 08.09.2022).

психологічного, або технічного аспекту, використовуючи терміни «мережева війна», «кібервійна», «інформаційно-психологічна війна».

Осмилення інформаційних війн, зокрема, відбувається у рамках психологічної парадигми. В.М.Брижко, визначає інформаційну війну як «відкриті та закриті цілеспрямовані невідомі інформаційні дії щодо нав'язування противнику небажаної інформації для зміни його поведінки через зміну мислення або для самознищення з метою отримання виграшу у матеріальній сфері»¹. І.І. Проноза констатує: «психологічна парадигма дозволяє детально досліджувати механізми впливу на внутрішньоособистісні процеси індивідів, що викликає зміни в ментальній сфері, визначає корекцію логіки світосприйняття і відповідного йому політичної поведінки»². Автори монографії «Війни інформаційної епохи: міждисциплінарний дискурс» теж розглядають поняття із точки зору психологічного підходу і підсумовують: «Головне поле бою перебуває в когнітивній площині...Експерти пропонують наразі нові типи інструментарію інформаційної війни – поведінкову війну, смислову війну та когнітивну війну»³.

П.С.Шпиґа та Р.М. Рудник виділяють чотири підходи до розуміння інформаційних війн: «Перший підхід трактує їх як сукупність політико-правових, соціально-економічних, психологічних дій, що передбачають захоплення інформаційного простору, витіснення ворога з інформаційної сфери, знищення його комунікацій, позбавлення засобів передачі повідомлень, а також інші подібні цілі. За другим підходом інформаційна війна визначається як найгостріша форма протистояння в інформаційному просторі, де першочергового значення набувають такі якості взаємодії, як безкомпромісність, висока інтенсивність суперечки та короткотривалість гострого суперництва. Третій підхід інтерпретує інформаційну

¹ Е-боротьба в інформаційних війнах та інформаційне право : монографія / В.М. Брижко та ін. ; за ред. д.е.н., проф., члена-кореспондента АПРН України М. Швеця. Київ : НДЦПІ АПРН України, 2007. С.142.

² Проноза І.І. Інформаційна війна: сутність та особливості прояву. *Актуальні проблеми політики*. 2018. Вип.61. С.76-84.

³ Війни інформаційної епохи: міждисциплінарний дискурс : монографія / за ред. В.А. Кротюка. Харків : ФОП Федорко М. Ю., 2021. С.496.

війну як форму забезпечення та ведення військово-силових дій за допомогою найсучасніших електронних засобів (цифрових випромінювачів, супутникових передавачів та інших аналогічних засобів, які застосовуються для виконання військових завдань). Четвертий підхід ототожнює інформаційні війни з кібернетичними війнами (протистояння між технічними системами)»¹.

На особливу увагу заслуговує й поліпарадигмальний (комплексний, інтегральний) підхід при визначенні дефініції «інформаційної війни». Е.Б. Талишинський визначає інформаційну війну як «комплексний відкритий, чи закритий цілеспрямований інформаційний вплив однієї сторони, чи взаємний вплив сторін один на одного, що охоплює систему методів і засобів впливу на людей, їх психіку і поведінку, на інформаційні ресурси й інформаційні системи з метою досягнення інформаційної переваги у забезпеченні національної стратегії, здатної привести до прийняття необхідних для ініціатора впливу рішень чи паралізувати інформаційну структуру противника з одночасним захистом власної інформації й інформаційних систем»². У контексті інтегрального підходу, О.П.Марунченко доходить висновку про необхідність розмежування понять «інформаційна війна» та «інформаційно-психологічна війна»: «в інформаційній війні об'єктом впливу стають комп'ютери та інформаційні системи; в інформаційно-психологічній війні до інформаційного напрямку приєднується психологічний – об'єктом впливу стає індивідуальна і масова свідомість»³. Між тим, з такою точкою зору ми можемо погодитися лише частково, адже вважаємо «інформаційні війни» – об'єднувальним поняттям, яке структурно можна поділити на два види – інформаційно-психологічну та інформаційно-технічну війну (кібервійну).

¹ Шпиго П.С., Рудник Р.М. Основні технології та закономірності інформаційної війни. *Проблеми міжнародних відносин*. 2014. Вип. 8. С. 326-339.

² Талишинский Э.Б. Сущность информационной войны в процессах глобализации. *Університетські наукові записки*. 2012. № 2(42). С. 385–389.

³ Марунченко О.П. Інформаційна війна в сучасному політичному просторі : дис. ... канд. політ. наук : 23.00.02. Одеса, 2012. С.173.

Однак, запропонований Е.Б. Талишинським комплексний підхід видається нам найбільш вдалим, оскільки відображає сутнісно-важливі для розуміння інформаційних війн аспекти поняття інформації – як 1) певних фактів або свідчень про осіб, предмети, події чи явища, що використовуються при впливі на людей, їх психічний стан і 2) як упорядковані дані, що можуть зберігатися на матеріальних носіях, бути частиною інформаційної системи, несанкціоноване втручання у яку може призвести до втрати цих даних, їх пошкодження або незаконного використання.

Окрім того, що комплексний підхід окреслює широкий об'єкт інформаційних війн, який варіюється від людської свідомості до окремих інформаційних систем, він ще й корелює із аспектами розгляду інформаційної безпеки, яка крім інформаційно-правового досліджується у «інформаційно-технічному – захист інформаційного середовища від несанкціонованих впливів за допомогою використання відповідних програмно-технічних засобів та інформаційно-психологічному аспекті – захист психіки людини у суспільстві від можливих негативних інформаційних впливів»¹. Під інформаційним середовищем можна розуміти сукупність людей, організацій і систем, які збирають, обробляють, розповсюджують інформацію. Воно містить три складові: когнітивну (люди), інформаційну і фізичну (матеріальні носії).

Теоретичний аналіз даних понять дозволяє виявити, що інформаційна війна – складний, багатофакторний об'єкт, а велика кількість аргументованих концепцій обумовлена тим, що автори належать до різних наукових шкіл та диференційовано підходять до методологічних засад визначення області дослідження. Ми не ставимо за мету розробку остаточного доктринального визначення – приглушення дисонансних голосів стосовно терміна, який повинен інтегровано описати розбіжні явища із світу технологій і політичної психології, на наш погляд, неможливе.

¹ Пілат М. Інформаційні впливи та інформаційні війни: сутність понять та їхній взаємозв'язок в інформаційну епоху. *Вісник Львівського університету. Серія «Міжнародні відносини»*. 2013. Вип. 32. С. 185-190.

Однак, застосуємо поліпарадигмальний підхід, об'єднану концепцію інформаційних війн, який є необхідним для практичного використання наукового знання і визначимо термін «інформаційна війна» як комбінацію людських або технологічних дій, призначених для присвоєння, видалення чи зміни інформації, що призводить до пошкодження або знищення критичної інфраструктури, порушення сталої роботи органів державної влади, економічних збитків у великих розмірах або порушення адекватного ментального сприйняття явищ і подій шляхом нав'язування певного бачення реальності. Попри об'єднувальне поняття, інформаційна війна має суттєву детермінацію, функціональну спрямованість на отримання різних результатів. Вона – політичний феномен, що слугує різним цілям.

Крім того, наявність різних підходів ставить ще одну дослідницьку проблему – співвідношення «інформаційних війн» та понять «інформаційна боротьба», «інформаційне протиборство».

Загальні терміни «війна», і «боротьба» у деяких джерелах мають певну різницю і етимологічно, наприклад, за філософським словником, боротьба виступає «основним видом діяльності» війни, «стан війни у суспільстві визначається наявністю організованої збройної боротьби в тій чи іншій специфічній формі»¹; у тлумачному словнику війна визначається як «організована збройна боротьба між державами, суспільними класами тощо», однак, боротьба має більш вузьке значення і означає «сутичку, бійку, в якій кожний з учасників намагається подужати іншого»².

За тривалий час існування інформаційна війна обзавелася власним збройним арсеналом, стала «збройною боротьбою», хоч і у переносному значенні цього слова, тому має повне право називатися «війною», адже, «використання «інформаційної зброї» в широкому розумінні може зазіхати на основні принципи міжнародного

¹ Філософський енциклопедичний словник / Шинкарук В.І. та ін. Київ : Абрис, 2002. С.89.

² Великий тлумачний словник сучасної української мови : 250000 / уклад. та голов. ред. В. Т. Бусел. Київ ; Ірпінь : Перун, 2005. – VIII. С.93, С.186.

права (у першу чергу, принципи невтручання у справи, що входять у внутрішню компетенцію держав, обов'язки держав співпрацювати одна з однією, сумлінного виконання зобов'язань з міжнародного права, поваги прав людини та основних свобод), може бути одним з елементів агресії»¹. До того ж саме це поняття укорінилося у суспільній свідомості і найчастіше використовується у пресі, лунає з уст політичних діячів, закріпилося у науці: дослідники відзначають, що «як і традиційна війна, інформаційна теж має свої наслідки, які можуть своїми масштабами прирівнюватися до справжніх бойових дій. Наслідками інформаційної війни можуть стати: окупація певних територій агресором внаслідок дестабілізації ситуації в державі або в окремих її областях (яскравим прикладом інформаційного протиборства стала окупація Криму та контролювання східних регіонів України проросійськими сепаратистськими угрупованнями)...»². Інформаційну зброю інколи навіть порівнюють зі зброєю масового знищення, «вона не вимагає спеціальних засобів виробництва або складної інфраструктури для використання. Засоби інформаційної війни — це програмне забезпечення, апаратні засоби комп'ютерних вірусів, логічних бомб тощо»³.

Окремі учені, розрізняючи ці дефініції вказують, що інформаційне протиборство – ширше поняття, ніж інформаційні війни, оскільки, до нього можна віднести, наприклад, вплив на радіоелектронні засоби, а інформаційна війна виступає формою інформаційного протиборства⁴. Однак, на нашу думку, радіоелектронна боротьба – різновид збройної (кінетичної) боротьби, а не інформаційної. Хоча, наприклад, зарубіжні учені вважають радіоелектронну

¹ Українська Революція гідності, агресія РФ і міжнародне право / Антонович М.М. та ін. ; упорядкув. і заг. ред. Задорожній О.В. Київ : К.І.С., 2014. С.865.

² Мудра І., Сінькова Є. Інструменти інформаційної війни проти України. *Вісник національного університету «Львівська політехніка»: журналістські науки*. 2017. Випуск 1. Номер 883. С.42-47.

³ [Валюшко І. О.](#) Еволюція інформаційних війн: історія і сучасність. [Історико-політичні студії](#). 2015. № 2. С. 127-134.

⁴ Історія інформаційно-психологічного протиборства : підруч. / Я.М.Жарков, Л.Ф.Компанцева, В.В.Остроухов В.М.Петрик, М.М.Присяжнюк, Є.Д.Скулиш; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д.Скулиша. Київ : Наук.-вид. відділ НА СБ України, 2012. С.26-27.

боротьбу складової інформаційної війни: «інформаційна війна включає у себе численні наступальні та оборонні аспекти, такі як psywar / psyops, кібервійну, обман, радіоелектронну боротьбу...»¹.

У літературі про інформаційну війну часто пишуть як про «специфічну форму сучасних воєнних конфліктів»². Разом з тим, у сенсі «збройної боротьби», «збройного протиборства», на наш погляд, «інформаційна боротьба» й «інформаційне протиборство» можуть виступати синонімами «інформаційної війни», оскільки за критеріями ідентифікації понять якими можуть виступити історія, теорія і практика стає зрозумілим, що вони не мають історичних та категоріальних відмінностей і є однаковими з точки зору розгляду їх як політичного і соціального явища.

Політика й інформаційна війна – поняття взаємообумовлені, адже, будь-які воєнні дії – завжди прояв політичної волі. Визначимо роль інформаційних війн у політичному просторі.

По-перше, інформаційна війна є складовою політичної війни – маючи універсальний характер вона може вестися у економічній, соціальній, оборонній, духовній сферах. Узагальнено, зміст політичної війни полягає у тому, що використовуються різні відкриті і приховані засоби держав (інформаційні війни, економічний тиск, входження до політичних союзів, таємна підтримка «дружніх» іноземних елементів, заохочення спротиву в підпіллі ворожих держав тощо) для досягнення своїх цілей, впливу на інші держави. У політичних війнах акцент часто робиться на примусі, прикладами якого можуть виступити активна підтримка зміни режиму, критика іншої держави та інші види політичного маневрування: 1) дипломатичні дії (демарш, публічна дипломатія); 2) використання економічних ресурсів (запровадження економічних санкцій);

¹ Ahluwalia V.K. Psychological Warfare: Call out Adversaries' Designs. *CLAWS Journal Winter*. 2020. Vol.13. No 2. URL: bit.ly/466X7D9 (дата звернення: 18.03.2021).

² Інформаційно-психологічна боротьба у воєнній сфері : монографія / Г.В. Певцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, А.О. Феклістов, К.І. Хударковський. Харків: Вид. Рожко С.Г., 2017. С.33.

3) використання інформаційних активів (кібератаки). У контексті політичної війни, інформаційну війну можна визначити як зовнішню діяльність держави, яка веде до досягнення конкретних політичних цілей, спрямованих на руйнування чи зміну ідей, поглядів, ціннісних орієнтирів та інформаційних систем противника, при цьому захищаючи свої ресурси від тотожних дій противника. Інформаційні війни, за слушним наголосом Д.В.Кіслова, це «відображення перманентного конфлікту інтересів міжнародної політичної системи та її впливових гравців»¹. Слушною виглядає і теза М.І.Сенченка про те, що «сучасна війна має три театри воєнних дій: геополітичний або фізичний; інформаційний чи психологічний; духовний або цивілізаційний»².

По-друге, політичний чинник завжди впливає на зміст інформаційної війни: «політичний чинник визначає концепцію (доктрину) інформаційного протистояння, форми і способи її організації, засоби, способи і особливості ведення; розмах і тривалість, забезпечення матеріальними і фінансовими ресурсами»³.

Б.М.Калініченко зауважує: «політологічне осмислення інформаційної війни гостро необхідне для формування цілісної політичної та воєнної стратегії держави... Інформаційне протистояння найчастіше відбувається між людськими спільнотами, що належать до різних цивілізацій або представляють різні системи цінностей, політичні режими та ідеології. Характерними ознаками інформаційних війн є їх безперервність та розгортання не лише під час збройного протистояння, а й у мирні часи»⁴.

Інформаційні війни не бувають поза межами традиційної боротьби – історія більшості конфліктів вказує на нездатність однієї лише військової міці досягнути переваги і перемоги.

¹ Кіслов Д.В. Інформаційні війни : монографія. Київ : Київ. нац. торг.-екон. ун-т, 2013. С.36.

² Сенченко М.І. Латентна світова інформаційна війна. Київ : ФОП Стебеляк, 2014. С.3.

³ Інформаційно-психологічна боротьба у воєнній сфері: монографія / Г.В. Певцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, А.О. Феклістов, К.І. Хударковський. Харків: Вид. Рожко С.Г., 2017. С.53-54.

⁴ Калініченко Б.М. Інформаційна війна: чинники ескалації і засоби протидії [Електронний ресурс] / Національний педагогічний університет імені М. П. Драгоманова. Київ, 2020. С.258.

Зазвичай вони ведуться паралельно із традиційною війною або є складовою «гібридної війни», де слугують для того щоб зламати головне – *волю* противника, нанести удар його моральному духу. Під війною, у загальному сенсі розуміється боротьба між двома чи більше сторонами із застосуванням смертельної зброї, цим вона відрізняється від окупації чи геноциду, де насильство відбувається лише з одного боку, а гібридну війну розуміють як «воєнні дії, що здійснюються шляхом поєднання мілітарних, квазімілітарних, дипломатичних, інформаційних, економічних та інших засобів з метою досягнення стратегічних політичних цілей. Специфіка такого поєднання полягає в тому, що кожний із військових і невійськових способів ведення гібридного конфлікту застосовується у воєнних цілях та використовується як зброя. Так само в прямому сенсі у ролі зброї, яка завдає ураження різного рівня системам противника, застосовуються всі інші невійськові засоби ведення гібридної війни»¹. Досліджуючи питання гібридної війни в Україні М.В.Цюрупа зазначає, що «йдеться про «зрощення» стану «озброєного миру», політики «ні війни, ні миру», використання м'яких та жорстких засобів у міжнародних справах, поєднання стратегій силового тиску та «не прямих дій», особливо через засоби «інформаційної війни», «зомбування» населення через одержавлені ЗМІ тощо»². Метою інформаційної війни із мілітарним ухилом, як складової гібридної війни, організованої у формі насильства є досягнення конкретних політичних цілей, спрямованих на знищення чи зміну поглядів, ціннісних орієнтирів і комбатантів, і ворожого населення, окремою ціллю ураження стають й інформаційні системи.

Як і війна у традиційному сенсі цього слова, інформаційна війна – це не одномоментний, а постійний акт насильства. У дослідженні Самчинської О.А., Фурашева В.М. зустрічається спеціальний термін – інформаційне насильство, під

¹ Світова гібридна війна: український фронт / за заг. ред. В. П. Горбуліна. Київ : НІСД, 2017. С.19.

² Цюрупа М. Питання визначення сутності «гібридної війни»: на прикладі збройної боротьби на Сході України (середина 2014–кінець 2015 рр.). *Наукові записки*. Вип. 5-6 (79-80). С.56-65. URL: https://ipiend.gov.ua/wp-content/uploads/2018/07/tsurupa_pytannia.pdf (дата звернення: 18.11.2021).

яким науковці розуміють «цілеспрямований вплив на свідомість людини (групи осіб) поза її волею, який здійснюється за допомогою інформаційних засобів, інформаційних технологій та психологічних прийомів в результаті якого порушується інформаційна свобода об'єкта впливу та який здатний заподіяти шкоду життю та здоров'ю людини (групи осіб) на яку впливають»¹.

1.3. Форми реалізації інформаційних війн.

Вивчення інформаційних війн неможливе без виокремлення їх форм. У словниковій літературі до них відносять інформаційний вплив, інформаційну атаку, інформаційну операцію, інформаційну битву. Спірним виглядає включення до цього списку інформаційного впливу, хоча така думка знайшла своїх пропонентів. Так, І.О. Валюшко вказує: «ще одним методом інформаційного протиборства є невидимі інформаційні впливи. Інформаційні впливи розраховані на перспективу і результати їх можна побачити не відразу»². Серед інших дефініцій інформаційний вплив визначається як елемент інформаційно-психологічної війни: «процес і результат зміни індивіда його установок і оцінок у ході взаємодії»³; «вплив словом, інформацією, психологічний вплив такого виду виокремлює основною метою пропаганду певних світоглядних ідей, поглядів, уявлень, переконань, із одночасним формуванням у людей позитивних або негативних емоцій, почуттів, масових психічних реакцій»⁴, «регульоване або нерегульоване інформаційне втручання у

¹ Самчинська О.А., Фурашев В.М. Інформаційне насильство, інформаційна маніпуляція та пропаганда: поняття, ознаки та співвідношення. *Інформація і право*. 2021. №1 (36). С.55-65.

² Валюшко І.О. Основні виклики і загрози в епоху інформаційних війн. *Науковий вісник Дипломатичної академії України*. 2016. Вип. 23(2). С. 142-147.

³ Ландэ Д.В. Моделирование репутации, информационного влияния и управления. *Деструктивна пропаганда: шляхи протидії та проблеми відповідальності* : матер. наук.-практ. конф., м. Київ, 21 травня 2015 року. Київ : ТОВ «ІВА», 2015. С. 56-62.

⁴ Чистоклетов Л.Г., Шишко В.Й. Інформаційно-психологічні впливи як невід'ємна складова парадигми інформаційної безпеки. *Науковий вісник Львівського державного університету внутрішніх справ*. 2012. № 2(1). С.183-193.

свідомість (підсвідомість) цільової аудиторії», яке може призвести до корекції її поведінки та (або світогляду), зміни морально-психологічного стану»¹. У науці цілком слушно визначають інформаційну війну як «комплексний відкритий чи прихований цілеспрямований інформаційний вплив однієї сторони на іншу, який охоплює систему методів та засобів впливу на людей, їхню психіку та поведінку, на інформаційні ресурси та інформаційні системи...»², вважаємо, що інформаційний вплив є невід'ємною складовою інформаційної війни загалом та не володіє окремими характеристиками, а сам виступає однією із них.

Відзначимо і певні проблеми, що існують із формами, методами: В.В.Антонюк зазначає, що «основними закономірностями інформаційної війни є: залежність форм і способів її ведення»³, а в окремих дослідження вказують і на «технології», так, Л.П. Макаренко вважає чутки «особливою *технологією* інформаційної війни», «провокацію – *елементом технологій і прийомом* ведення інформаційних війн у політиці», при цьому, визначає провокацію як «спеціальну інформаційну операцію, яка примушує суперника використовувати програшну для себе стратегію та лінію поведінки», а дезінформацію як «*форму* інформаційного впливу». Дослідниця вказує, що існують «різні *методи* проведення заходів із дезінформування, кожен з яких, звичайно має власні позитивні та негативні риси. Конкретний вибір того чи іншого методу безпосередньо залежить від оперативної обстановки. Найчастіше в світовій практиці застосовуються такі методи: тенденційне викладення фактів; дезінформування від «зворотного»; термінологічне

¹ Снітаренко П.М., Кацалап В.О. Методика оцінювання психологічного впливу. [Сучасні інформаційні технології у сфері безпеки та оборони](#). 2018. № 3. С.113-118.

² Фісун А.О. Теоретично-категоріальне осмислення поняття «інформаційна війна» в структурі інформаційно-політичного простору. *Інформаційне суспільство: науковий журнал*. 2011. Вип.13. С.43-48.

³ Антонюк В.В. Інформаційна війна в структурі сучасного геополітичного протистояння: нові контексти та інтерпретації. *Державне управління: удосконалення та розвиток* : електронний журнал. URL: http://www.dy.nayka.com.ua/pdf/7_2021/35.pdf (дата звернення: 04.03.2023).

«мінування»¹; зустрічається формулювання «*варіант*»: «першим варіантом інформаційної війни можна визнати пропаганду»².

Окремі дослідники пропонують свій перелік форм інформаційних війн, так, О.В.Курбан, досліджуючи інформаційні кампанії у соціальних онлайн-мережах, вказує: «за змістом, завданнями та термінами реалізації такі операції (*інформаційно-психологічні, курсив – наш*) можна поділити на два види: інформаційні акції та інформаційні кампанії»³. Однак, навіть етимологічно одним із визначень терміна «кампанія» є «сукупність воєнних операцій у визначений період часу, що мають певну стратегічну мету»⁴. Спірним також видається і звуження інформаційних війн лише до інформаційних атак: «інформаційна війна – це атака інформаційної функції незалежно від засобів, які застосовуються»⁵, оскільки, по-перше, окрема атака може і не призвести до повноцінної інформаційної війни, по-друге, досліджуючи феномен інформаційних війн потрібно говорити про співвідношення усіх її форм. У літературі існують інші точки зору на ієрархію форм інформаційних війн: О.Левченко формами інформаційної війни вважає «інформаційні кампанії, операції, удари, акції, атаки...Звичайно, ці форми мають тісний взаємозв'язок і певну ієрархію. Найнижчою формою інформаційної боротьби в такій системі є інформаційна атака, найвищою – інформаційна кампанія. Основу кожної з наведених форм інформаційної боротьби становлять інформаційні заходи, які плануються і проводяться системно й у визначеній сукупності утворюють інформаційну атаку,

¹ Макаренко Л.П. Еволюція форм та методів ведення інформаційної війни. *ResearchGate* : веб-сайт. URL: bit.ly/3PaKa9g (дата звернення: 23.04.2022).

² Яковчук В.С., Малець Б.І., Борзов Ю.О. Інформаційні війни в сучасному світі. *Електронний репозитарій Львівського державного університету безпеки життєдіяльності* : веб-сайт. URL : bit.ly/3Z7i2nj (дата звернення: 20.04.2022).

³ Курбан О.В. Інформаційні кампанії у соціальних онлайн-мережах: типологія та класифікація. *Поліграфія і видавнича справа*. 2017. № 1. С.172–182.

⁴ Словник української мови : в 11 т. / ред. тому: А. А. Бурячок, П. П. Доценко ; АН Української РСР, Ін-т мовознав. ім. О. О. Потебні. Київ : Наукова думка, 1973. Т. 4 : І-М. С.85.

⁵ Шпилик С. Інформаційна війна, пропаганда та PR: такі схожі й такі різні. *Галицький економічний вісник*. 2014. Том 47. № 4. С. 178-188.

акцію чи удар»¹. Такий підхід відображено і у Військовому стандарті Міністерства оборони України 01.004.007 (видання 1): «формами ведення інформаційної боротьби є інформаційна кампанія, інформаційна операція, інформаційний удар, інформаційна акція, інформаційна атака, інформаційний захід». У документі під інформаційною акцією розуміється «сукупність взаємопов'язаних заходів, які спрямовані на здійснення впливу на свідомість людей та/або втручання в об'єкти певної інформаційної інфраструктури», а під інформаційним заходом «спланована елементарна (поодинокі) цілеспрямована дія інформаційно-психологічного або інформаційно-технічного характеру на окремий об'єкт або суб'єкт інформаційної діяльності» інформаційну атаку визначають як «сукупність декількох короткочасних узгоджених за метою і часом інформаційних заходів, спрямованих на втручання в процес функціонування визначених об'єктів інформаційної інфраструктури».

Надмірна кількість форм, на наш погляд, ускладнює і без того кризовий з точки зору наукового світогляду категоріальний апарат інформаційних війн, у цьому контексті доречніше говорити про три найчастіше вживані.

1. Інформаційна атака в інформаційно-психологічній війні науковцями визначається як «спланований, цілеспрямований, масований (*зосереджений в одному місці – курсив наш*) вплив на адресата, результатом якого буде формування запрограмованої суспільної думки, а відповідно і поведінки; має чітко виражені часові межі». Інформаційна атака в інформаційно-технічній війні має синонім «кібератака» і визначається як «порушення прав і законних інтересів учасників кіберпростору за допомогою ІКТ, що здійснюються фізичними та юридичними особами за участі (сприяння, фінансування тощо) держав з політичних мотивів. Кібератаки ... за своїм характером не є значними, масштабними та систематичними,

¹ [Левченко О.](#) Форми ведення інформаційної боротьби: практичний підхід до понятійного апарату. [Наука і оборона](#). 2013. № 3. С. 21-26.

не можуть визнаватись кібервійною»¹. Відзначимо, що вітчизняне законодавство містить і легальне визначення терміна у п.4 ст.1 ЗУ «Про основні засади забезпечення кібербезпеки України» кібератака розуміється як: «спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту». Узагальнено визначимо інформаційну атаку як сукупність цілеспрямованих, локальних, обмежених у часі, одноразових інформаційних впливів на окремих/конкретних осіб (груп осіб), елементи інформаційних систем чи окремі/конкретні інформаційні системи; у Таллінському мануалі, термін «кібератака» пояснюється через «кібероперацію»: «кібератака – це наступальна чи оборонна кібероперація, яка може призвести до травмування чи смертей людей, знищенню чи пошкодженню об'єктів»².

Інформаційно-технічна атака як форма інформаційної війни проходить певні стадії:

1. Розвідка об'єкта – розпізнавання і пошук даних про об'єкт атаки і про ресурси (інформаційну зброю), яка дозволяє її вчинити.

¹ [Яцишин М.Ю.](#) Використання сили у кіберпросторі в рамках міжнародного права. [Інформація і право](#). 2018. № 4. С. 22-32.

² Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge : Cambridge University Press, 2017. P.93.

2. Сканування об'єкта – перевірка правильності отриманої у результаті розвідки інформації, спостереження за об'єктом атаки, створення інструментів для проведення атаки. Важливим на цих етапах є аналіз трафіку, який відбувається за допомогою сніфферів.

3. Отримання доступу – контроль над атакованим об'єктом, втрата такою системою цілісності, конфіденційності наприклад, шляхом отримання повноважень системного адміністратора.

4. Знищення слідів незаконного втручання (додаткова стадія).

Кібератака – скоординований набір шкідливих дій, які проводяться у кіберпросторі, що прагнуть ушкодити, захопити мережу чи комп'ютерну систему із метою вчинення дій, на які законний користувач не давав згоди. У свою чергу, кіберпростір можна визначити як віртуальний простір, що складається із глобального взаємозв'язку комп'ютерних систем, телекомунікаційних мереж, інфраструктури інформаційних технологій, що дозволяє обмінюватися інформацією між індивідуальними і колективними користувачами.

Проблемним є те, що термін «кібератака» може відноситися до великого кола відносин у віртуальному просторі від шахрайства до масштабних нападів з різними політичними і економічними мотивами. При цьому, масштабних атак може бути декілька, однак вони усі можуть бути пов'язані однією метою. Труднощі викликає питання, на якому з етапів дії можна визначати як інформаційно-технічну війну? Нечітке розмежування взагалі може наштовхнути на думку перманентної інформаційної війни. На перший погляд, відповідь проста: наявність серйозної і неминучої небезпеки, яка повинна загрожувати інтересам держави, наприклад, захист критичної інфраструктури.

Дещо штучним видається виділення «інформаційного удару» як окремої форми інформаційної війни, оскільки, «удар» і «атака» близькі за значенням слова – атаку можна визначити як «наступ, що має за мету нанести удар», натомість противник може отримати «атаку у відповідь». Не кожен кібератаку варто вважати

актом кібервійни, такими, на наш погляд, можуть бути кібератаки на критично важливу інфраструктуру, таку як енергетичний комплекс, системи зв'язку, фінансові ринки чи воєнну інфраструктуру, що має високий руйнівний потенціал. Кібератаку, що спонсорується державними органами, зацікавлених у нанесенні збитків інтересам іноземної держави можна вважати актом «кібервійни».

2. Другою формою інформаційної війни є інформаційна операція. О.В. Литвиненко надає більш вузьке визначення: «операції, які через управління інформаційним процесами реалізують вплив на суспільно-політичне життя. Під операціями тут розуміють сукупність заходів відповідних служб та інших державних і недержавних установ гласного і негласного характеру, пов'язаного за метою, об'єктом та часом здійснення»¹. На противагу, інформаційним атакам, інформаційні операції володіють ознаками сукупності; узгодженості завдань, цілей, об'єктам ураження; єдності плану реалізації. За переконанням Г.Г. Почепцова, термін «інформаційні війни» – суто публіцистичний чи політичний, навіть військові його не використовують. Їхній термін «військові операції», є ще «психологічні операції». Словосполучення «інформаційні війни» не використовують тому, що війни можна вести тоді, коли точиться війна, а операціями можна займатися завжди»². За переконанням М.П.Сніцаренка: «у теорії та практиці діяльності ЗС України доцільно застосовувати термін «інформаційна операція Збройних Сил України» як базовий...Ця операція є масштабною формою воєнних дій і має інтегрувати в собі дії сил оборони держави та інформаційної спільноти України як у кіберпросторі, так і поза його межами, охоплювати широкий спектр інформаційно-технічних та інформаційно-психологічних заходів з метою створення сприятливих умов застосування власних військ (сил)...»³.

3. Третьою формою інформаційної війни є інформаційна кампанія. У рамках психологічного підходу інформаційну кампанію визначають як «комплексну систему засобів впливу на певні групи населення (так звані цільові групи) за

¹ Литвиненко О.В. Інформаційні впливи та операції: теоретико-аналітичні нариси : монографія. Київ: НІСД, 2003. С.76

² Почепцов Г.Г. Сучасні інформаційні війни. Київ : Вид.дім «Києво-Могилянська академія», 2016. С.247.

³ Сніцаренко П.М. Інформаційна операція Збройних Сил України як інтегруюча форма воєнних дій в інформаційному просторі. *Наука і оборона*. 2020. №1. С.37-42.

допомогою різних способів та каналів масового й індивідуального інформування та навчання з метою спонукання до прийняття нових, корисних для них самих і для суспільства моделей поведінки у визначеній сфері життя»¹.

Невід’ємним атрибутом інформаційних війн є *інформаційна зброя*. Вона, на відміну від традиційного озброєння, не передбачає особливих умов зберігання і не виходить із ладу. Інформаційну зброю як і більшість категорій інформаційних війн не оминули доктринальні дискусії, її визнають способом чи засобом: «такі технічні, організаційні, політичні тощо засоби, що реалізують інформаційні загрози»²; «засіб здійснення запланованих дій з інформацією або ж алгоритм цілеспрямованого впливу на інформаційну систему шляхом передачі такій системі інформації»³; нею вважають саму інформацію: «інформація та інформаційні технології, включені до цілеспрямованої програми впливу на інформаційну систему, здатної призвести до досягнення запланованих суб’єктом впливу результатів»⁴ інформаційних війн, між тим, визначення не виглядають суперечливими: усі ці точки зору виглядають обґрунтованими.

1.4. Генеза та розвиток інформаційних війн як політичного інструменту.

Історичний аспект вивчення інформаційних війн передбачає періодизацію їхнього розвитку. Перш за все, слід сказати, що у цьому контексті важливе значення має історіософський підхід до наукового аналізу історичного досвіду функціонування інформації, інформаційних революцій. У роботі О.П. Дзьобаня

¹ Публічна комунікація та ділова мова в публічному управлінні: конспект лекцій / укл. Шмагун А.В. *Таврійський Національний університет імені В.І.Вернадського* : веб-сайт. URL: bit.ly/3sHDfI5 (дата звернення: 02.02.2022).

² Литвиненко О.В. Інформаційні впливи та операції: теоретико-аналітичні нариси : монографія. Київ: НІСД, 2003. С.30.

³ Кіслов Д.В. Інформаційні війни : монографія. Київ : Київ. нац. торг.-екон. ун-т, 2013. С.43.

⁴ Верголяс О.О. Правове забезпечення спеціальних інформаційних операцій: дис. ... канд.юрид.наук : 12.00.07. Київ, 2020. С.205.

«Філософія інформаційних комунікацій» простежується шлях інформаційних революцій: «Перша інформаційна революція пов'язана з винаходом писемності...З'явилася можливість фіксувати знання на матеріальному носії...Друга інформаційна революція (середина XVI ст.) викликана винаходом книгодрукування (першодрукарі Гуттенберг та Іван Федоров). З'явилася можливість тиражування й активного розповсюдження інформації, зросла доступність людей до джерел знань...Третя інформаційна революція (кінець XIX ст.) обумовлена винаходом електрики, завдяки якій з'явилися телеграф, телефон, радіо, що дозволило оперативно передавати й накопичувати інформацію в значних обсягах.... Підвищилася роль засобів масової інформації як механізмів розповсюдження повідомлень і знань на великих територіях... Четверта інформаційна революція (середина XX ст.) пов'язана з винаходом обчислювальної техніки й появою персонального комп'ютера, створенням мереж зв'язку й телекомунікацій. Стало можливим накопичувати, зберігати, обробляти і передавати інформацію в електронній формі...Сьогодні ми переживаємо п'яту інформаційну революцію, пов'язану з формуванням і розвитком трансграничних глобальних інформаційно-телекомунікаційних мереж, що охоплюють всі країни і континенти, проникають в кожен будинок і впливають одночасно і на кожну людину окремо, і на величезні маси людей. Найбільш яскравий приклад такого явища і результат п'ятої революції — Інтернет...»¹.

Стадійний історичний вимір інформаційних війн стає предметом вітчизняних досліджень, зокрема, Л.П.Макаренко пропонує виділяти три основні періоди: «Перший період охоплює Античність, Середньовіччя та частково Новий час. Упродовж даного періоду форми й методи інформаційно-пропагандистської діяльності залишалися здебільшого незмінними, зазнаючи лише незначних модифікацій. Якісні перетворення припадають на другий період історії

¹ Дзьобань О.П. Філософія інформаційних комунікацій: монографія. Харків: Майдан, 2012. С.3-4.

інформаційного протиборства і пов'язані вони зі зростанням ролі інформації в життєдіяльності суспільства... Часові межі зазначеного періоду – від середини XVIII ст., закінчуючи роками Другої світової війни. Якщо вказаний період розвитку форм і методів інформаційного протиборства відзначається зростанням ролі цієї боротьби як ефективного допоміжного засобу у вирішенні питань військового, політичного чи економічного характеру, то третій період ще більше підносить значення інформаційного впливу на суспільство в цілому. З допоміжного інструменту управління суспільством, інформаційне протиборство перетворюється на один з основних засобів досягнення успіху»¹.

Дослідження історичної традиції необхідне, аби зрозуміти сучасний характер явища. Додамо до мапи історико-політичних досліджень своє бачення і виокремимо наступні періоди розвитку інформаційних війн.

Перший етап розпочинається ще у архаїчні (стародавні часи). Важливе значення у можливості ведення перших форм інформаційно-психологічної війни мало створення писемності (пропагандистські написи на каменях, деревах, будівлях), хоча, переважними були вербальні технології впливу (виступи ораторів, дезінформація). Інформаційно-психологічна війна у давні часи була невід'ємною складовою військового конфлікту – її дію було спрямовано на підняття бойового духу нападника, здатності активно чинити опір, зменшення власних матеріальних та фізичних втрат чи послаблення волі ворога. Приклади такого впливу можна знайти у збройних сутичках епохи розпаду первіснообщинного ладу, війн рабовласницьких держав. Це найбільш тривалий етап, який охоплює і часи Середньовіччя, коли поява друку дозволила розповсюджувати газети, листівки і Добу Просвітництва.

¹ Макаренко Л.П. Еволюція форм та методів ведення інформаційної війни. *ResearchGate* : веб-сайт. URL: bit.ly/3PaKa9g (дата звернення: 23.04.2022).

Другий етап простягається із сер. XIX ст., яке охарактеризувалося появою нових способів доставки інформації, що пов'язано із винайденням електрики (фотографії, телеграфу, радіо тощо).

Третій етап розпочинається із поч. XX ст., яке охарактеризувалося войовничістю й існуванням біполярного світу холодної війни. Спочатку територію сучасної України охопила революція, яка розгорнулася масштабними пропагандистськими гаслами. Кожна з воєн XX століття мала своє ідеологічне оформлення, ідеологічну мотивацію, яка могла виражатися як в офіційному визначенні війни вищими політичними та ідеологічними інститутами, так і в безпосередніх гаслах, які використовувалися в пропагандистській роботі, особливо, під час Другої Світової війни. Протягом XX століття з'являються персональні комп'ютери і перші випадки кібератак. На цьому етапі можна говорити про появу перших форм інформаційно-технічної війни. Активно застосовувалися і теоретично досліджувалися засоби інформаційно-психологічної війни, найчастіше – один з найпоширеніших її методів – пропаганда. Цей етап простягнувся на століття.

Четвертий етап розпочався з поч. XXI ст. і триває до теперішнього часу: кібервійна утвердилася як нове деструктивне явище, а методи інформаційно-психологічної війни з огляду на масштабну цифровізацію стали справжньою політичною інфекцією.

Обман, інсинуація і дезінформація своїм корінням сягає ще греко-латинської міфології. Так, у Греції була богиня брехні і обману Апата, яка прибула на Землю через ящик Пандори, одним із злом якого вона була. А в «Іліаді» й «Одісеї» із житла греко-римської богині Фами доносилися тисячі чуток «наполовину правдивих, наполовину вигаданих». Легенда про «Троянського коня» розповідає про те, як греки обманули свого ворога. Троя довгий час знаходилася в оточенні і греки не могли увійти в місто. Використовуючи відволікаючий маневр, греки обманом змусили противників повірити у те, що вони відступили, залишивши лише великого дерев'яного коня, якого троянці сприйняли як воєнний трофей, однак, усередині

коня ховалися грецькі воїни, які відчинили ворота цілому війську. Сьогодні троянський кінь – не лише приклад класичної воєнної дезінформації, але й назва для шкідливого програмного забезпечення.

Інформаційно-психологічна війна виникла як один із соціально-небезпечних засобів впливу і на ворога, і на власне населення. Вона здавна використовувалася у політиці і щодо ворогів, із метою досягнення воєнних стратегічних цілей у боротьбі, і щодо власного населення, наприклад, щоб довести своє імператорське коріння, як це було при сходженні Дарія I на перський престол бл.515 р. до н.е.: «Бегістунський напис» є не лише різьбою Перської імперії VI ст. до н.е., але й рекламним щитом царя Ахеменидів Дарія I, який надає автобіографічну, історичну, королівську й релігійну інформацію про Дарія I. Текст Бегістуна був одним із декількох пропагандистських елементів, своєрідним політичним вихвалянням, яке підтверджувало право Дарія на владу. Основна ціль Дарія I була у тому, щоб встановити законність свого бажання посісти трон Кіра Великого із яким у нього не було кровної спорідненості»¹.

У битві при Фермопілах у 480 р. до н.е. перський правитель Ксеркс використовував тактику залякування, щоб зламати волю грецьких міст-держав, однак, грецький полководець Фемістокл виявився хитрішим – відправивши до Ксеркса свого раба Сицинна із «секретним» лже-повідомленням про відступ греків. Перський цар повірив у це і частину війська відправив на захід, аби заблокувати можливість відступу. Сподіваючись знищити греків у вузьких мілководних водах Саламину, перси, зрештою самі опинилися в оточенні грецького війська і програли битву.

Застосовувалися методи інформаційно-психологічної війни й для перебільшення своїх особистих заслуг – ними користувався Юлій Цезар у воєнних

1

Hirst K.K. Behistun Inscription: Darius's Message to the Persian Empire. *ThoughtCo*. URL: <https://www.thoughtco.com/behistun-inscription-dariuss-message-170214>. (дата звернення: 18.09.2021).

мемуарах «Записки про Галльську війну» і «Записки про громадянську війну». Ці роботи були написані для жителів Риму і мали важливе значення у формуванні іміджу полководця. Для неграмотного населення Риму – плебеїв, підтримка яких теж була потрібна Юлію Цезарю він відправляв бігунів, які читали його «Записки» у громадських місцях. Із них Юлій Цезар звичайному громадянину здавався героєм, який заслуговує на посаду Диктатора. Саме Юлію Цезарю, можна завдячити й упровадженню концепції пропаганди у тому вигляді, у якому ми розуміємо її сьогодні – возвеличена, добре написана, з елементами театральності. Крім того, В.Жадько відзначає, що «саме в Стародавньому Римі з'явилися перші газети – «Actasenatus» і «Acta diurna populi romani». І якщо основою контенту першої з них були переважно звіти засідань сенату, то друга наповнювалася серед іншого обговорюваними в місті та за його межами чутками й плітками. Популярним став факс «збирачів інформації», а разом із ним і уявлення про те, що за допомогою певних відомостей можна як прислужитися людям, так і завдати їм відчутної шкоди»¹.

Під час воєнних конфліктів у давнину, кожна із сторін протиборства намагалася внести плутанину у ворожі ряди, часто поширювалися чутки про більшу кількість бійців і вправність ворога (цей метод використовував Олександр Македонський). Із метою забезпечення раптової атаки, ворога всіляко намагалися дезінформувати.

Пропагандисти давніх часів не мали плакатів, радіо й кіно, проте, деякі засоби, що дійшли до наших днів непоодинокі використовувалися. Найбільш корисними інструментами були імперська риторика, письмо, пам'ятники, монети, література, маніпулювання подіями – розповідь історії так, щоб це уже була не просто точка зору, а історичний факт.

¹ Гібридна війна і журналістика. Проблеми інформаційної безпеки : навчальний посібник / за заг. ред. В.О. Жадька ; ред.-упор. : О.І. Харитоненко, Ю.С. Полтавець. Київ : Вид-во НПУ імені М.П. Драгоманова, 2018. С.67.

Перші монети з'явилися в Анатолії у VII ст. до н.е., а їх комерційне використання припадає на VI-V ст. до н.е. Правителі чеканили монети із портретами і написами, які виражали послання до громадян. У римський період (I ст. – кін. IV ст. н.е.) римська валюта стала засобом розповсюдження новин про імператорські досягнення. Так, монета «Вершник, що упав», чеканка якої відбувалася між 351 і 361 р. н.е. імператорами Констанцієм II, Констанцієм Галлом і Юліаном II була випущена у знак перемоги римського імператора над персами.

З Давнього Риму до нас дійшов образ племінника Гая Юлія Цезаря – Октавіана Августа, який використовував статуї («Август – воєначальник», «Август – державний діяч», «Август – миротворець») для подальшого укріплення і розповсюдження образу всією імперією. Октавіан був відомий і проведенням дезінформаційної кампанії проти Марка Антонія, метою якої було псування його репутації. Це прийняло форму коротких, гострих гасел (свого роду архаїчний Twitter), які зображували Антонія бабієм, п'яницею і ворогом Риму.

У Київській Русі (IX-XIII ст.) мислителі відтворювали картину історії східних слов'ян у високохудожніх творах – «Повісті временних літ», «Вченні Володимира Мономаха», Галицько-Волинському та інших літописах. Психологічна сторона військової справи теж відтворена у названих джерелах. Так, у «Повісті временних літ» використовується один із сучасних методів пропаганди – вказівка на ворога, якими у той час виступали половці: «...половці держать закон предків своїх: кров проливати і вихвалитися цим. І їдять вони мертвечину і всяку нечисть, хом'яків і ховрахів. А [за себе] беруть вони мачух своїх і ятрівок, і інші [сповняють] обичаї отців своїх», мораль і релігія серед населення грали дуже велику роль, тому далі продовження: «А ми ж, християни,— скільки [єсть] земель, що вірують у святую трійцю, і в єдине хрещення, і в єдину віру,— закон маємо один, оскільки ми в Христа охрестилися і в Христа втілились»¹.

¹ Літопис Руський. *Ізборник* : веб-сайт. URL: <http://izbornyk.org.ua/litop/lit01.htm>. (дата звернення: 16.04.2020).

У Середні віки воєнний обман використовувався монголами й різноманітними арміями. Монгольські полководці – Чингісхан та Батий у цьому сенсі були передовиками інформаційно-психологічної війни. Обоє діячі були широко відомі тим, що очолювали полки вершників і проводили політику дезінформації, у першу чергу, з метою залякування. Імідж монголів про тотальне варварство і панство було посилено за рахунок обману, який забезпечували так звані «агенти впливу», що відправлялися уперед армій для проведення очної психологічної практики, розповідаючи про жорстокість і велику кількість монгольської армії для створення ілюзії непереможних чисел. У 1241 р. військо Батия вторглося в Угорщину, знищивши угорську армію на р. Шайо, монголи знайшли королівську печатку. За наказом Батия, освічені полонені від імені угорського короля Бели написали наказ про припинення супротиву, копії якого було розіслано в усі куточки країни.

Попри цілий ряд історичних фактів застосування методів інформаційно-психологічної війни, власне термін «propaganda» з'явився лише у Середні віки; він має латинське походження і дослівно означає «та, що підлягає розповсюдженню». У 1622 р. поняття використовувалося в утвердженій Григорієм XV організації *Congregatio de Propaganda Fide*. Велику роль у її створенні відіграв Фома Ісуса, автор трактатів з місіології «Спонування до місії» і «Про турботу із спасіння всіх народів».

Спочатку Конгрегація пропаганди переслідувала ціль наворотити у католицьку віру людей у західному світі, створювала місії для Англії, Нідерландів та інших країн, де католицька церква переслідувалася владою. Пропаганда охоплювала і засоби розповсюдження, і зміст послання – християнське одкровення, католицьку віру.

Перехід пропаганди у політичне русло відбувався повільно. Ще у кінці XVII ст. значення терміна переважно обмежувалося релігійним сенсом. Однак, під час Французької революції цей термін отримав і друге значення – пропаганду

доктрин і думок. А ось слово «пропагандист» не використовувалося, переважала лексика античності – «оратор», «демагог», пізніше – «ідеолог» і «доктринер».

Після промислової революції 1845 р. рівень грамотності західного населення різко виріс, свобода виразу думок активно втілювалася у друковану продукцію.

Битва за інформацію, як і у античних війнах була частиною тогочасних конфліктів. Отто фон Бісмарк зміг спровокувати французів на вкрай неприємне оголошення війни Прусії у 1870 р., всього лише змінивши текст однієї телеграми (першу у світі телеграму було надіслано 1844 р.), відомої як «Емська депеша». Зміст тексту, відредагований О. фон Бісмарком, говорив про зухвалу поведінку посла В.Бенедетті до короля Прусії. 14 липня 1870 року було опубліковано текст депеші, яка мала ефект розірваної бомби. Наполеон III прийняв на віру її сфальсифікований зміст, а 19 липня розпочалася Французько-пруська війна.

На рубежі XIX-XX ст. з'явилися засоби, які активно сприятимуть проведенню інформаційно-психологічної війни й особливо одному із її методів – пропаганді: у 1895 р. з'явилося перше радіо і пройшов перший сеанс кінопоказу.

Буремне XX ст. із його прискореним технічним прогресом стало апогеем людської войовничості й еволюції війни як суспільно-політичного явища, хоча, на початку XX ст. ідеологічні інструменти обробки масової свідомості ще не отримали широкого розповсюдження: це стало справою наступних десятиліть.

Російсько-японська війна 1904-1905 рр. стала свого роду пропагандистською репетицією з нечіткою мотивацією, на кшталт, «аграрна колонізація далекосхідних земель», а образ тодішнього японця пов'язувався серед населення царської Росії із словами «дикар», «варвар», «язичник», «жовтолиций» і навіть – «макака».

Попри те, що Російська імперія, до складу якої входила Україна пережила велику кількість воєн, дві світових війни нового часу стали найбільш жорстокими і кривавими.

Перша Світова війна стала часом жорсткої цензури у ЗМІ. Питання секретності воєнних операцій і контроль над громадською думкою стали важливим

елементом політики кожної із воюючих країн. Преса стає «служницею» пропаганди, яка підтримувала віру у перемогу пишучи про неефективність зброї і слабку боєздатність ворога.

За декілька днів до Першої світової війни царська преса писала про батьківщину: «Що зробила Росія для Німеччини і Австрії і як вони віддячили? Здавна Росія була захисником слабких і пригнічених...» і захист вітчизни: «Стрепенулася земля руська, підійнялося наше доблесне військо...йде за своїми мужніми вождями»¹.

На початку Першої світової війни широкого вжитку набула карикатура, що виступила частиною полеміки і пропаганди проти ворога. Згодом почала використовуватися і фотографія, що на ряду із листівками була основними способами донесення пропагандистської інформації.

У центрі уваги політичних газет 1917 р. залишалася воєнна тематика. Пропаганда орієнтувалася на погану боєздатність ворога, так, за підсумками 1916 р. «державами німецької коаліції не вдалося отримати жодної стратегічної перемоги», тоді як «на фронті нашого театру пам'ятна блискуча перемога наших південно-західних армій, що зламали залізну оборону противника»².

Усі країни у Першій світовій війні використовували засоби інформаційно-психологічної війни. Так, 2 квітня 1917 р. Президент Вільсон, якого обрали у тому числі за обіцянку не вступати у війну і зберегти нейтралітет просить Конгрес оголосити війну Німеччині. Оголошення війни було підписано 6 квітня усупереч волі більшості населення.

13 квітня 1917 р. президент створив Комітет суспільної інформації, відповідальний за пропаганду до кінця війни. Цю комісію очолив Джордж Крил, журналіст і політик. Його метою було переконати американську громадськість підтримати участь США у Першій світовій війні. Крил використовував усі доступні

¹ Для Русской Армии. *Киевлянин* : литературная и политическая газета Юго-Западного края. 1914. 27 июля. С.2.

² Бурский П. Итоги войны 1916 г. *Утро России: ежедневная газета*. 1917. 1 января.

тоді засоби: фотографів, журналістів, авторів п'єс, так званих «4-хвилинних чоловіків», які подорожували країною, щоб виступати перед натовпом у церквах, кінотеатрах між показами фільмів, зборами масонської ложі, залами профспілок тощо; було написано патріотичні пісні і організовано лекційні тури французьких і британських героїв війни. Операція отримала шалений успіх й за декілька місяців американське населення перейшло від байдужості до воєнної лихорадки.

А, до прикладу, тогочасна британська пропаганда була зосереджена на демонізації ворожих німців. «The Times» і «The Daily Mail» друкували відверто дезінформаційні тези, у статті під назвою «Німці і їх мерці» стверджувалося, що через брак жиру в Німеччині, внаслідок британської морської блокади, німці на «Фабриці із утилізації трупів» піддавали переробці мертвих солдат. У «North China Daily News» говорилося про те, що із трупів солдат вилучається гліцерин. Німецький уряд гучно протестував проти цих історій, однак, крик спростувань заглушив виступ китайського посла, який публічно висловився на цю тему. 14 серпня 1917 р. Китай оголосив війну Німеччині.

Під час більшовицько-української війни пропаганда використовувалася з обох сторін. Так, однією із знакових борців за незалежність України був Симон Петлюра – головний отаман армії і флоту УНР і один з найбільших ворогів більшовиків. Із завданням його морального та фізичного знищення було запущено цілий пропагандистський механізм: випускалися, рекламувалися, перевидавалися і перекладалися різними мовами книги, у якій петлюрівці виставлялися злодіями, мародерами і антисемітами. Так, у радянському романі-дебюті М.Островського «Як гартувалася сталь», описуються події громадянської війни і прекрасні якості радянської молоді, а ще погром євреїв петлюрівцями. Саме убивство С.Петлюри теж подавалося як покарання за єврейські погроми.

В умовах зростання інформованості й посилення боротьби з буржуазною й ревізіоністською ідеологією зростала необхідність у неухильному підвищенні ідейного рівня й ефективної ідеологічної роботи. Створення пропагандистської

структури розпочинається з контролю над засобами масової інформації (преса, книги), де неволі, яка панувала при імператорському урядові протиставлялася свобода: «Майорять червоні знамена, чується пісня свободи. Усе злилося в одне радісно-хвилююче море – робочі і студенти, обивателі, офіцери і солдати, солдати без кінця. На всі обличчях одна думка: «Ми знову громадяни із самовизначенням, самодержавні. Життя, що нещодавно пішло із їх рук знову стало матеріалом для творчості»¹; «Здійснилося...Стара влада впала. Рухнули основи підгнилого деспотичного трону, хвилі народного гніву змили і поглинули його. Уже близько час торжества вільної Росії, близький момент перемоги і свободи, рівності і братства»². Разом з тим, заголовками тематичних рубрик були «Робота темних сил», «Провокатори».

Вимоги до якості пропаганди марксистсько-ленінського учення зростали. Жовтнева революція проходить під гаслами: «Пролетарії усіх країн об'єднуйтеся!», «За мирний жовтень». Тема миру була однією із основних у всій радянській пропаганді, власне, можна сказати, що офіційна радянська пропаганда з цієї теми і розпочалася: 28 жовтня 1917 року було видано перший Декрет радянської влади – Декрет II Всеросійського з'їзду рад «Про мир», у якому новостворена влада пропонувала урядам усіх країн, що воюють почати переговори про справедливий, демократичний мир: «справедливим чи демократичним миром, якого прагне переважна більшість виснажених, вимучених і змучених війною робочих і робітничих класів усіх воюючих країн, миром, якого найбільш визначеним и наполегливим чином вимагали російські робітники і селяни після повалення царської монархії – таким миром уряд вважає негайний мир без анексій (тобто без захоплення чужих земель, без насильницького приєднання чужих народів) і без контрибуцій».

¹Фриче В. Раскованный Прометей. *Утро России*. 1917. 8 марта.

² Климов В. К войне! К победе. *Утро России*. 1917. 8 марта.

На рівні із миром тісно вплетеною у радянську ідеологію була пропагандистська **вказівка на ворога** – внутрішнього і зовнішнього. У «Зверненні до населення про перемогу Жовтневої революції і про завдання боротьби на місцях» Голови Ради Народних Комісарів В.І.Леніна від 5 листопада 1917 р. такими ворогами нарекли «поміщиків, капіталістів, вищих службовців і чиновників, які тісно співпрацювали з буржуазією, загалом, всі багаті... класи робітників ні на хвилинку не злякаються цього спротиву, ні краплі не затрусяться перед загрозами і страйками сторонників буржуазії». Так усередині країни утворився біполярний світ із поділом на «свій – чужий», де робітничому класові необхідно було «Згуртуватися навколо своїх Рад... встановити найсуворіший революційний порядок, нещадно придушувати спроби анархії зі сторони п'яниць, хуліганів, контрреволюційних юнкерів, корніловців і т.д.».

Далі тему «боротьби за мир» і «вказівки на ворога» було розвинуто у Зверненні РНК до всіх армійських організацій, військово-революційних комітетів, усіх солдат на фронті «Про боротьбу з буржуазією і її агентами, що протидіють справі продовольства армії і перешкоджають укладенню миру» від 11 листопада 1917 року: «боротьба за мир наптовхнулася на супротив буржуазії і контрреволюційних генералів. Солдати, робочі і селяни безумовно підтримують радянську владу і боротьбу за негайне перемир'я». Було названо прізвища агентів буржуазії, «які планували організувати нову владу проти Рад...Вся армія повинна згуртуватися навколо радянської влади для боротьби за хліб і за мир», парадоксально, але до проблем із хлібом також був причетний буржуазний ворог, так, Декретом ВЦВК «Про надання народному комісару продовольства надзвичайних повноважень по боротьбі із сільською буржуазією, яка приховувала хлібні запаси і спекулювала ними» від 9 травня 1918 року: «наполегливості жадібних сільських кулаків-багачів повинен був бути покладений кінець... на насильство власників хліба над голодною біднотою відповіддю повинно бути

наси́льство над буржуазією». Так, маніпулятивно нова влада обіцяла «мир» усім прихильним і «наси́льство» призначеному ворогові.

У Зверненні РНК до всього населення «Про боротьбу із контрреволюційним повстанням Каледіна, Корнілова, Дутова, що підтримується Центральною Радою», пропаганда звернулася до небезпеки, що загрожує революції: «революція у небезпеці, потрібно народну справу довести до кінця, потрібно змести геть злочинців, ворогів народу...». У Зверненні РНК «Про придушення контрреволюційного повстання буржуазії, яке керувалося Кадетською Партією» були заклики: «Геть буржуазію! Вітаємо революцію! Вітаємо Ради! Вітаємо мир». Із цих звернень видно, як із документа у документ під різними назвами і різними приводами повторювалися одні і ті ж тези про ворогів, мир, необхідність гуртування навколо рад і розрахунок на «підтримку і незламну вірність революції зі сторони усіх революційних робітників, селян, солдат, матросів, зі сторони усіх чесних громадян». Усе це призвело до того, що Постановою РНК «Про Червоний терор» від 5 вересня 1918 року: «забезпечення тилу шляхом терору є прямою необхідністю... необхідно убезпечити Радянську Республіку від класових ворогів шляхом ізоляції їх у концентраційних таборах; що підлягають розстрілу усіх особи, причетні до білогвардійських організацій, змов і бунтів; що необхідно опублікувати імена усіх розстріляних, а також підстави застосування до них цього заходу». Г.Г. Почепцов слушно підкреслює: «Пропаганда характерна тим, що звинувачує у всіх бідах ворогів, відводячи критику від влади»¹.

Крім того, у перші роки радянської влади було проголошену агітаційну програму комуністичної ідеології, що увійшла до історії як «Ленінський план монументальної пропаганди». Пам'ятники імперської епохи почали знищуватися уже після Жовтневої революції.

¹ Почепцов Г.Г. Пропаганда: основные характеристики. *ДМ media sapiens* : веб-сайт. URL: <https://ms.detector.media/mediaanalitika/post/20334/2018-01-07-propaganda-osnovnye-kharakterystiky/> (дата звернення: 04.03.2023).

У Декреті РНК «Про пам'ятники Республіки» від 12 квітня 1918 р. був опублікований детальний список осіб, яким планувалося поставити монументи (пам'ятники, бюсти, меморіальні дошки і комплекси) у найбільших містах – Києві, Москві, Петрограді та ін. Список містив 66 прізвищ, серед яких революціонери і громадські діячі (Маркс Енгельс, С.Разін, Бебель, Лассаль тощо), письменники і поети (М.Є.Салтиков-Шчєдрін, Ф.І.Тютчев, О.С.Пушкін, Н.В.Гоголь тощо), філософи і учені (Г.С.Сковорода, М.В.Ломоносов, Д.І.Менделєєв), художники (А.Рубльов, М.О. Врубель та ін.), композитори (Ф.Шопен, М.П. Мусоргський, О.М.Скрябін), акторам (В.Ф.Комісаржевська, М.Г.Мочалін). У Києві на Радянській площі (Майдан Незалежності) було встановлено пам'ятник К.Марксу, на Червоноармійській (площа Л.Толстого) – Ф.Енгельсу і т.д. Більшість з цих пам'ятників було зруйновано у роки громадянської війни. Попри те, що В.І.Леніна у списку не було, його пам'ятники теж почали височіти повсюди у Радянському союзі. Так, П.Ю. Леньо відзначає, що на кінець 1980-х рр. лише в Закарпатті було «48 монументів Леніну, які відносилися до категорії пам'ятників історії та культури. Ці кілька десятків бетонних та бронзових «кафедральних» Леніних доповнювалися великою кількістю типових бюстів, розкиданих серед населених пунктів, заводів, шкіл і т.д.»¹.

«Сила нашого ладу у свідомості мас» – говорилося у Звіті ЦК КПСС XXV з'їзду партії – і партія вважає своїм обов'язком виховання комуністичної свідомості, готовності, волі і уміння будувати комунізм». Широко розвинена партійна пропаганда була покликана нести у маси наукові знання про об'єктивні закони розвитку природи і суспільства, допомагати виробляти ясні класові переконання, спрямовувати вирішення практичних завдань у відповідності з ідеалами комунізму.

¹ Леньо П.Ю. «Ленініана» на Закарпатті: дослідження радянської монументальної пропаганди (1944-1991). *Науковий вісник Ужгородського університету*. 2020. Вип 1 (42). С.397-412.

Крім того, набувала свого поширення ще одна пропагандистська форма інформаційно-психологічної війни – «м'яка сила». Загалом, дипломатія вважалася переважно формальним спілкуванням між урядами: не було необхідності встановлювати контакт із населенням іншої країни, оминаючи офіційні канали. Однак, наприкінці 1920-х стало очевидним, що культура переплітається із зовнішньою політикою і бере участь у формуванні національного іміджу. Так, у США набули свого поширення перші європейські ініціативи в плані культурної дипломатії – складової «м'якої сили». Спочатку німецькі, італійські, французькі культурні інститути орієнтувалися на еліту, їх завдання полягало у тому, щоб просувати інтереси нації серед людей, які часто відвідували МЗС, університети чи торгові палати. Однак, розвиток масових ідеологій у 1920-ті роки і використання все більш ефективних засобів масової комунікації привели до розширення аудиторії, на яку було націлено розповсюдження європейської культури. З того часу, реклама, автомобільні перегони, наукові і спортивні зустрічі, радіопрограми, фільми стали засобами укріплення репутації нації, а радіо було переважним ЗМІ. Усвідомлюючи силу впливу, європейські урядовці організували служби радіомовлення за кордоном: 1926 р. – СРСР, 1927 р. – Нідерланди, 1931 р. – Франція і 1932 р. – Велика Британія створили систему мовлення за кордоном.

У 1933 р. у Німеччині створено Імперське міністерство народного просвітництва та пропаганди Третього Рейху, яке очолив гауляйтер Берліну Й.Геббельс, чиє ім'я й досі не роздільне із концепцією основного методу інформаційно-психологічної війни – пропагандою, а у СРСР досягав свого піку Голодомор, між тим, пропагандистська преса писала про «завдання колгоспної торгівлі»: «Через вільний продаж хліба кооперації укріплюй колгоспи!»¹ і про події у фашистській Німеччині – радянська пропаганда точно не відображала реальних подій у суспільстві, а слугувала формуванню стереотипів, які були потрібні владі.

¹ Семенов Г. Бойцы рассказывают о задачах колхозной торговли. Через свободную продажу хлеба кооперации укрепляй колхозы. *Красная звезда*. 1933. 22 декабря. С.1.

Фашистська пропаганда під керівництвом Й. Геббельса включала політичні мітинги, зібрання, які повинні були переконати німецьке населення у тому, що Гітлер – надлюдина, яка готова рятувати Німеччину. Підкріплювалися ці переконання прямими патріотичними текстами, на кшталт: «Ми – свідки найбільшого чуда в історії! Геній створить світ!». Нацистські заклики переконували німецький народ, що фюрер – людина без людських слабостей і на нього треба рівнятися. Крім того, за вказівкою А.Жадька, у гітлерівській Німеччині «величезна увага приділялася ритуалам і символіці, які можна розцінювати як засоби психологічного тиску, навіювання, маніпулювання»¹. Символів у нацистській Німеччині була велика кількість, деякі із них окремі угруповання використовують досі²: «Вольфсангель», емблема «СС», «Свастика», «Мертва голова», «Чорне сонце» etc.

Й.Геббельс не оминув увагою і потенціал кінематографу. Через вплив на емоції нацистська пропаганда хвалила німецький характер, мистецтво і досягнення минулих епох, але війна вимагала радикального перегляду ідеологічного впливу і в Німеччині з'явилися відверто антисемітські фільми «Євреї Зюсс», «Ротшильди».

Преса, радіомовлення, література, музика, кінематограф, театр, образотворче мистецтво – під керівництвом Й.Геббельса працювало тисячі офіційних пропагандистів. Активно застосовувався такий вид пропагандистської роботи як *вказівка на ворога* – ним стали євреї. Нацисти розпалювали ненависть і організовували насильство проти євреїв, яких вважали такими, що паплюжать расу, нівечать мораль, псують звичаї німців і руйнують міць великої Німеччини: «Євреї – наше нещастя», «Не купуй у єврея – не продавай націю», «Обережно. Ворог підслуховує. Знай, твоїм сусідом може виявитися єврей». Як наслідок з моменту

¹ Гібридна війна і журналістика. Проблеми інформаційної безпеки : навчальний посібник / за заг. ред. В.О. Жадька ; ред.-упор. : О.І. Харитоненко, Ю.С. Полтавець. Київ : Вид-во НПУ імені М.П. Драгоманова, 2018. С.75.

² Детальніше Грінберг М. Символи ненависті: довідник / укл.М.Петров. *Українська Гельсинська спілка з прав людини* : веб-сайт. URL: https://helsinki.org.ua/wp-content/uploads/2021/02/Prev-Hate_Symbols_A4.pdf (дата звернення: 18.03.2022).

приходу Гітлера до влади розпочався Холокост (іврит – Шоа, ідіш – Хурбн) – масове знищення євреїв. Цікаво, що більшість німців були впевнені у тому, що євреїв просто депортують за межі Німеччини. Насправді ж, їх очікувало гетто, рови для розстрілів і табори. Треба наголосити й на тому, що це не був чітко вибудований мученицький механізм, а хаотична діяльність, яка не піддається осмисленню. Ось як писав Чарльз Резнікофф у поемі «Голокост»: «...У будь-якого єврея, що не зняв капелюха на знак поваги при перетині мосту, німці стріляли, і таких було багато. А когось застрелили просто так».

У 1935 р. Дж. Геллапом було створено інститут суспільної думки Пристонського університету, що у тому числі займався вивченням і вимірюванням настроїв населення. Поява цього інституту сприяла корегуванню політичного дискурсу, у тому числі з метою успішного ведення інформаційно-психологічної війни чи «управління» свободою слова. Крім того, США починає експериментувати із явищем, яке через декілька десятиліть утвердиться у політичній площині як «публічна дипломатія», запустивши серію культурних і освітніх програм для забезпечення лояльності південноамериканських народів.

Тим часом у Радянському Союзі досягав свого піку сталінський терор (1937-1938 рр). Жертвами Великої чистки ставали академіки, інженери, письменники – «вороги народу» у розумінні радянської влади розстрілювалися або відправлялися у ГУТАБ (ГУЛАГ). Пропаганда, яка лежала в основі сталінської системи не залишала шансу ні альтернативним поглядам (якщо не вважати такими чутки, які ширилися у чергах за дефіцитними товарами, особистих листів і листівок із закликами народу підійматися), ні можливості супротиву, адже, щодня люди отримували інформацію про радощі радянського життя (популярним було гасло «жити стало краще, жити стало веселіше») і жахи капіталізму (зокрема через радіомовлення і телебачення; відмітимо, що 1 жовтня 1931 року в СРСР почалося регулярне телемовлення), геніальності Й. Сталіна і очевидної вини «ворогів народу» і усе це під цензурою «заборонених тем» (наприклад, про нестачу хліба).

Паралельно велася підготовка населення до можливої війни – 1930-ті певно єдиний майже 20-ти літній період у радянській історії, коли тема «миру», який був фундаментом радянської пропаганди поступилася місцем потенційній воєнній небезпеці: мир більш не може бути досягнутий просто так, його треба завоювати, а пропагандистський дискурс розвернувся у сторону озброєння і підготовки до війни, звісно з нахилом на антифашистський фронт і «братство народів». Із цього періоду починають з'являтися портрети «батька народів» Й. Сталіна у військовій формі, які разом із статуями заповнюють СРСР – ще одна пропагандистська ілюзія про те, що «один великий вождь» може врятувати і захистити.

Крім того, у 1938 р. було знято ряд воєнних та історичних фільмів, зокрема, «Болотні солдати», «Виборгська сторона», «Якщо завтра війна...», «Перемога», «Людина з рушницею» тощо і уже у листопаді 1939 р. СРСР зробив спробу захопити Фінляндію. Розв'язання цієї війни було складовою частиною загарбницької зовнішньої політики Й.Сталіна, адже у п.1 «Секретного додаткового протоколу» Молотова-Ріббентропа вказувалося, що «у випадку територіально-політичного перерозподілу областей, які входять до складу Прибалтійських держав (Фінляндія, Естонія, Латвія, Литва), північний кордон Литви одночасно є межею сфер інтересів Німеччини і СРСР». Іншими словами, Фінляндію очікувала насильницька анексія і включення до складу СРСР у якості «радянської республіки». У кінці жовтня 1939 р. у періодиці з'являється серія публікацій про погіршення становища фінських робітників, збільшення їх робочого дня і зростання безробіття, а в листопаді розгорнулася повномасштабна антифінська кампанія. Здаватися без бою Фінляндія не планувала і було прийнято рішення розпочати війну. Найбільш передові засоби доставки пропаганди – газети «Правда», «Червона зірка», «Більшовик» писали про «визволення фінського народу». Постійно підкреслювалася класова приналежність «ворога» – розповідалося про звірства фінських офіцерів, фашистів-шюцкоровців (добровільна військова організація).

Оскільки війна розцінювалася як визвольна, пропаганда велася й через мистецтво. Так, було знято фільм «Лінія Маннергейма» – радянську пропагандистську кінострічку, яка однобічно пояснювала причини війни, звітувала про тривалі бойові дії і високу ефективність стратегічних і тактичних рішень командування.

Із вересня 1939 до червня 1940 рр. у Нью-Йорці було організовано семінар Фонда Рокфеллера із масових комунікацій. Особливо важлива роль на цьому семінарі Гарольда Д.Лассвела, адже він на ньому сформулював знамениту модель: хто що кому говорить? через який канал? і з яким ефектом? Ця модель орієнтується на проблематику ефектів масової комунікації. Формула Лассвела із часом стане домінуючою основою для визначення всіх проблем, якими будуть займатися спеціалісти із досліджень масових комунікації.

Перед Другою світовою війною, радянський патріотизм опирався на штучні, виховані пропагандою гасла. Бравурні пісні і бадьорі кінострічки про непереможність Червоної Армії, заголовки газет, січневі номери яких починалися заголовками «Рік великих перемог» (під час війни вони змінилися на заклик «До нових перемог») знижували рівень готовності до тривалої боротьби, викликали самозаспокоєння і, як наслідок, майбутня війна в уяві населення була чимось більше схожа на парад. Фільми «Місто під ударом», «Ескадрилья номер п'ять», «Голос Тараса», «Розгром Юденича» дезорієнтували потенційних воїнів в оцінці майбутньої війни. Натхненними були і кращі твори представників соціалістичного реалізму.

Класові гасла у Другій Світовій змінилися на патріотичні: «За честь жінок, за життя дітей, за щастя їх батьків, за наші пейзажі і наші луки, убий ворога-окупанта!» і гасла-символи: «За Батьківщину! За Сталіна!». Разом з тим, активно розвивалися антирадянські політичні рухи. У 1943 р. було опубліковано текст «Прокламації Смоленського комітету», який було підписано генералом А.А.Власовим. Уперше

населенню пропонувалося знищення сталінізму, укладення миру із Німеччиною і створення нової держави.

Атмосфера сталінської епохи виразилася у тенденційності ЗМІ і великій кількості фальсифікацій. Активна інформаційна війна часів Другої світової проявлялася у технічних новинках ХХ ст.: радіо, кінематограф, масовий друк. Радянський воєнний плакат був найбільш масовим видом образотворчого мистецтва. У Другій світовій відомими карикатуристами були Кукринікси – творчий колектив радянських художників-графіків. Їх військові плакати супроводжували всю війну із гаслами: «Нещадно розгромимо і знищимо ворога». Так, радянська пропаганда була зорієнтована на патріотизм, любов до своїх і ненависть до чужих.

Якщо перед війною була ідея світової революції і звільнення «пригнічених братів», то з вторгненням фашистів їх замінили національно-політичні гасла. На завершальні стадії війни з'явилися нові відтінки розуміння її цілей – не тільки перемогти і вигнати ворога з рідної землі: «Звільнені радянські люди! Ви звільнені з-під гніту фашистської неволі! Повертайтеся якнайшвидше на батьківщину» (плакат 1944 р.), але й принести визволення сусіднім народам – саме так це виглядало в офіційній пропаганді і свідомості людей. Натомість, Т.Джадт відзначає: «післявоєнні десятиліття були справді безкровними порівняно з тим, що їм передувало, але тільки завдяки непроханій присутності Червоної Армії: це був мир тюремного подвір'я під прицілом танкової гармати... Окрім Німеччини та глибинки Радянського Союзу, кожна континентальна європейська держава, втягнута в Другу світову війну, щонайменше двічі зазнавала окупації: уперше – ворогами, а потім – арміями-визволителями»¹.

В офіційній пропаганді всі перемоги і успіхи пов'язували з іменем Й. Сталіна. Перемога на війні укріпила його авторитет і усередині країни, і за

¹ Джадт Т. Після війни. Історія Європи від 1945 року / пер. з англ. К.Заремби. Київ : Наш формат, 2020. С.31, 89.

кордоном, він став героєм, завдяки якому світ зустрічає «червону весну»: «Погляди, поёт и пляшет вся Советская страна... Нет тебя светлей и краше наша красная весна» (плакат 1946 р.). Роками після перемоги у Другій світовій війні радянська газетна пропаганда прославляла Й.Сталіна: «Безпосереднім натхненником і організатором найважливіших перемог Радянської армії у роки громадянської війни та інтервенції був товариш Сталін. Молода Радянська армія відбила воєнні походи полчища 14 капіталістичних держав»¹.

Говорячи про антагоністичний світ часів Другої світової війни, варто сказати про спорідненість форм і методів інформаційно-психологічної війни СРСР і Німеччини: паради, переконливий характер, масовість, символи і гасла, порядок і регулярність. Маніпулювання натовпом за допомогою пропаганди, культ лідера, символи, заклик до дисципліни, нероздільність індивідуумів із масою, солідарність – усе це ознаки тоталітарних держав, якими були Німеччина і СРСР.

Одразу після закінчення війни пацифізм став основою радянської ідеології і це на фоні того, що уже менш ніж через два роки старі союзники стали противниками у результаті відновлення ідеологічного конфлікту: 5 березня 1946 р. В.Черчилль у Фултоні заявляє, що над Європою упала «залізна завіса». А.Жданов у своїй пропагандистській доповіді від 22 вересня 1927 р. сказав: «мріючи про підготовку нової, третьої світової війни, американські експансіоністські кола крєвно зацікавлені у тому, щоб придушити всілякий можливий спротив зовнішнім авантюрам усередині країни, щоб отруїти шовінізмом і мілітаризмом політично відсталі і малокультурні маси рядових американців, щоб «обдурити» американського мешканця за допомогою різних засобів антирадянської, антикомуністичної пропаганди через кіно, радіо, церкву й друк...Воєнщина стає активною політичною силою у США, здійснюючи у великій кількості поставки державних діячів, які проводять агресивний мілітариський курс у всій політиці

¹ Яхлаков П. Слава героической Советской Армии. Армия-освободительница. *Колхозная правда*: орган Ново-Ивановского райкома КпБУ и районного совета депутатов Измайловской области. 1949. 22 февраля. С.1.

країни». Так, войовничій Америці протиставлявся миролюбивий СРСР, який стояв на позиції «створення єдиної миролюбивої та демілітаризованої демократичної Німеччини»¹. Дійсність була інакшою – «мир і роззброєння» були лише формальними концепціями на службі в ідеології: сталінська армія окупувала частину Європи, на фоні демілітаристських гасел проходило фактичне укріплення Червоної Армії, і її невпинний рух у сторону «ядерної наддержави», крім того, радянська влада підтримувала локальні конфлікти.

У період холодної війни інформаційно-психологічна війна у СРСР координувалася новим інформаційним бюро – Інформаційним бюро комуністичних та робітничих партій (Комінформ), яке розпочало свою діяльність 27 вересня 1947 року. У цей період для впливу на іноземне населення було використано міжнародне мовлення. У СРСР працює численна кількість «агентів впливу», їх робота у ЗМІ, наукових гуртках й іноземних спецслужбах полягає у проведенні дезінформаційних кампаній і пропагандою радянських ідей та цінностей.

США повертають до життя ліквідований апарат психологічної війни. Поруч із офіційними структурами й інформаційно-психологічною війною за допомогою радіо, листівок, газет, ВВС, «Голосу Америки» країна використовує *«м'яку силу»* шляхом популяризації власної культури в іноземних державах – голлівудські фільми, «Coca-Cola» й американський ідеал життя.

У Радянському союзі пропаганда 1950-х пройшла під викриттям антирадянських і антикомуністичних дій західного табору і уже стандартних тезах про мир. 12 березня 1951 р. було прийнято Закон «Про захист миру», у якому наголошувалося на «радянській миролюбивій політиці» і небажання «миритися із безкарністю пропаганди війни, яка ведеться окремими державами», пропаганда війни за цим законом утверджувалася як тяжкий злочин проти людства.

¹ Доклад А.Жданова (22 сентября 1947 г.). *CVCE.eu* : веб-сайт. URL: https://www.cvce.eu/content/publication/1997/10/13/914edbc9-abdf-48a6-9c4a-02f3d6627a24/publishable_ru.pdf (дата звернення: 17.05.2022).

Інформаційно-психологічна війна відігравала неабияку роль у «холодній війні», адже, це була не лише гонка озброєння, але й війна ідеології, у якій, образи, символи, дезінформація і пропаганда були головним озброєнням.

Інтенсивно розвивалися ЗМІ – основні виразники радянської ідеології: «Радіо Москви», «Радіо миру і прогресу» etc. В Америці мовлення вели «Голос Америки», «Вільна Європа» etc.

У 1960-ті з'явилися перші комп'ютерні віруси. Першим шкідливим ПО вважається «Pervading Animal» – ним був заражений лише один комп'ютер, той на якому його створили. У 1961 році архітектор Кісе Курокава і антрополог Тадао Умесао першими увели термін «інформаційне суспільство». Вони передбачили, що за аграрним й індустріальним суспільством прийде час інформаційного суспільства, для якого цінність інформації буде найвищою.

Інформаційно-психологічна війна кін. 1970-х поч. 1980-х у СРСР балансувала між миром і війною, розпалюючи страх і паніку – тепер уже перед ядерним вибухом. США у цій парадигмі виступали підбурювачами війни, СРСР – миротворцями. Радянська преса майоріла заголовками: «НАТО – філія Пентагону», де НАТО описувалося як «зловіщий альянс, відмічений постійним нагнітанням міжнародної обстановки, нестримною гонкою озброєнь, безпардонним втручанням у внутрішні справи не лише країн, що входять до НАТО, але й держав, розташованих за межами європейського континенту»¹, а статті про США носили назву на кшталт «В атмосфері жорстокості і насильства»².

Дезінформація виливалася у шокуючі історії, які стосуються людських інтересів. Відомою стала операція «Інфекція» у 1980-х. КДБ СРСР звинуватило американських військових у створенні вірусу СНІДу та випусканні його як біологічної зброї. Уперше ця історія з'явилася на підконтрольних радянських точка.

¹ Павлов В. НАТО – филиал Пентагона. Международные заметки. *Советский патриот*: Орган центрального комитета ДОСААФ СССР. 1979. 4 апреля. С.4.

² Грачиков Г. Их облик, их нравы. В атмосфере жестокости и насилия. *Советский патриот*: Орган центрального комитета ДОСААФ СССР. 1979. 10 января. С.2.

У 1985 р. його підхопив радянський тижневик «Літературна газета», а потім багато інших видань. Тільки у 1987 р. це повідомлення з'явилося понад 40 разів у радянській пресі.

Висновки до I розділу

Процес створення теоретичної бази із напрацювань щодо інформаційно-психологічної війни розпочався ще у давні часи, однак, войовничість ХХ ст., яка супроводжувалася інформаційно-психологічною складовою зумовила більш активне наукове вивчення і впровадження методів інформаційно-психологічної війни, зокрема пропаганди як основного її методу. Теоретичне вивчення пропаганди відбувалося у радянській, німецькій, англійській, американській доктрині.

Після Другої світової війни велися дослідження нацистського пропагандистського апарату, вивчалася, британська і американська пропаганда окремі дослідження порівнювали роботу пропаганди під час двох світових війн.

Теоретичне осмислення інформаційно-технічної («кібервійни») розпочалося значно пізніше – ближче до кінця ХХ ст., оскільки сам термін «кібервійна» було уведено у науковий обіг лише у 1993 р.

Вітчизняна теорія інформаційних війн характеризується широтою підходів, хоча така їх кількість інколи вносить плутанину і не сприяє ясності. Разом з тим, небагато дослідників обирають комплексний підхід: робота наукового апарату зосереджується або на психологічній парадигмі розуміння, або зводить категоріальне осмислення до кібервійни.

Конструктивна дискусія продовжується і щодо форм та методів інформаційних війн, а триваюча російсько-українська війна змушує вітчизняних

науковців пропонувати способи протидії, тоді як увага зарубіжних прикута у тому числі до російських кібератак проти України.

Концептуальний простір інформаційних війн широкий: її осмислення відбувається у рамках психологічної парадигми із подальшим поділом на поведінкову війну, смислову війну та когнітивну війну. Окремі дослідники вбачають необхідність у розмежуванні «інформаційної війни» та «інформаційно-психологічної війни».

Найбільш вдалим, на наш погляд, є комплексний (інтегральний) підхід до розуміння інформаційних війн, а інформаційна боротьба та інформаційне протиборство можуть виступати синонімами інформаційної війни.

Роль інформаційної війни у політиці неможливо недооцінити, адже, окрім того, що будь-яка війна – прояв політичної волі, маючи універсальний характер інформаційна війна може вестися у економічній, соціальній, оборонній, духовній сферах, інформаційні війни не бувають поза межами традиційної боротьби – зазвичай вона ведеться паралельно із традиційною війною або є складовою «гібридної війни».

Політична наукова думка виробила перелік форм інформаційної війни, утім, на наш погляд, їх надмірна кількість додатково перевантажує категоріальний апарат. У цьому контексті найбільш доречним видається виділення трьох найчастіше вживаних: інформаційна атака (кібератака якщо мова йде про інформаційно-технічну війну), інформаційна операція, інформаційна кампанія.

За тривалий час існування інформаційна війна обзавелася власним збройним арсеналом, стала «збройною боротьбою», хоч і у переносному значенні цього слова. Збройний арсенал інформаційно-технічної війни програмно-математичний, а зброя інформаційно-психологічної війни вербальна або невербальна, у будь-якому разі – комунікативна.

Інформаційна війна часто сприймається як нова загроза, проте, розповсюджена практика XX-XXI ст.: пропаганда, дезінформаційні кампанії,

покликані заплутати, маніпулювати і налякати – не продукт нового часу, а складова безцінного історичного досвіду. Її різні, інколи дуже витончені форми, що розпочалися з пропагандистських зображень, текстів й усних розповідей знайшли своє відображення в історії.

Стадійний історичний вимір інформаційних війн з урахуванням надбань вітчизняної науки запропоновано розділити на чотири етапи. Виокремлено наступні періоди розвитку інформаційних війн.

Перший етап розпочинається ще у архаїчні (стародавні часи). Важливе значення у можливості ведення перших форм інформаційно-психологічної війни мало створення писемності. Це найбільш тривалий етап, який охоплює і часи Середньовіччя, коли поява друку дозволила розповсюджувати газети, листівки і Добу Просвітництва.

Другий етап простягається із сер. XIX ст., яке охарактеризувалося появою нових способів доставки інформації, що пов'язано із винайденням електрики (фотографії, телеграфу, радіо тощо).

Третій етап розпочинається із поч.XX ст., яке охарактеризувалося войовничістю й існуванням біполярного світу холодної війни. Кожна з воєн XX ст. мала своє ідеологічне оформлення, мотивацію, яка могла виражатися як в офіційному визначенні війни вищими політичними та ідеологічними інститутами, так і в безпосередніх гаслах, які використовувалися в пропагандистській роботі, особливо, під час Другої Світової війни. Протягом XX століття з'являються персональні комп'ютери і перші випадки кібератак. На цьому етапі можна говорити про появу перших форм інформаційно-технічної війни. Активно застосовувалися і теоретично досліджувалися засоби інформаційно-психологічної війни, найчастіше – один з найпоширеніших її методів – пропаганда. Цей етап простягнувся на століття.

Четвертий етап розпочався з поч.XXI ст. і триває до теперішнього часу: кібервійна утвердилася як нове деструктивне явище, а методи інформаційно-

психологічної війни з огляду на масштабну цифровізацію стали справжньою політичною інфекцією.

РОЗДІЛ 2. ВИДОВІ ОСОБЛИВОСТІ ІНФОРМАЦІЙНИХ ВІЙН

2.1. Комунікаційні та психологічні впливи як підґрунтя інформаційно-психологічної війни.

У рамках комплексного підходу до розуміння інформаційних війн, єдину складну структуру простіше сприймати за двома спрямуваннями, розділити на два види – інформаційно-психологічну та інформаційно-технічну: «виходячи з того, що основними об'єктами інформаційного протиборства є, з одного боку, інформаційно-технічні системи різного масштабу і призначення, а з іншого – інформаційно-психологічні об'єкти, виділяються два основні напрями інформаційного протиборства – інформаційно-технічне та інформаційно-психологічне»¹; «на нашу думку, сьогодні інформаційна війна як реальна практика проявляється у двох просторових вимірах: як війна у кіберпросторі і як війна у просторі смислів. Перша проявляється у кіберзагрозах, порушенні інформаційних комунікацій, спробах державного регулювання інтернету, утворенні цифрових монополій тощо. Друга є війною контенту та боротьбою за контроль над каналами його розповсюдження»².

На наш погляд, *інформаційно-психологічна війна* – це інструмент впливу політичної, військової, економічної, ідеологічної дії, логічне застосування якого дозволяє: 1) впливати на формування громадської думки (у т.ч. викликати інакомислення, невдоволення чи навпаки – підтримку у населення); 2) захистити національні інтереси шляхом зниження морального духу, бойової ефективності ворогів; 3) впливати на поведінку іноземних держав, неурядових організацій, окремих груп чи осіб. Сучасна інформаційно-психологічна війна має наступні ознаки:

¹ Інформаційно-психологічна боротьба у воєнній сфері : монографія / Г.В. Певцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, А.О. Феклістов, К.І. Хударковський. Харків: Вид. Рожко С.Г., 2017. С.54.

² Мамонтова Е.В. Псевдоморфоз як техніка символізації у державотворчій практиці Доби Відродження. *Актуальні проблеми політики*. 2018. Вип.61. С.34-45.

1. Основним об'єктом впливу є психічна діяльність людини чи груп людей. До інших об'єктів у літературі відносять: «ресурси, які розкривають духовні, культурні, історичні, національні цінності, традиції, надбання держави, нації в різних сферах життя суспільства; інформаційну інфраструктуру, тобто абсолютно всі проміжні ланки між інформацією та людиною; систему формування суспільної свідомості (світогляд, політичні погляди, загальноприйняті правила поведінки тощо); систему формування громадської думки; систему розроблення та прийняття політичних рішень»¹.

2. Може розширювати традиційні форми конфлікту, оскільки впливає на здатність керувати, боротися, коритися, підтримувати, або бути самостійним засобом агресії, окремим видом протиборства, у цьому аспекті, слушно наголошують Л.Г.Чистоклетов та В.Й.Шишко, що «інформаційно-психологічний вплив відіграє роль своєрідного інструментарію або так званої нелегальної зброї, за допомогою якої в мирний час, без війни, у звичайному розумінні цього явища, здійснюється агресія в соціальні, політичні, економічні, військові та інші сфери суспільного буття»².

3. Може вестися різними способами: пропагандисти і дезінформатори повинні використовувати всі наявні технічні засоби. Загалом, до каналів або засобів інформаційно-психологічної війни можна віднести: Інтернет-ресурси: сайти, блоги, соціальні мережі; візуальні і звукові носії: телебачення, радіо, кінотеатр, документальні фільми, пісні, новини, ток-шоу; промови: концерти, особисті зустрічі із великою аудиторією, політичні події; мистецтво: картини, плакати; преса і література: брошури, книги, газети, журнали.

¹ Марута Н.О., Маркова М.В. Інформаційно-психологічна війна як новий виклик сучасності: стан проблеми та напрямки її подолання. *Український вісник психоневрології*. 2015. Т. 23, Вип. 3 (84). С. 21–28.

² Чистоклетов Л.Г., Шишко В.Й. Інформаційно-психологічні впливи як невід'ємна складова парадигми інформаційної безпеки. *Науковий вісник Львівського державного університету внутрішніх справ*. 2012. № 2(1). С.183-193.

4. Інформаційно-психологічна війна завжди інтенційна (має вектор спрямування, націленість) – виклик певних емоційних реакцій для досягнення конкретних поведінкових результатів.

Рационалізація розуміння інформаційно-психологічної війни як соціально-політичної категорії неможлива без констатації її трансдисциплінарного характеру. Перехід від аналітичного дослідження до розгляду основ інформаційно-психологічної війни у подальшому дозволить впорядкувати вчення про інформаційно-психологічну війну у контексті багатоманніття її термінології, адже не можна осягнути ціле, не бачачи частин – єдину складну структуру простіше сприймати, виділивши її елементи.

Визначимо складові, «будівельні блоки» інформаційно-психологічної війни як психосоціолінгвістичної та політичної категорії.

До елементів, що формують політичну платформу інформаційно-психологічної війни, перш за все, належить теорія комунікації, однак, основою будь-якого спілкування є мова, а відтак, при дослідженні інформаційно-психологічної війни неможливо ігнорувати лінгвістичний аспект адже «мова – засіб обміну інформацією у всіх суспільно важливих сферах комунікації»¹, у тому числі і в політиці, невід’ємною складовою якої є політична лінгвістика, що «знаходиться на перетині мови і влади»².

Лінгвістичні аспекти інформаційно-психологічної війни найбільш яскраво проявляються у пропагандистських, дезінформаційних текстах. Тому, необхідним є розуміння мовленнєвих прийомів, лінгвістичних особливостей, дискурсивних стратегій. І.Є.Фролова дискурсивний контекст трактує «як сукупність загальноконтекстних чинників (знання і уявлення певної епохи, культури, соціуму, соціальної групи, особистості) та контекстно-ситуаційних чинників (частина цих

¹ Психологія спілкування : навч. посіб. / Л.Г. Кайдалова, Л.В. Пляка, Н.В. Альохіна, В.С. Шаповалова. - 2-ге вид., перероб. і допов. Харків : НФаУ, 2018. С.37.

² Нагорна Л.П. Політична мова і мовна політика: діапазон можливостей політичної лінгвістики. Київ : Світогляд. 2005. С.51.

знань і уявлень, що активується у певний конкретний момент спілкування, відповідно до осмислення індивідом усіх його параметрів)... Наголошуючи на соціальній природі як мовленнєвих, так і дискурсивних (стратегічних) смислів, зазначимо, що саме останні характеризують вербальну інтеракцію як соціальну взаємодію, бо їхнє призначення (зміна знань, уявлень, переконань, поведінки) відіграє суттєву роль не лише у процесах комунікації, а й у суспільній діяльності індивіда в цілому»¹. Зосередження уваги на дискурсивних стратегіях у контексті інформаційно-психологічної війни є необхідним з огляду на те, що дискурсивний обмін як діяльність соціуму: 1) бере участь у конструюванні соціальної реальності; 2) сприяє розповсюдженню нових знань, поглядів, інформації в цілому; 3) у публічній площині контроль дискурсу дозволяє впливати на дії аудиторії, соціальні процеси і відносини. Дискурсивні стратегії в інформаційно-психологічній війні полягають у підготовці тексту таким чином, щоб викликати зміни у поглядах шляхом використання спеціальних формул. Вони є складовою політичного дискурсу, який С.-В. О. Кривенко визначає як «політичну мережу текстів, які завдяки своїм властивостям (комунікативність і цілісність, символічність, обмежений доступ до продукування, раціональність і аргументованість, культурна детермінованість, темпоральність, просторовість, структурованість і абстрактність) здатні сконструювати символічну реальність політичної спільноти»². О.Ковальова під «політичним дискурсом» розуміє «багатоаспектне явище, основними компонентами якого є текст (в усній або письмовій формі), екстралінгвістичний контекст (мета, обставини, спосіб та час утворення), адресант і адресат... Найбільш типовими характеристиками ПД, що розкривають його природу, є риторичність, емоційність, маніпулятивність, динамічність, ритуальність»³. Р.М. Ключник

¹ Фролова І.Є. Дискурсивна стратегія як організуючий конституент вербально-соціальної інтеракції. *Лінгвістика XXI століття: нові дослідження і перспективи*. 2009. № 3. С. 242-249.

² Кривенко С.-В.О. Семантична парадоксальність політичного дискурсу (теоретико-методологічний аналіз) : дис. ...канд.політ.наук : 23.00.01. Львів, 2016. С.186.

³ Ковальова О. Політичний дискурс: сучасні лінгвістичні інтерпретації. *Актуальні питання гуманітарних наук*. 2020. Вип.27. Т. 2. С.101-107.

виокремлює «два розуміння політичного дискурсу: вузьке (політичний дискурс – це весь масив усного й письмового мовлення політичних лідерів або осіб, які прагнуть ними стати, провідних громадських активістів) і широке (політичний дискурс – це множина всіх комунікацій у суспільстві, які прямо чи опосередковано стосуються політичної сфери)»¹. Такий підхід видається нам виправданим.

Н.Г. Акінчиць відзначає, що у рамках лінгвістичних досліджень виокремлюються два підходи до аналізу дискурсів – дескриптивний і критичний. «Дескриптивний зосереджений на вивченні мовної поведінки політиків, риторичних прийомів, маніпулятивних стратегій, а також змістовної сторони політичних текстів. Критичний підхід націлений на дослідження мови як засобу владарювання й соціального контролю, з акцентом на соціальні нерівності, втілені в дискурсі як *veiling* (одна з форм схованого соціального тиску за допомогою мови). Головна мета дискурс-аналізу – простеження форм і методів, за допомогою яких дискурсивні структури (лексеми, тематичні структури) стають об'єктами політичних маніпуляцій»². Важливий наголос робить Л.Нагорна, вказуючи, що «політичний дискурс» – це не лише мовленнєва діяльність, але й політична поведінка»³.

Інформаційно-психологічна війна, що може знаходити своє вираження у політичному дискурсі найбільш яскраво проявляється у масовій пропаганді. Політичний дискурс (промова) – це сильний символічний, соціальний й психологічний історично обумовлений механізм впливу на аудиторію: «важливою рисою ПД є його опосередкованість ЗМІ та засобами масової комунікації

¹ Ключник Р.М. Дискурс протесту та політична коректність: до питання про евфемізми у політичній комунікації. *Регіональні студії*. 2018. № 13. С.30-35.

² Акінчиць Н.Г. Політичний дискурс як об'єкт наукового аналізу. *Культура народів Причорномор'я*. 2007. № 107. С. 72-76.

³ Нагорна Л.П. Політична мова і мовна політика: діапазон можливостей політичної лінгвістики. Київ : Світогляд. 2005. С.15.

(соцмережі). Це зумовлює рухливість його меж, завдяки якій ПД взаємодіє з іншими дискурсами, насамперед із масмедійним дискурсом»¹.

Говорячи про політичний дискурс, неможливо оминати й персону референта, лідера громадської думки – особливо харизматичного доповідача, артикуляція якого дозволить успішно вести пропагандистський чи дезінформаційний дискурс. В інформаційно-психологічній війні, політик, або «довірений» пропагандист, що розмовляє, не стільки індивідуальний суб'єкт, чи окреме джерело, скільки виразник міжособистісної взаємодії, початок колективного суб'єкта. У їх промовах чергуються агітаційні заклики, мрії (часто про світле майбутнє, яке от-от настане), словесне нагромадження, повтори. Крім того, слушною, у цьому контексті є думка С.М.Наумкіної та П.Л.Гайдаєнка: «Методи, оформлення та ступінь впливу, сигнали для успішного впливу через вербальні форми комунікації у соціальних медіа включають не тільки риторику та частоту використання метафор, а й особливості самого лідера: сила голосу, жести, які тим або іншим чином впливають на сприйняття виступу тощо...З точки зору впливу через мережі де превалює текстовий формат, лідери-харизмати активно використовують креолізовані тексти, або семіотично збагачений текст, де задля акцентування на специфічному повідомленні використовуються візуальні прийоми, тобто колір у тексті, або ілюстрації кадрів, фотоматеріалів, таблиць, що викликають бажані для лідера реакції у групи»².

Крім того, не останню роль у цьому аспекті відіграє іміджологія. У найбільш спрощеному вигляді політичний імідж – це «суспільна думка електорату про політика чи партію»³. М.І.Милосердна відзначає: «лідер, якщо говорити про

¹ Ковальова О. Політичний дискурс: сучасні лінгвістичні інтерпретації. *Актуальні питання гуманітарних наук*. 2020. Вип.27. Т. 2. С.101-107.

² Наумкіна С.М., Гайдаєнко П.Л. Роль харизматичної сигналізації у контексті політичного лідерства в соціальних мережах. *Актуальні проблеми політики* : зб. наук. пр. Одеса : Видавничий дім «Гельветика», 2022. Вип. 69. С. 48-54. DOI <https://doi.org/10.32837/app.v0i69.1301>.

³ Лактіонов О.М., Хомуленко Т.Б. Політична психологія та іміджеологія : навчально-методичний посібник. Харків, 2009. С.59.

агресивну складову проявів його політичної поведінки, – це особистість, яка вміє робити постійний психологічний тиск на людей (принаймні у формі латентного, внутрішньо відчутного виборцями нападу), має рішучість, демонструє метафоричну погрозу, як можливість потенційної дії. При цьому реальної загрози може і не бути, є лише її імітація...»¹.

Не менше важливою є вага окремих слів. У роботі В.Клемпепера «LTI. Мова Третього рейху. Записки філолога» відзначено: «Який пропагандистський засіб гітлерівщини був найбільш сильним? Були це окремі промови Гітлера і Геббельса, просторікування з того чи іншого питання, їх цькування євреїв, паплюження більшевизму... Ні, найсильніший вплив мали не окремі промови і не статті, листівки, плакати чи знамена, такого ефекту не могли мати засоби, розраховані на мислення чи осмислення сприйняття. Нацизм в'їдався у плоть і кров мас через окремі словечка, звороти мови, конструкції речень, що втовкмачувалися у натовп мільйонними повторами і поглиналися ним механічно і безсвідомо»².

Інформаційно-психологічна війна, що ведеться через політичний дискурс полягає не в тому, аби думати згідно з правилами логіки, а в тому, аби звести думку до переконання, не використовуючи чи майже не використовуючи аргументи, а якщо вони навіть є, то апелюють до емоцій, а не до розуму; часто існує сценарій протиставлення «інших» – «нам». Крім того, широко використовуються мовностилістичні засоби, такі як: риторичні фігури, або як висловлювався Т.Прокопович – «мовні фігури – те, що виражається граціозніше, красивіше, ніж звичайно прийнято»³. Оминаючи питання характеристики ораторських формул і стилів, які стали уже класичними, відзначимо лише, що риторичні фігури повинні прикрасити дискурсивну структуру, виразити певну послідовність і емоційну

¹ Милосердна І.М. Імідж політичного лідера як категорія PR-технології. *Актуальні проблеми політики* : зб. наук. пр. 2019. Вип.64. Одеса : Фенікс. С. 118-133.

² Клемперер В. LTI. Язык третьего рейха. Записная книжка филолога. С.9. *Almenda.org* : веб-сайт. URL: bit.ly/3r5Ai3I (дата звернення: 18.02.2022).

³ Прокопович Т. Філософські праці. Вибране. Київ : «Дніпро», 2012. С.270.

значимість, переконливість інколи з театральними елементами через тон, голос, ритм, паузи, жести, символи; ідеологеми – «певна одиниця когнітивного рівня чи багаторівневий концепт, у структурі якого актуалізуються ідеологічно марковані концептуальні ознаки, що містять колективні, стереотипні, міфологізовані уявлення про владу, суспільство, інститути тощо»¹. В інформаційно-психологічній війні використовуються різні ідеологеми – «демократія», «конституція», «буржуазія», «геноцид». Так, із початку російсько-української війни, Росія просуvala дезінформаційні наративи про «геноцид» – вбивства українськими військовими мирного населення на Донбасі; міфологеми – емоційно-забарвлені із символічно-міфологічним характером позначають міфологічні сюжети, сцени, образи – «смерть», «воскресіння», «рай», «пекло» тощо; інфологеми – поняття, що «використовується для позначення неправдивої або викривленої інформації зазвичай свідомо створюваної політтехнологами для заміщення базових фактів артефактами...Завдання інфологем – формування викривленої картини світу, стійких стереотипних уявлень, ідеологічних міфів і под. із метою цілеспрямованого маніпулятивного впливу на свідомість і поведінку людей»²; метафори, які за словами Г.Добровольської є «не тільки засобами оформлення мовлення, а й способом пізнання навколишнього світу. Вони допомагають краще зрозуміти політичні явища, а також можуть впливати на людей»³. Так, російська стаття «Настання Росії і нового світу», яка була присвячена «успіху спецоперації в Україні» розпочинається із метафори «новий світ народжується на наших очах», крім того, у тексті можна зустріти такі: «відновлення історичної повноти», «історична відповідальність», «комплекс розділеного народу», «підвищення градусу супротиву», «європейський проєкт просто рухне», «побудова нового

¹ Лютий Т.В. Мова та ідеологія. *Магістеріум. Історико-філософські студії*. 2016. Вип. 65. С. 14-22.

² Новітня політична лексика (неологізми, okazіоналізми та інші новотвори) / І.Я. Вдовичин, Л.Я. Угрин, Г.В. Шипунов та ін.; за заг. ред. Н.М. Хоми. Львів : «Новий Світ – 2000», 2015. С.156.

³ Добровольська Г. Семантичні групи метафор в українському політичному дискурсі. *Філологічні студії*. 2017. С.30-34.

світового порядку», «епоха західного глобального господарювання» тощо; досліджуючи інформаційно-психологічну війну потрібно звернути увагу і на пейоративи (пейоративну лексику). Л. Білоконенко відзначає, що, «залежно від контексту, конкретна лексична одиниця може реалізовувати своє пейоративне значення, якщо структура цієї одиниці має емотивно-оцінний аспект»¹, однак, основною ознакою пейоративів залишається негативне ставлення до конкретних людей, країн чи подій і їх висловлення у формі, на кшталт: «Польща без мізків», «пан Зю», «НА Україні» тощо; неологізми, наприклад, «неонацизм»; евфемізми – «слово або вислів, троп, що вживається для непрямого, прихованого, зокрема пом'якшеного, ввічливого позначення певних предметів, явищ, дій, замовчування їх прямої назви»². Евфемізмом є, наприклад, «спеціальна воєнна операція»; гіберболізація – ефект перебільшення, надмірності; в інформаційно-психологічній війні використовують як «хороші», «ідеальні» форми, які живлять внутрішні фантазії мас про «захист», «нову країну», так і максимально негативні гіперболи про «руїни», «крах», «вимирання», «знищення людства».

В окремих випадках інформаційно-психологічна війна супроводжується наявністю певної символіки, гасел із стилістичними і риторичними властивостями і специфічними способами звернення. Вони, зокрема, покликані провести «чітке оцінювання, ярлики, захист «своїх», приниження «ворогів», підміна понять, розділення понять, узагальнення, пропагандистські кліше, багаторазове повторення меседжу з незначними варіаціями»³.

Н.К. Ктитарова знаки-символи визначає як «знаки, які використовують для передачі (визначення) абстрактного змісту. Для них характерна відсутність

¹ Білоконенко Л.А. Пейоративна й інвективна лексика в міжособистісному конфлікті. *Філологічні студії : Науковий вісник КНУ* : зб. наук. праць. 2012. Вип. 7. Ч. 2. С. 119–127.

² Бовгиря О.О., Кирилюк М.А. Евфемізми як засіб маніпуляції в німецькому політичному дискурсі. *Філологічні науки: історія, сучасний стан та перспективи досліджень* : матеріали науково-практичної конференції, м. Львів, 20-21 вересня 2019 р. Херсон : Видавництво «Молодий вчений», 2019. С.35-38.

³ Писаренко Л.М. Комунікативна пропаганда та маніпуляція в гаслах та слоганах політичних лідерів. *Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (з нагоди 30-річчя проголошення незалежності України та 25-річчя прийняття Конституції України)* : у 2 т. : матеріали міжнар. наук.-практ. конф., м. Одеса, 21 трав. 2021 р. Одеса : Видавничий дім «Гельветика», 2021. Т. 1. С. 712-715.

природного зв'язку з позначуваними об'єктами»¹. У словниковій літературі політична символіка (гр. *symbolikós* – знаменуючий, образний, алегоричний) визначається як «різноманітні знаки, символи, які є предметами або актами людської поведінки, що відноситься до політичної сфери і є культурною пам'яттю певних соціальних груп чи усього *суспільства*. Вона безпосередньо пов'язана із боротьбою за владу та її здійсненням; її основним завданням є пробуджувати певні почуття та спонукати до дій. До головних ПОЛІТИЧНИХ СИМВОЛІВ відносяться мовна символіка (документи, лозунги та ін.), зображальна символіка (плакат, карикатура, герб та ін.)»². Символьна інженерія інформаційно-психологічної війни породила політичну мітологію: «інформаційне конструювання політичної реальності і комунікація між суспільними та державними інститутами здебільшого здійснюється за допомогою різноманітних символічних форм, серед яких чи не найбільшим потенціалом володіє політичний міф, що спирається на архаїчні уявлення та звичні образи»³. У загальному, як відзначає Є.Макаренко, «політичні міфи містять перекручений і містифікований образ конкретної політичної та економічної ситуації й мають здатність швидко поширюватися у суспільній свідомості. Як свідчить досвід, політичні міфи, піднесені в ранг офіційної політики становлять велику небезпеку і виступають засобом маніпулювання масами. Вони негативно впливають і на буденну політичну свідомість, яка внаслідок неповноти або відсутності потрібної інформації здатна до некритичного сприйняття хибних уявлень»⁴. Ю.Шаргородський відмічає «багатоаспектність політичного міфу (міф як феномен свідомості, наукова категорія, історична реальність, складова символічного світу політики тощо)» і визначає це явище як «певну світоглядну систему, яка з теоретичної точки зору включає такі структурні елементи: архетип певної ситуації, пов'язаної зі здійсненням заходів соціального регулювання і

¹ Китарова Н.К. Загальне мовознавство : навчальний посібник для студентів вищих навчальних закладів. Дніпродзержинськ : Дніпродзержинський державний технічний університет, 2009. С.13.

² Політологія: сучасні терміни і поняття : короткий навчальний словник-довідник для студентів ВНЗ I-IV рівнів акредитації / укладач В. М. Піча ; наук. редакція Л.Д. Климанської, Я.Б. Турчин, Н. М. Хоми. Львів : Новий Світ – 2000, 2015. С.361.

³ [Закіров М.](#) Міф як засіб інформаційного впливу та інструмент політичної комунікації. *Наукові праці Національної бібліотеки України імені В. І. Вернадського*. 2017. Вип. 48. С. 630-644.

⁴ [Макаренко Є.](#) Проблема міфу в системі сучасної політичної науки. *Наукові записки Інституту політичних і етнонаціональних досліджень ім. І.Ф. Кураса НАН України*. 2012. Вип. 4. С. 289-299.

примусу («якщо..., то...»); зміст конкретного досвіду, отриманого в ситуаціях, об'єднаних цим архетипом; сукупність алегоричних образів, функціональна символіка яких співвідносить «бажане» з «належним», тобто зі сформованим архетипом. Аксіологічна цінність політичного міфу полягає в можливості викликати до життя той архетип, який дозволить задати певний мотив діяльності – через політичну рекламу, ритуал, містерію. Архетип уможливорює поєднання бажаного і належного спочатку в міфологічних категоріях, згодом – у політичній діяльності»¹. Міфи розвивають діапазон «інтуїтивних» знань, які, при цьому допускають лише одну інтерпретацію. Політичні міфи мають здатність настільки сильно укорінюватися у свідомості, що мають рушійну силу для контролю над особистістю, яка стає не сприйнятливою до інших точок зору.

І.І. Проноза, О.Г. Деревянко відзначають: «в інформаційно-психологічній війні, війні нового типу, використовується канал безпосереднього впливу на суспільну свідомість, на душі людей. Завдання полягає в тому, щоб змусити маси діяти в потрібному напрямі навіть проти своїх інтересів, а в стані супротивника розколоти людей, щоб вони повстали один проти одного. У цій війні істотне значення має практичний досвід впливу на свідомість людей»².

У літературі комунікацію визначають як «технічний процес обміну інформацією між двома і більше індивідами (або групами)... Поняття комунікація може вживатися у значенні: 1) соціальна комунікація, спілкування між людьми та іншими соціальними суб'єктами; 2) зв'язок за допомогою технічних засобів; 3) певна система, за допомогою якої забезпечується сполучення між віддаленими об'єктами, наприклад, підземні комунікації...»³. Очевидно, що для інформаційно-

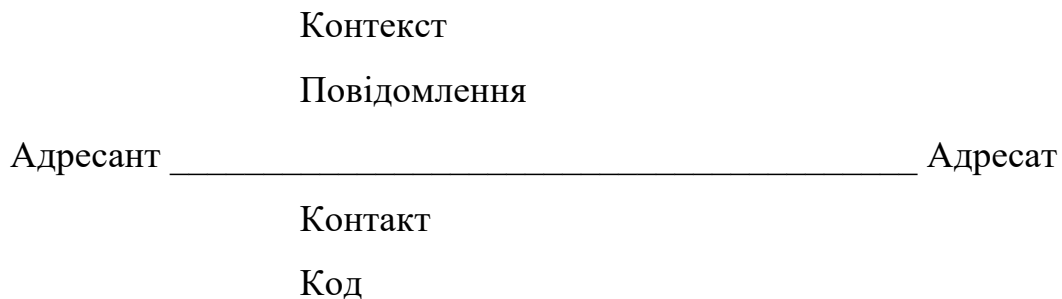
¹ Шайгородський Ю. До визначення сутності поняття «політичний міф». *Сучасна українська політика : політики і політологи про неї*. 2009. Вип.16. С. 49-53.

² Проноза І.І. Інформаційно-психологічні війни як механізм управління суспільно-політичною свідомістю. *Сучасна українська держава: вектори розвитку та шляхи мобілізації ресурсів* : матеріали П'ятої Всеукраїнської науково-практичної конференції, м. Одеса, 3 квітня 2020 року. Одеса : ПНПУ імені К. Д. Ушинського, Центр соціально-політичних досліджень «Politicus», 2020. С. 46-50.

³ Косенко Ю.В. Основи теорії мовленнєвої комунікації : навч. посібник. Суми : Сумський державний університет, 2013. С.19.

психологічної війни значення мають перші два розуміння комунікації. Інформаційно-психологічна війна є частиною політичної комунікації – вона звернена до всього суспільства, а не до обмеженого кола осіб, її мета не у тому, аби спілкуватися із науково доказовим змістом, а більше емоційно переконати громадян чи виборців, однак, ототожнювати на наш погляд ці поняття не варто, хоча б з урахуванням того, що політична комунікація – діалог з громадськістю, який може бути заснований на довірі і не містити маніпулятивних впливів. М.І. Милосердна вказує: «політична комунікація є своєрідним соціально-інформаційним показником політики, який представляє собою процеси передачі, обміну політичною інформацією, яка структурує політичну діяльність і надає їй нового значення»¹.

До інформаційно-психологічної війни можна застосувати різні комунікаційні моделі, наприклад, модель Лассвелла: Хто? Що? Яким засобом? До кого? З яким результатом? або модель Якобсона:



До адресантів інформаційно-психологічної війни можна віднести:

1. Недержавні суб'єкти – ретлянслятори маніпулятивних впливів, які не обмежуються ЗМІ, інформаційно-психологічна війна яких цільова і багатовекторна, часто включає медіа-контент з уроками історії, новини, репортажі, сюди ж можна віднести і терористів, апарат джихадистської пропаганди з курсами теології, засновані на екстремістському прочитанні релігійного тексту. Так, ІДІЛ використовує соціальні мережі, блоги, месенджери, Twitter, Facebook, Instagram, WhatsApp, Tumblr, Телеграм і на спеціалізованих формах (форуми тероризму).

¹ Милосердна І.М. Комунікація та зворотний зв'язок у структурі кібернетичного механізму політичного управління. *Актуальні проблеми політики* : зб. наук. пр. 2019. Вип. 63. Одеса : Фенікс. С.153-165.

2. Державні суб'єкти – загалом, «в політології прийнято виділяти кілька видів суб'єктів політики, причому існує кілька концепцій щодо даного поділу. Перша концепція поділу політичних суб'єктів на види. Перший вид – це безпосередні учасники політичного життя: держава, партії, політичні лідери, громадські організації, рухи. Саме ці суб'єкти політики постійно обертаються на політичній сцені, з ними масову свідомість пов'язує політику. Другий вид суб'єктів політики – великі соціальні групи і спільності (соціальні класи, стани, міжкласові і внутрішньокласові групи). Третій вид – політична еліта, фінансово-промислові структури, тіньові і напівлегальні об'єднання. Цей вид суб'єктів дуже складно виявити...»¹. Інформаційно-психологічна війна може бути спрямована як *внутрішньо, так і зовнішньо*. У більшості випадків, влада маніпулює інформацією аби укріпити своє становище, тому важливе значення мають три фундаментальні фактори: 1) розуміння ключових принципів роботи; 2) розуміння цільової аудиторії; 3) оцінка ефективності різних методів інформаційно-психологічної війни.

Адресатами інформаційно-психологічної війни є маси, оскільки інформаційно-психологічна війна – складова політичних комунікацій і масових комунікацій.

Серед характерних рис інформаційно-психологічної війни як політичної комунікації можна виділити:

1. Одна із сторін, яка може бути представлена й у виді групи є спікером (адресант), чи тим, хто надсилає повідомлення. Інша сторона називається респондентом (адресат) і зазвичай є масовою аудиторією, отримувачем повідомлення. Спікер є активною стороною, адресат – більш пасивним отримувачем повідомлення. Однак, така асиметричність характерна не для всіх випадків інформаційно-психологічної війни. У деяких випадках, група, респонденти беруть участь у двосторонньому діалозі, відповідаючи позитивно чи

¹ Мамонтова Е.В., Краснопольська Т.М. Гібридні форми сучасної політики : навчально-методичний посібник для здобувачів третього (освітньо-наукового) рівня вищої освіти. Одеса, 2021. С.15.

негативно на повідомлення спікера чи навіть сумніваючись чи критикуючи це повідомлення, відбувається генерування інформації, яке спікер може використовувати у якості зворотнього зв'язку.

2. Зміст повідомлення зазвичай виражений словесно чи іншими способами (наприклад, іконографічно), які підходять для зміни поглядів і спонукання до дій. Або бути сумішшю того й іншого, наприклад, телеведучий може коментувати створений відеоряд, у пропаганді часто використовують матеріали сцени, такі як барабани і прапори, може використовуватися музика, театр чи інформація передається у драматичному форматі, такому як фільм чи роман. У деяких випадках пропаганда може передаватися за допомогою таких предметів, як монети чи статуї, чи навіть за допомогою костюмів (сукні, маскування) і сценарії, які виражають цінності певного способу життя. Змішування психології з ідеологією; духовних явищ із пропагандистськими деклараціями, що спрямовані не на відображення реальної атмосфери у суспільстві, а слугують формуванню стереотипів масової свідомості, які потрібні владі. Важливу роль у цьому процесі відіграє простота ідей, близьких народній свідомості понятійних категорій, спрощена лексика, розмовна мова.

3. Успішною можна вважати ту інформаційно-психологічну війну, у результаті якої адресат прийме певні дії чи підтримає певну політику дій, адже її метою є підтримка існування, мети й інтересів конкретного режиму, організації, точки зору чи групи інтересів. Нерідко метою інформаційно-психологічної війни є підтримка інтересів країни чи політичної партії, уряду, режиму.

Інформаційно-психологічна війна ведеться не з індивідуумом, а з масами, індивід не є предметом її цікавості, це пов'язано, зокрема із тим, що переконати у чомусь окрему особу може бути складно. Індивід вважається частиною маси, адже за цих умов його можливість до супротиву слабшає, із його поведінкою легше працювати: телеглядач чи радіослухач ніколи не розглядається ізольовано, він

завжди – частина групи, одиниця, що поміщена у невидимий, але натовп і разом ця спільнота взаємно впливає один на одного.

Натовп не роздумує, про те, приймає він ідеї чи відкидає їх, він не хоче ні обговорень, ні заперечень, його пропозиції повинні негайно перетворитися у дії, оскільки ними рухає емоційність та імпульсивність. Так, маси готові пожертвувати собою заради ідеала життя, чи особи лідера, який його надихає. Бурхливі відчуття і крайнощі, симпатія швидко переходить в обожнювання, а майже антипатія перетворюється у ненависть, оскільки інформаційно-психологічна війна створила вакуум, у якому натовп живе спільними ідеями, мітами, мотивами, вони отримують однакові імпульси, враження, переживають однакові почуття, і як наслідок – мають однаковий порядок реакцій і формують однакові ідеї, їх увагу сфокусовано на одних і тих самих темах. При цьому, тривалість уваги публіки завжди обмежена. Щось миттєво стає публічною темою, коли всі ЗМІ конкурують за те, щоб виділити йому центральне місце в етері: так, під час пандемії Covid-19 із новин у всьому світі практично зникли і збройні конфлікти, і проблеми екології, діяльність терористичних організацій etc. Коронавірус перейняв на себе роль світової небезпеки. Тому інформаційно-психологічна війна не може існувати поза ЗМІ, оскільки її невід’ємна складова – тотальність. Однак, ефективність маніпулювання ЗМІ залежить не від символів чи метафор як таких, а від здатності за допомогою цих інструментів створювати емоційний контекст. Наприклад, у політичному контексті, слово «допомога» – фрейм, який включає постраждалу сторону і рятівника. Цей рятівник – герой, якому хочеться бути вдячним. Тому, будь-хто, хто намагається зупинити рятівника вважається злим. Якщо у цьому сенсі ми поєднаємо термін «полегшення» із терміном «податки», створивши таке політичне гасло як «звільнення від податків», то будь-хто, хто пропонує відмінити податки – герой, а хто хоче цьому перешкодити – зло. До того ж, слід звернути увагу на слова

Г.Г.Почепцова: «раніше в основі інформаційної війни стояло повідомлення, нині ж базою стає інтерпретація»¹.

Наративи можуть миготіти спорадично, або навіть випадково: гасла на стінах, стаття у газеті, допис у соціальній мережі. Кожна платформа має свій спосіб проникнення, своїх слухачів і глядачів, доповнює одна одну у досягненні спільної мети. А цілі групи людей опиняються у ситуації позаемоційного й позаінтелектуального життя, оточені з усіх сторін інформаційно-психологічною війною. О.В.Максимчук, С.С.Бондар вказують: «За допомогою ЗМІ інформацію можна: спотворити за допомогою неповного, одностороннього викладу (тобто фрагментарний спосіб поширення інформації – частка інформації подрібнюється на менші частки та коли інформація подається єдиним неопрацьованим потоком, що не дає людині змогу сформувати цілісну картину подій); показати щось у тому вигляді, в якому вигідно для когось; звертаючи увагу на окремі аспекти події, приховати малозначну деталь, замовчуючи інші, що створює додаткову змогу маніпулювати свідомістю людей; створити «інформаційний галас», коли зниження сприйняття фактів досягається шляхом подачі такої кількості новин, за якої стає неможливим їх сортування; відволікти увагу від дійсно важливих подій шляхом надання яскравої, але несуттєвої інформації; оперативно подати навіть неперевірену інформацію, адже будь-яке перше повідомлення про подію справляє значно сильніший вплив на аудиторію, ніж наступні»².

Інформаційно-психологічна війна намагається отримати контроль над масами, цілі можуть бути різні: збудження, організація, маніпулювання. Цей стратегічний процес, призначений для отримання різних результатів – починаючи від нестабільності і закінчуючи захопленням влади. Інформаційно-психологічна

¹ Почепцов Г.Г. Смыслові та інформаційні війни. *Інформаційне суспільство*. 2013. Вип. 18. С. 21-27.

² Максимчук О.В., Бондар С.С. Роль мас-медіа у формуванні політичних міфів. *Актуальні проблеми політики*. 2020. Вип.65. С.49-54.

війна присутня у зовнішній політиці, наприклад, для розхитування ситуації і заклики виступити проти політики влади зарубіжної країни.

Інформаційно-психологічну війну можна охарактеризувати як процес масово організований – «систематичне розповсюдження спеціально підготовлених повідомлень із застосуванням технічних засобів тиражування інформації (радіо, телебачення, преса, відео-, звукозаписи тощо), які мають соціальне значення і використовуються з метою впливу на установки, поведінку, думки й оцінки людей»¹ або *масово* стихійний «це чутки, інформація, що надходить від однієї або кількох осіб про непідтверджені події. Чутки з'являються тоді, коли система офіційної комунікації замовчує певні події. Інформація, яку вони містять, задовольняє потребу людини чи групи людей у змісті інформації, яку вони не отримали офіційними шляхами»². Відмітимо, що у науковій літературі щодо чуток існують різні точки зору: Вауліна В.Ф. відносить їх до мітології: «Іншим засобом розповсюдження міфу можуть бути чутки. Вони представляють собою форму масової комунікації з якою стикається кожна людина принаймні раз на день»³. В.Лисенко визначає чутки «як різновид неформальної комунікації, коли інформація в ситуації невизначеності чи напруги очікування з невизначеним ступенем достовірності, який з'ясувати в даний момент неможливо, викликаючи підвищений інтерес, швидко поширюється і стає надбанням великої аудиторії»⁴.

В.В.Воротинський в умовах підвищеної тривожності суспільства головним типом чуток вважає «чутку-лякалку». Зростання популярності соціальних мереж як джерел інформації є основою для формування нової форми чуток і

¹ Психологія спілкування : навч. посіб. / Л. Г. Кайдалова, Л. В. Пляка, Н. В. Альохіна, В. С. Шаповалова. - 2-ге вид., перероб. і допов. Харків : НФаУ, 2018. С.32.

² Психологія спілкування : навч. посіб. / Л. Г. Кайдалова, Л. В. Пляка, Н. В. Альохіна, В. С. Шаповалова. - 2-ге вид., перероб. і допов. Харків : НФаУ, 2018. С.32.

³ Вауліна Ф.В. Політична міфотворчість у сучасній Україні. *Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Питання політології»*. 2015. Вип. 14. С. 106-111.

⁴ Лисенко В. Чутки – активний засіб модифікації суспільної думки. *Політичний менеджмент*. 2004. №6. С.96-102.

способів їх розповсюдження, чим активно користуються протидіючі сили, політичні партії та лідери, громадські організації»¹.

До особливостей чуток можна віднести: 1) анонімність першоджерела – «його мати моїй матері – двоюрідна Параска», як мовиться в українському прислів'ї зазвичай була «свідком» події: прямих свідків немає, є лише другорядні, які «важливу новину» й переказують; 2) повідомлення – неформальне, псевдоподібне; 3) вільно циркулює у публічному просторі, звертається до колективної уяви; 4) зазвичай інформація песимістичного характеру, але дуже цікава для населення; 5) чутки здатні підтримувати атмосферу недовіри та невпевненості.

Досліджуючи питання масових настроїв, Я.Є.Кульба відмічає: «Очевидним у заданому контексті є й той факт, що способи та прийоми формування масових настроїв що раз відображено у виразних політико-психологічних технологіях відповідних політичних сил (звісно ж з використанням різноманітних сублімінальних форм впливу). У практиці ж ЗМІ масові настрої більшою мірою формується за допомогою відповідно забарвлених, уніфікованих (спрощених) уявлень та суджень (стереотипів, чуток, міфів, іміджу). Систематичне упровадження останніх у потік «організованих» новин автоматично зумовлює в масовій свідомості негативну або позитивну реакцію на конкретну подію, або ж формує відповідний загальний емоційний фон цільової аудиторії»². Людина у колективі більш сугестивна, хоча сам індивід вважає себе сильнішим, більш нестабільна, хоча переконана у твердості своїх намірів. У роботі К.Юнга відзначено: «можна сказати, що колективній психіці ніби як неадекватний усілякий індивідуальний розвиток, якщо тільки він безпосередньо не служить цілям колективного»³; «у наш час простяглася глибока прірва між тим, що людина є і тим,

¹ Воронинський В.В. Чутки як інструмент політичного маніпулювання в Інтернеті (на прикладі ситуації в Україні 2014 – початку 2015 років). *Сучасне суспільство*. 2015. Вип. 2(1). С. 4-12.

² Кульба Я.Є. Масові настрої: генеза та особливості функціонування. *Inforum: science for the future*. URL: <https://www.inforum.in.ua/conferences/15/19/116> (дата звернення: 17.03.2022).

³ Jung C.G. Psychological Types or The psychology of individuation / translated by Godwin Baynes M.B., Cantab B.C. London. 1946. P.106.

що вона собою являє, іншими словами між людиною-індивідуумом і людиною, що функціонує як частина колективу»¹.

Колективне сприйняття фундаментальних істин зберігаються і їх складно змінити з плином часу. Елементи, що підлягають впливу багатьох факторів, в тому числі індивідуальні і культурні переконання, норми, вразливість, мотивація, емоції, переживання, мораль, освіта, психічне здоров'я, ідентичність, ідеологія.

Однією із функцій комунікації є здійснення впливу – «зміна стану, поведінки; ціннісно-мотиваційної сфери, особистісно-сміслових утворень; намірів, настанов, думок, рішень, потреб, дій, оцінок»². У цьому контексті, інформаційно-психологічна війна нерозривно пов'язана із такими поняттями, як «навіювання», «переконання» (обидва асоціюються із чимось гіпнотичним) – «свідомо аргументований вплив на іншу людину або групу людей, що має своєю метою змінити їхнє судження, ставлення, намір або рішення. Переконуючий вплив розуміється переважно як інтелектуальний психологічний вплив, заснований на передачі логічно побудованої інформації, що має на меті добровільне її прийняття як спонукальний мотив діяльності»³, «емоційне зараження», «наслідування», а відтак, фундаментальне значення має соціальна психологія, предметом якої «є закономірності психічної діяльності, поведінки та взаємодії людей як представників соціальних груп, психологічні характеристики самих цих груп та психологічні аспекти будь-яких інших явищ соціального життя»⁴, одним із розділів якої є політична психологія – «галузь соціальної психології, яка вивчає психологічні компоненти політичного життя суспільства, політичну свідомість та поведінку суб'єктів політичних процесів. У рамках цієї галузі досліджують соціально-

¹ Jung C.G. Psychological Types or The psychology of individuation. / translated by Godwin Baynes M.B., Cantab B.C. London. 1946. P.96.

² Психологія спілкування : навч. посіб. / Л. Г. Кайдалова, Л. В. Пляка, Н. В. Альохіна, В. С. Шаповалова. - 2-ге вид., перероб. і допов. Харків : НФаУ, 2018. С.9.

³ Захаренко Л.М., Давидова О.В. Психотехнології ведення перемовин із правопорушниками : метод. рекомендації / за заг. ред. О. І. Мотляха. Київ : Освіта України, 2020. С.46.

⁴ Соціальна психологія : навч. посіб. для здобувачів ступеня бакалавра / Н. Ю. Волянчук, Г. В. Ложкін, О. В. Винославська, І. О. Блохіна, М. О. Кононець, О. В. Москаленко, О. І. Боковець, Б. В. Андрійцев. Київ : КПІ ім. Ігоря Сікорського, 2019. С.12.

психологічні умови формування суспільно-політичних інтересів молоді, психологічні чинники впливу на поведінку виборців, характерні психологічні особливості політичних діячів та інші проблеми»¹. Наприклад, пропагандист вибудовує свою діяльність з урахуванням знань про людську природу: схильності людини, потреби і психічні механізми, проводить аналіз середовища.

Інформаційно-психологічна війна спрямована на бажанні зміни волі. Психіка – індивідуальна та колективна представляється як поле битви, а психологія є зброєю, особливо у частині психологічного впливу, сутність якого у літературі зводиться до «проникнення» однієї особистості (або групи осіб) у психіку іншої особистості (або групи осіб). Даний вплив на психічний стан, думки, почуття і дії іншої людини здійснюється винятково за допомогою психологічних засобів (вербальних або невербальних). Психологічний вплив має зовнішнє (відносно реципієнта) походження і, будучи сприйнятим ним, приводить до зміни конкретних психологічних регуляторів певної активності людини»². До стратегій психологічного впливу і літературі відносять маніпулятивну стратегію – «об’єкт психологічного впливу активний, володіє внутрішнім потенціалом і логікою розвитку: мета впливу відкрито не оголошується, а досягається суб’єктом впливу шляхом формування активності об’єкта впливу в бажаному напрямі»³.

Таким чином, маніпуляція – є одним із видів психологічного впливу, об’єднувальним поняттям стосовно методів інформаційно-психологічної війни. Інформаційно-психологічна війна використовує методи маніпулювання з як непомітний вплив на громадську думку у великих масштабах. Перетворення реальності шляхом маніпулювання громадською думкою часто відбувається за

¹ Соціальна психологія : навч. посіб. для здобувачів ступеня бакалавра / Н. Ю. Воляннюк, Г. В. Ложкін, О. В. Винославська, І. О. Блохіна, М. О. Кононець, О. В. Москаленко, О. І. Боковець, Б. В. Андрійцев. Київ : КПІ ім. Ігоря Сікорського, 2019. С.15.

² Ніколаєнко С., Ніколаєнко Св. Категорія психологічного впливу в психології. *Світогляд - Філософія – Релігія* : 36. наук. пр. 2011. № 1. URL: bit.ly/3PwfU56 (дата звернення: 14.02.2022).

³ Захаренко Л.М., Давидова О.В. Психотехнології ведення перемовин із правопорушниками : метод. рекомендації / за заг. ред. О.І. Мотляха. Київ : Освіта України, 2020. С.9.

допомогою стереотипних висловлювань, і має тенденцію до зв'язку не з розумом, а з безсвідомим, ірраціональним. Теми особливого соціального значення – шокуючі теми расизму, війна, екологія, тощо.

Інформаційно-психологічну війну не слід ототожнювати із маніпулюванням, оскільки останнє її супроводжує, а не зливається. Крім того, попри систематичний характер інформаційно-психологічної війни, маніпулювання використовується ще частіше не лише на маси, але й у міжособистісних стосунках, починаючи від торгівлі і закінчуючи внутрісімейними відносинами.

В.М.Петрик, М.М.Присяжнюк, Л.Ф.Компанцева під маніпулюванням розуміють «вид психологічного впливу, майстерна реалізація якого веде до прихованого збудження в іншій людини намірів, які не збігаються з її реальними бажаннями»¹. На думку М.І.Задорожної, «головне завдання інформаційних війн полягає у маніпулюванні масами. Мета такої маніпуляції найчастіше полягає: у внесенні в суспільну та індивідуальну свідомість ворожих, шкідливих ідей та поглядів; дезорієнтації та дезінформації мас; послабленні певних переконань, устроїв; залякуванні свого народу образом ворога; залякуванні супротивника своєю могутністю»².

Говорячи про психологічні особливості, неможливо оминати і середовище. Середовище відтворює специфічні ефекти, які не пов'язані безпосередньо із повідомленням, а пов'язані з умовами сприйняття. У цьому різниця, між, наприклад, пропагандою у великій залі і по телевізору чи радіо. У залі повідомлення видається теплішим, оскільки його сприймає натовп (враховуємо і наведені вище характеристики натовпу), який зібрався на відносно короткий час, часто занурений у пітьму, інстинктивно, у стані зачарованості і анонімності, натомість, домашнє

¹ Сугестивні технології маніпулятивного впливу : навч. посіб. / В.М.Петрик, М.М.Присяжнюк, Л.Ф.Компанцева, Є.Д.Скулиш, О.Д.Бойко, В.В.Остроухов; за заг. ред. Є.Д.Скулиша. 2-ге вид. Київ : ЗАТ «ВІПОЛ», 2011. С.11.

² Задорожна М.І. Державне управління в умовах гібридної війни: маніпуляція суспільною свідомістю. Публічне адміністрування: теорія та практика. 2017. Вип. 2 (18). С.1-17. URL: http://nbuv.gov.ua/UJRN/Patp_2017_2_9 (дата звернення: 18.03.2022).

телебачення фрагментарне і увага часто відволікається на їжу, бесіди, а часте перемикання каналів сприяє інтелектуальній віддаленості, хоча, при безсистемному «споживанні» інформації через телебачення із вправними спікерами, інформаційно-психологічна війна досягне своїх цілей.

Беззаперечно, інформаційно-психологічна війна сьогодні – складова технологічного Всесвіту. Сьогодні інформаційно-психологічна війна прийняла нову форму, пов'язану із технічним прогресом – це війна у високотехнологічних умовах, а Інтернет став місцем її активного розгортання що загрожує внутрішній безпеці та сталому функціонуванню демократичних інститутів. Особливо корисним для інформаційно-психологічної війни став зростаючий успіх соціальних мереж: сучасні платформи, альтернативні традиційним ЗМІ, безкоштовні, прості у доступі, а головне – охоплюють широкі маси. «Сьогодні народжується новий тип прямої демократії – мережева демократія, яка формує середовище і механізми мобілізації для прояву активності, допомоги, захисту, громадського активізму та волонтерства, для вибудовування ефективних вертикальних і горизонтальних комунікацій в суспільстві, для акумулювання соціального капіталу та сприйняття інновацій. Інтернет-простір є важливим фактором модернізації в сучасній Україні, підвищує громадянську активність, забезпечує необхідні умови формування громадянського суспільства та інтеракцію громадянського суспільства і держави в цифровому просторі»¹.

Фільтри в Інтернеті, зокрема, у соціальних мережах на сучасному етапі здатні показувати контент, який відповідає особистим поглядам користувача. Алгоритми створюють набір даних, які відображають максимально персоналізований результат, що призводить до ситуації, де у користувача усе менше шансів ознайомитися з іншими поглядами, він ізолюється в «інформаційному міхурі». Прагнучи встановити монополію на «інформаційну комунікацію» тоталітарні

¹ Краснопольська Т.М., Милосердна І.М. Цифрові технології в механізмі взаємодії громадянського суспільства та держави. *Актуальні проблеми політики* : зб. наук. пр. 2021. Вип.67. Одеса. С. 68-74.

держави пішли далі, спеціально перемішуючи комунікацію державної політики із інформацією про стан політики. Так, вони побудували симулякри реальності, які подаються населенню як дійсність.

Методи інформаційно-психологічної війни і зростаюча цифровізація сприяють створенню «мережі альтернативних уявлень» у віртуальному середовищі, що найкраще розповсюджуються через соціальні мережі у той час як телебачення втрачає домінуючий вплив. Експоненціальний розвиток цифрових платформ підвищив ризик маніпулювання інформацією багатьма способами: 1) надлишок інформації – «інфоожиріння», який є шкідливим для прийняття рішень; 2) більша точність сегментації і адресність населення (мікротаргетинг); 3) дешевизна подачі інформації: декілька кліків – декілька хвилин; 4) демократизація журналістської діяльності – легко зробити блог, одна сторінка, один сайт «професійне» подання інформації, де кожен – «репортер». Досліджуючи відеоблог як інноваційний засіб політичної комунікації учені К.М. Вітман та А.І. Кормич відзначають «миттєва реакція на контент і загроза втрати популярності через скандали або критику від інших представників спільноти є особливим важелем етичної регуляції дій блогера. Однак відсутність законодавчих обмежень щодо Інтернету розширює діапазон фейкової інформації, спонукає до існування ботів тощо. З цієї позиції традиційні ЗМІ набагато сильніше обмежені нормативно-правовими актами у своїй діяльності, однак при цьому масового реагування на неаргументовано негативний матеріал або розміщення недобросовісної реклами очікувати не варто. Відеоблогери ж несуть особисту відповідальність за якість рекламованого продукту і зацікавлені в тому, щоб втримати або розширити свою аудиторію»¹; 5) технічний прогрес у редагуванні фото, відео та аудіо-контента, як наслідок – можливість підроблення, наприклад, діп-фейки.

¹ Вітман К.М., Кормич А.І. Відеоблоги як інноваційний засіб політичної комунікації. *Актуальні проблеми політики* : зб. наук. пр. 2021. Вип.68. Одеса : Видавничий дім «Гельветика». С. 52-57.

Інформаційно-психологічна війна в Інтернеті характеризується такими аспектами: використання «емоційно-заряджених» чи «підбурювальних» висловів; цитування мітів (у тому числі тих, які було розвінчано); вербальна аргесія, спрямована на конкретних осіб, організації чи країни, а не на аналіз фактів; скептицизм і критика тих, хто розкриває факти, а не зворотня аргументація.

Зазвичай, для досягнення цих цілей використовують послуги так званих «інтернет-ботів» (політичні боти, тролі) – такі можливості надають інформаційно-психологічній війні ефекту достовірності.

Інформаційно-психологічна війна ведеться у мирний, кризовий чи воєнний час (означимо його як конфліктний) і, зведемо до двох основних типів – мирного і конфліктного.

Фактично, саме фізичне насильство є єдиним диференційним критерієм мирного і конфліктного часу.

Якщо зброя орієнтована на фізичне знищення, то інформаційно-психологічна війна намагається домогтися капітуляції ворога, уселити у його розум сумніви чи страх, змусити збройні сили зрадити свого лідера. Відбувається перетворення реальності шляхом маніпулювання громадською думкою як у напрямку деморалізації противника, так і створення розколу у його країні. Тому, заволодіння інформаційним полем у великих обсягах стає однією із *sine qua non* умов ефективності інформаційно-психологічної війни. Оскільки той, хто більше і краще спілкується охоплює найбільше поле думок.

Таким чином, цілісне уявлення про інформаційно-психологічну війну неможливе без виокремлення ряду її складових, логічна послідовність яких окреслює горизонт дослідження інформаційно-психологічної війни.

2.2. Інструментарій інформаційно-психологічної війни.

Інформаційно-психологічну війну не оминули проблеми термінології, зокрема, змішування уже класичних понять «пропаганди», «маніпуляції», «дезінформації», «чуток», «змови» із неологізмами «fake news», «постправда», що множить і без того складне розуміння інформаційних війн. До того ж, дискусії викликає розуміння *методів* інформаційно-психологічної війни. В.М.Петрик основними з них вважає: «дезінформування; пропаганду; диверсифікацію громадської думки; психологічний тиск; поширення чуток»¹. Частково підтримаємо таку точку зору – на наш погляд, дезінформація, пропаганда та поширення чуток відносяться до методів інформаційно-психологічної війни. Щодо диверсифікації громадської думки, Ю.О. Горбань вказує, що вона «має на меті розпорошення уваги правлячої еліти держави на різні штучно акцентовані проблеми і тим самим відволікання її від вирішення першочергових завдань суспільно-політичного та економічного розвитку з метою забезпечення нормального функціонування суспільства і держави. Її формами є: дестабілізація обстановки в державі чи її окремих регіонах; активізація кампанії проти політичного курсу правлячої еліти держави та окремих її лідерів різними міжнародними установами; ініціювання антидемпінгових кампаній та іншого роду скандальних судових процесів, застосування міжнародних санкцій з інших причин»². Виділення диверсифікація громадської думки як методу інформаційно-психологічної війни видається дещо абстрактним: яким чином досягається дестабілізація обстановки в державі чи окремих її регіонах? Із досвіду російського вторгнення нам відомо, що така дестабілізація може досягатися пропагандистськими та дезінформаційними наративами, тобто дестабілізація – це уже наслідок, те саме стосується і активізації кампанії – яким чином вона «активізовувалася»? Сама по собі активізація ще не

¹Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал*. 2009, № 5. С.122-135.

²Горбань Ю.О. Інформаційна війна проти України та засоби її ведення. *Вісник НАДУ*. 2015. №1. С. 136-141.

означає, що вона має маніпулятивне підґрунтя. Крім того, сумнівним видається саме уведення цього англіцизму у науковий обіг. У Оксфордському словнику іменник «diversification» розуміється як диверсифікація у щось (а не чогось) і визначається як 1) «акт розвитку більш широкого спектру продуктів, інтересів, навичок тощо, аби досягнути більшого успіху чи знизити ризик (наприклад, диверсифікація компанії у сторону товарів для здоров'я); 2) процес зміни, аби було більше розмаїття (еволюційне розмаїття квіткових рослин)»¹. Центр протидії дезінформації при РНБО використовує, на наш погляд, більш вдалий термін «заговорювання» – цей метод використовує пропаганда, коли необхідно знизити актуальність та викликати негативну реакцію до будь-якої події. Мета «заговорювання» – викликати втому в аудиторії від дезінформації з певної «гострої» теми, щоб відбити подальше бажання цікавитися нею. Приклад: не маючи можливості приховати відео, викладені у соцмережах, пропагандисти рф використовують метод «заговорювання» населення щодо [населення](#) щодо вибухів на Новофедорівському аеродромі в окупованому Криму»².

Психологічний тиск також видається надто узагальненим: «в психолого-юридичній літературі поняття «психологічний тиск» зазвичай розглядають у межах поняття «психологічний вплив», що є більш ширшим за значенням. Однак, дослідники часто ці поняття ототожнюють. Психологічний вплив неоднозначно оцінюється у психолого-правовій практиці і визначається як вплив на психічний стан, почуття, думки і вчинки інших людей, що відбувається як безпосередньо, так і опосередковано, оминаючи свідомість, логіку і розум, через навіювання і зараження, через звернення до почуттів і переживань, до несвідомого і звичок, до

¹ «Diversification». *Oxford learner's dictionaries* : веб-сайт. URL: <https://www.oxfordlearnersdictionaries.com/definition/english/diversification?q=diversification> (дата звернення: 22.02.2023).

2

ЦПД пояснює механізм «заговорювання» в дезінформації. *Центр протидії дезінформації при РНБО України* : веб-сайт. URL: bit.ly/44FzKiQ (дата звернення: 06.03.2023).

живих вражень і уявних страхів тощо»¹. Ми уже вказували на те, що інформаційно-психологічний вплив закономірно пронизує методи інформаційно-психологічної війни, а не є одним з них. Ю.М.Твердохдіб під методами (способами, механізмами, прийомами) ведення інформаційно-психологічної операції розуміє «усю сукупність дій та процесів, які здатні здійснювати інформаційно-психологічний вплив на свідомість та психіку людини та провокувати бажані поведінкові реакції...До основних методів інформаційно-психологічного впливу відносять: дезінформування; чутки; рефреймінг інформації; психологічний тиск; звертання до сильних емоцій – ненависті та ідеалізації. Ненависть – моральна якість, що відповідає відношенням ворожнечі, відрази і бажання зла іншим. Ідеалізація – нереалістично завищені характеристики об'єкта чи оцінювання щодо його поведінки та його дій». Вважаємо, що рефреймінг інформації та звернення до сильних емоцій можна віднести до пропаганди.

У літературі під дезінформацією розуміється «хибне повідомлення, свідомо перекручене й поширюване під виглядом достовірної інформації з метою введення в оману громадськості чи політичних конкурентів, спонукання їх до очікуваних дій; свідомо помилкова, неправильна, неправдива інформація; система прийомів, засобів, технологій, використання яких спрямоване на введення в оману, маніпулювання свідомістю, послаблення позицій конкурентів, опонентів, приховування прорахунків та помилок»². Синонімом дезінформації можуть виступати терміни «фейкові новини» і «політичні містифікації», хоча, окремі дослідники цілком слушно, на наш погляд, у фейкових новинах вбачають лише різновид більш широкого та нейтрального поняття «дезінформації». Так, М.О. Кіца відзначає: «Часто фейк трактують як синонім до поняття «неправдива інформація». Проте вважаємо таке тлумачення не зовсім коректним. Адже фейк передбачає *навмисне перекручення*, вигадкування, дезінформування, а неправдива інформація може бути подана у ЗМІ випадково — через халатність журналістів,

¹ Юридическая психология: терминологический словарь / сост. Бандурка А.М., Венедиктов В.С., Тимченко А.В., Христенко В.Е., Калиновский В.Б. / под ред. Бандурки А.М. Харьков : Тимченко, 2005. 432 с. *Цитується за* Лефтеров В., Третьякова Т. До проблеми психологічного тиску на учасників кримінального провадження під час проведення слідчих еспериментів та допитів. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія «Психологічні науки»*. 2019. № 3(14). С. 159-169.

² Політологія: сучасні терміни і поняття : короткий навчальний словник-довідник для студентів ВНЗ I-IV рівнів акредитації / укладач В. М. Піча ; наук. редакція Л.Д. Климаської, Я.Б. Турчин, Н. М. Хоми. Львів : Новий Світ – 2000, 2015. С.77.

неуважність, недостатню перевірку інформації. Неправдива інформація може бути спростована засобом масової інформації, у якому вона була подана, а отже, дезінформаційний вплив на аудиторію буде не таким вагомим. Тому, на нашу думку, фейк є видом неправдивої інформації, а не її ототожненням»¹. О.Звоздецька підкреслює: «зарубіжні дослідники намагаються не використовувати поняття «фейкової інформації», оскільки воно охоплює складні явища забруднення інформації, а також цей термін почали активно вживати політики у всьому світі для медіа, інформацію яких вони вважають не вигідною, і цим самим підривають свободу та довіру до ЗМІ. Тому, чітко виокремлюють такі поняття як «дезінформація» («dis-information») – це інформація, яка є неправдивою та навмисно створена для заподіяння шкоди людині, соціальній групі, організації чи країні; «помилкова інформація» («mis-information») – неправдива інформація, яка не створена з метою заподіяння шкоди та шкідлива, зловмисна інформація («mal-information») – інформація, яка базується на реальних подіях та використовується для заподіяння шкоди людині, організації чи країні. Ще однією перешкодою, яка утруднює дослідження феномену «дезінформації», є наявність чисельної термінології, яка позначає неправдиву інформацію як в роботах науковців, так і в документах ЄС, зокрема, фейки, дезінформація, пропаганда, маніпулювання інформацією, інформаційний розлад, гібридна війна...»².

Загалом, англіцизм *fake news* перекладається як «брехлива, фальшива інформація» – фальсифікована (підроблена), сфабрикована і має різні визначення. Дж.Педро Баптіста та А.Градін під фейковими новинами розуміють «різновид онлайн-дезінформації із повністю або частково брехливим змістом, умисно

¹ [Кіца М.О.](#) Фейкова інформація в українських соціальних медіа: поняття, види, вплив на аудиторію. *Наукові записки Української академії друкарства*. 2016. № 1. С. 281–287.

² Звоздецька О. Дезінформація як загроза національній безпеці Європейського Союзу: проблеми та підходи. *Історико-політичні проблеми сучасного світу*, 2021. Т. 43, С. 30–39.

створений для обману і/або маніпулювання певною аудиторією у форматі, що імітують новини чи звіт (з метою отримання довіри), яка може бути пов'язана із реальними подіями, структурована (назва, зображення, зміст) для привернення уваги читачів і переконує повірити у брехню, аби отримати більше кліків і репостів, відповідно, більш високий дохід і/або ідеологічну вигоду»¹. Визначення дає змогу виділити наступні характеристики: 1) умисність обману; 2) популярність фейкових новин, які часто звернені до страхів, тривог; інколи – скандальний контент незалежно від його правдивості. Фейкові новини прагнуть заслужити довіру і отримати визнання, імітуючи репортажі чи новини, з метою маніпулювання і обману читача, надають фейковому контенту вигляд правдивості. Опорне поняття дезінформації «брехня» у найбільш загальному вигляді полягає у спотворенні фактів і подій або у їх відкиданні, запереченні чи відкиданні фактів; повідомленні неправдивих фактів або пряме протиріччя їм; замовчування інформації, яка повинна бути доведена до відома (наприклад, замовчування фактів біографії, які можуть закріпити у свідомості населення потрібну думку).

Сучасні фейкові новини широко розповсюджуються у соціальних мережах, де відбувається гонитва за увагою, за кількістю переглядів сторінок у соціальних мережах. Мета фейкових новин – стати вірусними, а відтак, і факти приносять у жертву на вівтар вірусності. Цифровізація відкриває більше можливостей для переконливої дезінформації: монтаж, аудіовізуальні технології; цифрові можливості удосконалюють старі процеси фотографічних спецефектів і кінематографічного монтажу; підроблення зображення, звуку, наприклад, шляхом створення імітації присутності там, де потрібно. Невід'ємною складовою сучасності є й «потенціал штучного інтелекту і діп-фейків – технологія, що використовується для виготовлення реалістичних аудіо- чи відео- носіїв»².

¹ Baptista J.P., Gradim A. Understanding fake news consumption: a review. *Soc. Sci.* 2020. № 9 (10). URL: <https://doi.org/10.3390/socsci9100185> (дата звернення: 18.03.2022).

² Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States. *European Parliament* : веб-сайт. URL: bit.ly/45LjOwG (дата звернення: 16.04.2022).

Натомість, окремі автори взагалі відкидають можливість використання терміна «фейкові новини». Так, у «Посібнику із журналістської освіти» (UNESCO Series on Journalism Education), відзначено: «поняття «новини» означають достовірну інформацію у відкритому доступі, а інформація, що не відповідає цим стандартам не може бути «новинами». У цьому сенсі «фейкові новини» – це оксюморон...». У виданні випадки, пов'язані із «експлуаторським маніпулюванням мовою... особливі категорії фальшивої інформації у різноманітних формах»¹ вважають дезінформацією.

Зарубіжні дослідники цього явища вказують, що «термін не має сталого визначення і залежить від контексту... термінологія абсурдна і непотрібна, оскільки має велику кількість визначень і слугує для пропагандистських цілей»². Відзначимо, що дезінформація може бути однією із функцій пропаганди і грає особливу велику роль, наприклад, у зовнішній пропаганді, у якій об'єктом є ворог держави.

Про зв'язок дезінформації і пропаганди пишуть і вітчизняні науковці: «Створення фейку – це своєрідне мистецтво пропаганди, яке активно застосовують і боти, і тролі. Фейк за змістом може бути у чистому вигляді неправдою, але поданий і сформульований таким чином, що стає сприйнятим певними громадянами й соціальними групами. В той же час, фейк може являти собою поєднання правди з брехнею у співвідношенні необхідному маніпулятору»³ – правда наполовину, яка у літературі визнається формою пропаганди. Пропаганда та дезінформація особливо тісно переплітаються у фальсифікації історії чи її спрощені. Політичний продаж історичної пост-правди

¹ Journalism, «Fake News» & Disinformation: Handbook for Journalism Education and Training. UNESCO : веб-сайт. URL: https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf (дата звернення: 14.12.2021).

² Joshua H.-C. Stop Talking about Fake News! *PhilPapers* : веб-сайт. URL: <https://philpapers.org/rec/HABSTA> (дата звернення: 16.04.2022).

³ Війни інформаційної епохи: міждисциплінарний дискурс : монографія / за ред. В.А. Кротюка. Харків : ФОП Федорко М. Ю., 2021. С.122.

може бути обумовлено різними причинами: тут, і розрахунок на підтримку на майбутніх виборах, і штучне вигадкування внутрішніх і зовнішніх ворогів, і глобальне – відвернення пильного ока народу від соціально-економічних проблем. «Ідеологічний контроль» радянських часів змінила ідея самоцензури ЗМІ, суть її – не задаватися питаннями, які могли б привести до проблем бізнес-власників телевізійних каналів. Цінність інформації – пріоритет відкладений, важливіше – маса, яка буде залучена й політичне зміцнення становища конкретних осіб, разом з тим, дезінформацію можна визнати і окремим методом інформаційно-психологічної війни, яка характеризується повідомленням та/або розповсюдженням завжди умисно брехливої інформації. Більш широко дезінформація визначається як «публічне поширення неправдивої інформації, що не була перевірена або в результаті перевірки виявилася неправдивою та має або може мати негативні наслідки для реалізації конституційних прав громадян та/або загрожувати національній безпеці»¹. Розуміння «дезінформації» як розповсюдження завідомо неправдивої інформації і широке, і вузьке водночас. Широке, тому що може і не мати ворожих намірів, хоч і мати реальні наслідки. Поняття вузьке, оскільки, не завжди інформація брехлива – інколи вона перебільшена, чи применшена, чи подана надто емоційно. У центрі роботи дезінформації – когнітивна складова, експлуатація властивої людській природі лінії, яка відмовляється мислити критично і перевіряти отриману інформацію, з цієї точки зору, явище дезінформації – результат епістеміологічної кризи.

У січні 2019 р. єврокомісар М. Габріель спеціально наголосила, що «сформульовані на сьогодні визначення різновидів дезінформації та пропаганди все ще потребують подальшого детального аналізу». Відсутність адекватного визначення: не дозволяє ввести поняття в нормативно-правову площину; створює

¹ Фейки як інструмент впливу на вибори: аналітична доповідь / Дубов Д.В., Корецька І.О., Баровська А.В. та ін. Київ : Національний інститут стратегічних досліджень: центр безпекових досліджень. Школа політичної аналітики НАУКМА. 2020. С.18.

підстави для численних обвинувачень у порушенні свободи слова як реакція на контрдії; стає причиною нерозуміння/хибного сприйняття заходів захисту, запропонованих іншими країнами, отже, не сприяє спільному вирішенню глобальної проблеми; нівелює будь-які спроби отримання правдивих новин, адже «демонізує» традиційні новинні організації; унеможлиблює побудову та тестування нової теорії вироблення й споживання новин; не сприяє здійсненню нових продуктивних досліджень»¹.

Дезінформація може бути разовою – коли спотворення фактів пов'язане із конкретною ситуацією, людиною (наприклад, чутки) або систематичною, яка вирізняється вищим рівнем підготовки і організації для уведення в оману великих груп людей, населення однієї чи багатьох країн.

Дезінформація може вплинути на громадськість такими способами:

- 1) дезінформація за рахунок подання неправдивої інформації або проведення брехливого аналізу може змусити прийняти людей хибні рішення, які не відповідають їхнім бажанням, які вони б не прийняли, якби не були дезінформовані. Особливо це проявляється під час виборчої кампанії: проводяться «резонансні розслідування», які розкривають «темні сторони» особи політичного опонента, пропонуються спрощені рішення складних проблем;
- 2) викликає розбіжності у поглядах і залишає надто полярні, безкомпромісні точки зору;
- 3) викликає масову недовіру до інститутів ЗМІ і відмову від співпраці і захисту тих, які чесно стоять на службі громадськості і демократії;
- 4) на дезінформаційному фоні громадськість менш схильна брати участь у вирішенні важливих політичних питань, оскільки «не знає, кому вірити».

Попри, негативний відтінок дезінформація як метод інформаційно-психологічної війни, в окремих випадках може служити і корисним цілям. Так,

¹ Фейки як інструмент впливу на вибори: аналітична доповідь / Дубов Д.В., Корецька І.О., Баровська А.В. та ін. Київ : Національний інститут стратегічних досліджень: центр безпекових досліджень. Школа політичної аналітики НАУКМА. 2020. С.12.

обман ворога на війні не може засуджуватися. Інша справа – її невід’ємний специфічний вид діяльності – різні хитрощі: починаючи від переконання у тому, що війни не буде і закінчуючи відволіканням брехнею уже тоді, коли вона йде.

Найбільш поширеним методом інформаційно-психологічної війни є пропаганда: «пропаганда дійсно виступає у якості основної інформаційної зброї..., що дозволяє суб’єктам пропаганди впливати на масову свідомість населення та формування громадської думки»¹. Дослідники визначають пропаганду як: «1) розповсюдження політичних, соціологічних, філософських, науково-технічних знань, художніх та ін. ідей з метою їх впровадження в *суспільну свідомість* і активізацію масової практичної діяльності; 2) політична або ідеологічна *пропаганда* з метою формування певного світогляду людини, в т.ч. й релігійного»²; 3) «форму комунікації, спрямовану на маніпулювання свідомістю конкретно визначеного суб’єкта з метою формування у нього певних уявлень і позицій»³. Ж.З. Денисюк під пропагандою розуміє «політично мотивований інформаційно-психологічний вплив на емоційно-вольову сферу масової свідомості, за допомогою якого впроваджуються політичні ідеї, погляди, установки і формується політична поведінка. Основною психологічною метою пропаганди є вплив на систему ідейних, громадських і політичних установок людей, яку можна змінити шляхом формування нових установок або через посилення (ослаблення) вже існуючих»⁴. Доповнимо вказані дефініції і визначимо пропаганду як метод інформаційно-психологічної війни, що характеризується комплексом дій – переконання, розповсюдження ідей, думок, доктрин, ідеології та іншої інформації, що впливають на цільову аудиторію із метою примушування до певного способу поведінки та

¹ Полторак В.А., Стадник А.Г. Пропаганда та її місце в процесі ведення інформаційних війн. Основні форми пропагандистського впливу: пряма пропаганда, джінса, пабліситі, пропаганда 2.0. *Epistemological studies in Philosophy, Social and Political Sciences*, 2020. № 3 (1) С.126-138.

² Політологія: сучасні терміни і поняття : короткий навчальний словник-довідник для студентів ВНЗ I-IV рівнів акредитації / укладач В.М. Піча ; наук. редакція Л.Д. Климанської, Я.Б. Турчин, Н.М. Хоми. Львів : Новий Світ – 2000, 2015. С.330-331.

³ Шевців М.Б., Гончарук К.А. Пропаганда, як соціально-політичне явище: проблеми розуміння. *Південноукраїнський правничий часопис*. №1. 2019. С. 119-122.

⁴ Денисюк Ж.З. Пропаганда та контрпропаганда в контексті стратегій державної інформаційної політики. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління*. 2021. Том 32 (71). № 2. С.46-51.

мислення, а в окремих випадках і руху маси до дії – наприклад, до війни, слідкуючи за тим, щоб вони адаптувалися до образу дій, які треба прийняти і не висували заперечень. Пропаганда особливо помітна і широко вивчається у контексті **війни**. Під час війни учасники опиняються у стані емоційної ненависті і злість явно не сприяє можливості холодного розсуду, можливості без емоцій обдумати докази, які надані обома сторонами предметно. Політична віра потребує не лише міфів і утопій, ритуалів і символів, вона також повинна ефективно надходити у маси.

Розгорнуту типологію пропаганди пропонує в однойменній роботі Ж. Еллюль, він виділяє такі категорії: 1. Політичну (у свою чергу поділяється на стратегічну – встановлює загальну пропагандистську лінію, чергування кампаній і тактичну – прагне отримати результати у цих рамках, наприклад, брошури воєнного часу і гучномовці, аби досягнути негайної капітуляції противника) і соціологічну пропаганду, яка прагне змінити стиль життя, культури, створити новий спосіб життя, що, очевидно, досягається у відомому понятті м'якої сили або культурної дипломатії. 2. Пропаганда агітаційна та пропаганда інтеграційна, остання спрямована на стабілізацію обстановки усередині конкретного середовища. 3. Вертикальна (згори від «верхівки» до низу) та горизонтальна (реалізується усередині конкретної групи). 4. Ірраціональна, що спрямована на емоційне придушення індивіда, його почуття та емоції та раціональна (заснована на фактах)¹.

Крім того, у політичному контексті особливо актуальними є інші типології:

1. Модель пропагандистської комунікації В.О'Доннела і Г.Джоуета: «біла» пропаганда – надходить від чітко визначеного мовника; «сіра» – джерело повідомлення не може бути правильно ідентифіковане й інформація, яка надійшла є не зовсім точною; «чорна» – характеризується неправдивим джерелом повідомлення, яке приховує реального відправника і брехливою інформацією.

¹ Ellul J. Propaganda. *Monoskop.org* : веб-сайт. URL: https://monoskop.org/images/4/44/Ellul_Jacques_Propaganda_The_Formation_of_Mens_Attitudes.pdf (дата звернення: 18.04.2022).

2. За спрямуванням впливу пропаганду можна розділити на: зовнішню (зазвичай використовується під час ведення воєнних дій, спрямована на громадян інших країн) і внутрішню (направлена на громадян власної держави, так телебачення у Росії стало запорукою впровадження принципу «економії мислення» громадян).

3. За способом розповсюдження виділяють: пряму – особистий контакт відправника з отримувачем, який характеризується прямою, зворотнім зв'язком, невеликою дистанцією (наприклад, при зустрічі кандидатів із електоратом) і непряма – через ЗМІ, які стають посередниками у пропагандистському процесі.

На перший погляд, пропаганда асоціюється із нав'язуванням альтернативного світу, передбачає негативний контекст, зокрема, у соціальних науках, термін має найбільш яскраве негативне забарвлення коли він використовується для стратегії маніпулювання, яке було типовим для тоталітарних режимів, характеризується маніпулятивною інтенційністю. Однак, це розуміння є надто вузьким, оскільки пропаганда може бути й позитивною. Розповсюдження «доброго слова» у політиці має на меті вплив на цінності й не завжди негативний. Так, використане у системі охорони здоров'я «куріння убиває» – теж містить ознаки пропаганди, однак такий стан речей вважається похвальним, а у ЗУ «Про дорожній рух» до компетенції міських рад та їх виконавчих органів, районних рад та районних державних адміністрацій належить, зокрема «проведення роботи по пропаганді безпеки дорожнього руху» (ст.6). Сам факт того, що пропаганда означає будь-яку спробу вплинути на відношення чи погляди групи, ще не означає, що вона нечесна чи ірраціональна. Таким чином, позитивне розуміння пропаганди можна звести до: 1) заклику, корисного для передачі інформації; 2) частини просвіти.

Негативне ж розуміння пропаганди виражається тому що вона:

- 1) приносить не користь, а просуває інтереси пропагандиста;
- 2) є байдужою до істини, натомість спрямована на управління думками і установками шляхом маніпулювання соціальною сугестивністю;
- 3) є спробою

контролю поведінки індивідів, коли цілі, що переслідуються є ненауковими, недоведеними, неаргументованими, і загалом, мають сумнівну цінність; 4) є засобом узурпації влади шляхом психологічного маніпулювання групами чи масами людей.

Пропаганда завжди спрямована на переконання – мета пропаганди не лише вплив на масову аудиторію чи згода слухача, її мета більш практична – реалізація певного плану дій, активна дія, тобто прийняття певного курсу, який дозволяє активно співпрацювати у конкретному напрямі політики. Пропаганда вважається переконливим типом діалогу, хоча й часто помилковим за своєю суттю. Крім того, метою пропаганди може бути примушування аудиторії підтримувати цілі, інтереси і політику певної групи шляхом отримування згоди громадськості на майбутні дії, або більше – посіяти страх, недовіру, тривогу, розділити суспільство, створити ситуацію, де громадяни не знають, кому вірити. Тому, роль пропагандиста полягає не лише у тому, щоб переконати чи «перевиховати» громадськість, щоб змінити свої переконання, отримати згоду громадськості з тим, щоб вони потім діяли на основі нової точки зору, яку вони за посередництва пропаганди прийняли. Вона може мати еристичну форму або вигляд перемовин. В окремих випадках, пропаганда має аргументативну структуру, схожу за своєю структурою на сварку, діалог еристичного типу. Частими для пропаганди є слова «боротьба» та «битва». Передбачається, що будь-які засоби, необхідні для боротьби із злом, небезпекою чи «ворогом» виправдані. Еристика – це емоційний гнівний обмін, іскристий, але нелогічний. Він часто опирається на просування своїх інтересів, а не орієнтується на істину по обговорюваному питанню, використовується для посилення «сенсації», щоб викликати тривогу. Думка про те, що українські «нацики» здатні зруйнувати життя у Росії абсурдна, але коли вона правильно сформульована – напівкрикливо і безапеляційно, широко розповсюджена через ЗМІ і соціальні мережі, не відкинута у зрозумілій і доступній для мас формі, вона приймається і у неї вірять.

Г.Г. Почепцов до рис пропаганди відносить: масове охоплення, обов'язковість, повторюваність у часі і просторі, блокування альтернативної інформації, розповсюдження того ж в інших модусах (література, кіно, тощо)»¹.

До основних ознак пропаганди як методу інформаційно-психологічної війни можемо віднести:

1. Односторонність аргументів. Пропаганда – це умовна адвокація чи адвокаційний діалог. Використання «переконливих» аргументів для підтримки тільки однієї сторони теми і представлення аргументів на користь цієї позиції. Пропаганда – це не спроба раціонально обдумати правильність тези із розбором альтернатив із їх подальшим розумним і справедливим порівнянням. Проблема посилюється й тим, що люди схильні шукати інформацію, яка співпадає із їх власною точкою зору навіть попри те, що лунають «раціональні» голоси, які суперечать пропагандистському дискурсові.

Інформаційне, раціональне, рефлексивне судження чи логічне мислення не завжди відкидаються, однак, якщо ці способи не спрацюють пропаганда застосує інші – містифікації, «зручні вимисли», казки, символи, групову лояльність, ентузіазм публіки, візуальні образи і будь-які методи переконання які є психологічно ефективними. Освіту теж не можна вважати нейтральною, особливо на фоні того, що пропаганда може просочуватися крізь шкільну програму і вкладатися із раннього віку. Еволюція повідомлень, що передаються підручниками з історії, як правило, точно оформлені програмними директивами, відповідальність за які, зрештою, несе міністерство, представники якого із трибуни будуть говорити про неутручання державної ідеології, однак, у реальності – контрасту між викладанням дисциплін і пропагандою не повинно бути, аби це не призвело до незалежного мислення. У таких умовах не лише дисципліни історичного циклу

¹ Почепцов Г.Г. Пропаганда: основные характеристики. *ДМ media sapiens*: веб-сайт. URL: <https://ms.detector.media/mediaanalitika/post/20334/2018-01-07-propaganda-osnovnye-kharakterystyky/> (дата звернення: 04.03.2023).

трансформуються, але і педагогічні методи загалом. У довгостроковій перспективі управління пам'яттю грає ключову роль у формуванні психіки, переконань, схильності притримуватися певних поглядів. Крім того, освітня система покликана навчити осмислювати інформацію, із якою людина стикатиметься щодня.

2. Виправдання результатами. Пропаганда виправдовується потенційною цінністю отримання результату, завжди є необхідною для «благих намірів», таких як громадська безпека, адже, в окремих випадках умілі пропагандисти вказують громадянам, кого їм варто боятися. І пропагандистський дискурс будується крізь призму існування ворога, протиставлення «ми – вони». Створення образу ворога, який може посягнути на встановлені загальнолюдські цінності і потреби – релігійні, особиста і національна безпека, працевлаштування, економічна стабільність etc. На цьому фоні люди особливо схильні підтримувати того, хто цей світ цінностей і потреб захищає. Однак, такий ухил є особливо небезпечним для демократії, оскільки при постійному повторенні наративів про ворогів і неухильної віри у них, складається ситуація, де більша частина населення починає підтримувати політичних діячів із авторитарними цілями, а відтак, готові на жертву власними свободами – задля того, аби захистити загальнолюдські цінності від часто уявного, створеного пропагандою ворога, маси готові жертвувати навіть загальнолюдськими правами. Позиція політичної еліти у цьому контексті зосереджена не на побудові демократії, а навпаки – концентрації влади у своїх руках, та відновленні політичного трайбалізму, який «є суттєвою загрозою для демократичних перетворень та передумовою гібридизації політичного режиму та зворотного руху трансформаційних процесів у бік авторитаризму»¹.

3. Байдужість до логічних роздумів і доказової бази. Мета пропаганди – рух масової аудиторії у певному спрямуванні і у питанні використанні логічних

¹ Краснопольська Т.М. Політичний трайбалізм: прояви на пострадянському просторі та загрози для України. *Правові та інституційні механізми забезпечення розвитку України в умовах європейської інтеграції* : матеріали Міжнародної науково-практичної конференції, м. Одеса, 18 травня 2018 р. Одеса : Видавничий дім «Гельветика», 2018. С. 216-220.

роздумів і відповідних доказів вона нейтральна. Пропаганда відбирає факти, які вона надає аудиторії. «Відбір» фактів є однією із найбільш розповсюджених стратегій пропаганди. Так, підсумки одного бою мають пропагандистське значення для одного із противників, тоді як результат другого бою має значення для іншої сторони конфлікту. І обидві сторони говорять правду у своїх пропагандистських звітах. Недолік полягає у вибірковості: обидві сторони дають частковий звіт. І цей аспект також суперечить цілям раціонального обговорення, заснованого на повноцінній оцінці фактів. Висновок полягає у тому, що така пропаганда ірраціональна чи нечесна у тому плані, що вона протиставляється раціональному, обґрунтованому і критичному обговоренню теми.

У цьому контексті, важливо підкреслити, що думку людей можна змінити і повідомивши факт повністю, так, цифри померлих ворогів на війні можуть слугувати пропагандистським цілям довіряти власним збройним силам і викликати тривогу на стороні ворога. Це чесний спосіб впливу пропаганди через подання нової і достовірної інформації. У таких випадках, пропаганда є твердженням, яке одночасно вірне й інформативне для населення. Такі дії не є нечесними чи такими, що суперечать цілям раціонального обговорення, тому що відбувається інформування громадськості про правдивий факт, попри те, що він має пропагандистське значення.

4. Емоційна мова і переконливі визначення. Невід’ємна частина будь-якого прикладу пропаганди – це використання емоційно заряджених слів і фраз, які роблять точку зору стверджувальною, настільки, що вони набувають «правдивих» рис і будь-яка протилежна точка зору має суцільне негативне забарвлення. Так, «борцям за свободу» протиставляються – «терористи». Фрази приниження можуть використовуватися для позначення протилежної точки зору. Ефективна пропаганда робить заклики до патріотизму і так званого «здорового глузду», хоча, звертається більше до емоцій. У цьому контексті вона – частина психологічного насильства, оскільки апелює до елементарних почуттів ненависті, страхів, які приховані у

безсвідомому, вивільнює стереотипи, а в окремих випадках є попередником фізичного насильства.

5. «Квазіодноголосся». За своєю природою, пропаганда виключає протиріччя і дискусію: переговорний тип може мати місце, однак, немає нічого спільного із пошуком істинності чи раціональністю. Пропаганда досягає своєї мети тоді, коли сили, що намагаються її побороти затихають або залишаються у меншості, а в ідеалі – противник повинен бути інтегрований у неї. Її завдання – створення відчуття ізоляції для тих, хто ще не долучився до більшості. Вона грає на почуттях колективності, бажанні будь-якого індивіда бути складовою своєї суспільної групи.

6. Створення накопичувального повідомлення у ЗМІ. Попри мінливий медійний ландшафт, пропаганда повинна бути тривалою і безперервною, без прогалин заповнювати все життя індивідуума, створювати йому альтернативну реальність, де він повинен функціонувати без зовнішніх орієнтирів: так, кіно – кращий засіб для пропаганди з точки зору соціального клімату, повільного, але впевненого проникнення; особисті зустрічі і плакати носять елементи шокової пропаганди, інтенсивної, направленої на прийняття швидких рішень і дій; преса формує спільність поглядів etc. Тому як тільки враження від одного наративу починає йти на спад, йому на зміну у наступальному порядку приходять інші. Інколи раптові і навіть непослідовні пропагандистські повороти, коли сьогодні заперечується те, що ще вчора було головною темою насправді спрямовані на безперервність пропаганди: пропагандистська машина не перестає рухатися «на різких поворотах», аби утримати увагу у потрібному пропагандистові контексті і відповідно контролювати здатність індивіда до супротиву. Переоцінюючи нові сили жертва пропаганди знаходить їм виправдання і докази на їх користь.

Причини успішної роботи пропаганди полягають, перш за все, у привласненні демократичних інститутів. По-друге, кризі політичної комунікації, появі нових гравців і каналів, на кшталт блогосфери із пропагандистськими напрямками. По-

третє, кризі преси, а точніше її стандартів, наприклад, розвиток соціальних мереж дав можливість розповсюджувати неперевірену інформацію.

Аналізуючи відношення між рекламою і пропагандою можна підкреслити їх семантичну двосенсність. Рекламу в окремих випадках теж можна вважати методом політичної комунікації, де важливе значення має візуальна складова і звук, орієнтований на переконання. І пропаганда, і реклама розміщуються у контексті соціальної комунікації, вони розділяють за змістом ідеологічну площину, громадський і колективний реципієнт, цілі переконливого характеру, риторико-аргументовану систему, лінгвістичні стратегії. Реклама може слугувати популяризації продукту, бренду чи заходу. Як і пропаганда, вона покликана не правдиво інформувати громадськість, а впливати на неї, привертати увагу більше шляхом використання образів чи коротких повідомлень.

Реклама має менш негативний смисловий відтінок, попри те, що як і пропаганда спрямована на переконання аудиторії психологічними методами. У контексті політичної реклами вони можуть бути синонімами.

Сьогодні у боротьбі за сфери політичного впливу акцент із застосування фізичної сили усе більше зміщується на сторону прихованих й гнучких форм агресії, у числі яких – інформаційні війни. Інформаційно-психологічна війна виходить з ідеї, що контролюючи отриману інформацію, можна зменшити здатність людини думати самостійно. Можливо заволодіти розумом окремих людей, груп і навіть суспільства в цілому. Це зводиться до використання нових методів захоплення влади м'яко, без насильства, без державного перевороту, війни, просто шляхом інформаційно-психологічної війни. А.Кройтор з цього приводу відзначає: «М'які інформаційні технології сьогодення акцентують увагу на формування необхідного інформаційного порядку денного, відбираючи потрібні повідомлення та приховуючи події, що можуть негативно вплинути на кінцеву мету інформаційного потоку. Особливістю інформаційних посилок у різних ЗМІ сьогодні є відсутність прямого висловлювання, або чіткої оцінки певній політичній

події, явищу або особі. Проте інформація подається з прихованим підтекстом, що виділяє окремі елементи повідомлення, або ж приховуються певні обставини, зокрема причини, що зумовили окремі політичні явища»¹.

Цікавим у політичному контексті видається і співвідношення інформаційно-психологічної війни та «м'якої сили». Г.Г. Почепцов відзначає: «Відголоском пропаганди можна вважати і сьогодишню м'яку силу, адже по суті це також інформаційна чи віртуальна інтервенція із однієї цивілізації в іншу»², а О.В.Литвиненко вважає інформаційну війну «найяскравішим прикладом «м'якої сили»³. М'яка сила у політиці – різнопланове поняття, яке показує державу із точки зору високих політичних цінностей, культури привабливою для інших, а її зовнішню політику не лише законною, але і високоморальною. Джозеф Най у роботі «Soft Power» визначив м'яку силу як «здатність отримати бажані результати у відношеннях із іншими державами за рахунок привабливості власної культури, цінностей і зовнішньої політики, а не примусу чи фінансових ресурсів»⁴, але, різного роду маніпулятивні впливи на кшталт пропаганди, дезінформації, які є методами інформаційно-психологічної війни навряд чи можна вважати «яскравими прикладами» високих політичних цінностей.

У рамках підходу політичного реалізму м'яку силу ототожнюють з пропагандою (хоча Дж.Най їх тотожність відкидає) за такого підходу, «м'яку силу» можна вважати методом інформаційно-психологічної війни, однак, на наш погляд, вона, за аналогією із дезінформацією і fake news є формою пропаганди.

Тотожним «м'якій силі» можна вважати поняття «культурної дипломатії». Н.Ф. Сербіна, О.П. Кучмій визначають культурну дипломатію як «наукову

¹ Кройтор А.В. Технології маніпуляції у конструюванні інформаційного порядку денного. *Актуальні проблеми політики* : зб. наук. пр. 2018. Вип. 62. С. 36-43.

² Почепцов Г.Г. Пропаганда: основные характеристики. *ДМ media sapiens*: веб-сайт. URL: <https://ms.detector.media/mediaanalitika/post/20334/2018-01-07-propaganda-osnovnye-kharakterystiky/> (дата звернення: 04.03.2023).

³ Литвиненко О.В. Інформаційні впливи та операції: теоретико-аналітичні нариси : монографія. Київ: НІСД, 2003. С.30.

⁴ Nye J.S. Soft Power. *Foreign Policy*. 1990. № 80. P. 153–171. URL: www.jstor.org/stable/1148580 (дата звернення: 16.11.2021).

субстанцію та як реальність політики міжкультурного співробітництва, має національну специфіку і технології здійснення, використовується як інструмент міжурядового співробітництва або «м'якого впливу» задля забезпечення національних інтересів на глобальному, регіональному і національному рівнях»¹. Г. Луцишин, А. Гончарук зазначають: «практика показує, що для багатьох сучасних держав культурна дипломатія належать до першочергових справ, зокрема, особливо важливим напрямом зовнішньої політики залишається для сучасних європейських держав... Окремими напрямом розвитку культурної дипломатії є вивчення та поширення державної мови... підтримка молоді альтернативної музики... розвиток альтернативних пошуків і нових тенденцій у мистецтві...»². Перелік ключових інструментів культурної дипломатії доповнюють Т.Р.Браніцька, Н.В.Кашченко, І.Г. Кухар: «програми освітніх обмінів (для вчених, науковців, аспірантів та студентів); організація внутрішнього та зовнішнього туризму; програми відвідування країни іноземними послами; забезпечення широкого спектра мовлення (радіо, телебачення, мережа Інтернет) для закордонних аудиторій; популяризація та поширення національної кухні в Європі та світі; створення легкого доступу іноземним громадянам до інформації про історію, звичаї та традиції України; висвітлення України як держави високих спортивних та культурних досягнень...»³.

На перший погляд, ця частина зовнішньої політики здається віддаленою від пропагандистської діяльності. Однак, це не так, і з огляду на історичний аспект: у 1930-х рр. у різних країнах, наприклад, Великобританії використовувався термін «культурна пропаганда», і з огляду на ціль, яка так чи інакше дотична до цілей

¹ Сербіна Н.Ф., Кучмій О.П. Культурна дипломатія як інструмент зовнішньої політики сучасної європейської держави. *Актуальні проблеми міжнародних відносин*. 2011. Вип. 100(1). С. 122-131.

² Луцишин Г., Гончарук А. Особливості розвитку культурної дипломатії України в сучасних умовах. *Academic Journals and Conferences* : веб-сайт. URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2017/nov/6654/lucishin.pdf> (дата звернення: 14.03.2022).

³ Браніцька Т.Р., Кашченко Н.В., Кухар І.Г. Культурна дипломатія як спосіб комунікації в інтересах національної безпеки України. *МАУП* : веб-сайт. URL: <https://maup.com.ua/assets/files/expert/16/13.pdf> (дата звернення: 14.03.2022).

пропаганди – охоплення конкретної аудиторії з метою впливу на її поведінку. В окремих випадках «культурна дипломатія» (а, відтак і м'яка сила) має всі ознаки інформаційно-психологічної війни. Так, ґрунтуючись на загальній ідентичності, похвалі і звеличенні особливо символічних цінностей, таких як «батьківщина», «релігія», «традиція», «історія», пропагандисти, творять нову уяву, міжнародний сценарій, що висловлюється наприклад, у тезах: «Росія справжня спадкоємиця Київської Русі».

Багата термінологія, що об'єднала всі варіанти маніпулятивної політичної комунікації утруднює проведення розмежування між «пропагандою», «дезінформацією», «переконанням». Плутанина, часто зводить все до однієї лише пропаганди. Однак, з огляду на визначені нами особливості пропаганди, вона ніколи не зобов'язана випадковості – це результат скоординованої реалізації заздалегідь продуманої стратегії. Під час війни чи революції вона може набувати форми «агітаційної пропаганди», яка спрямована на провокування дії. На стику дезінформації і пропаганди існує ще один, давно відомий метод, який, на наш погляд, відповідає розумінню інформаційно-психологічної війни – теорії змови (конспірологічні теорії), що характеризуються епістеміологічною кризою із її відмовою від критеріїв доказовості, послідовності і встановлення фактів, невірним тлумаченням, спрощенням: «відсутність чітких наукових знань або щонайменше раціональних суджень стосовно суб'єктів та об'єктів політичної маніпуляції на глобальному, національному, регіональному та локальному рівнях сучасної політики породжує конспірологічні теорії, які своєю чергою стають надбанням громадськості і додатковим чинником дестабілізації політичної ситуації»¹. Крім того, часто у теоріях змов фігурує «всесильний елемент» і «таємні стратегії». Є. Джиджора під теорією змови розуміє «модель маніпулятивної комунікації, покликаної заперечити сформований погляд на певне явище, процес або постать, а

¹ Мошак Д.С. Сучасні політичні маніпуляції: політико-комунікаційний та політико-технологічний виміри. *Науковий журнал «Політикус»*. Випуск 4, 2020. С.42-46.

відтак — викрити «брехню» та «відкрити очі» начебто обдуреним людям. На перший погляд, теорія змови передбачає ускладнення процесу сприйняття дійсності, адже тут ідеться про пошук прихованих кричущих фактів, зацікавлених осіб, таємничих стосунків, підступних намірів тощо»¹.

На наш погляд, не зовсім вдалим видається саме вживання терміна «теорія змови». Адже, за словами К.Поппера «теорія – інструмент, перевірка якого здійснюється шляхом його застосування і про придатність якого можна судити за результатами такого застосування...»². Теорія – це не просто ідея, а висновки або їх сукупність, які виведені шляхом ретельного аналізу фактів, між тим, щодо теорії змови це просто неможливо, оскільки це судження без фактів: в основі конспірології – прихована сторона реальності, це невидимий світ секретних операцій із зловіщою таємною спільнотою, тому, конспіраціонізм – це, швидше, соціальна гіпотеза.

У роботі «Чому конспірологічна пропаганда успішна і що з цим робити», автори виокремили декілька найбільш розповсюджених у вітчизняній політичній площині конспірологічних тез: «Україна перебуває під прихованим зовнішнім управлінням «західних» кураторів, «Україною керують соросята», «Сорос та МВФ хочуть розграбувати українські землі», «США створили в Україні мережу біолабораторій для проведення експериментів на людях»³. Такі твердження дозволяють знімати відповідальність, яка перекладається на «зовнішнє управління», їх активне просування лідерами думок дають змогу широкому загалу засумніватися у встановленому політичному ладі, політиці держави, у цьому сенсі вони можуть слугувати засобом супротиву; крім того, «конспірологія веде

¹ Джиджора Є. Теорія змови як пропагандистська модель комунікації (як вишки 5G пов'язані з коронавірусом та «вакцинами Білла Гейтса»). *Діалог: медіа-студії*. 2020. № 26. С.37-51.

² Popper Karl R. The logic of scientific discovery basic books / пер. с англ. В.Н.Брюшинкина (предисловия гл. I, II, V, VI, VII) и А.Л. Никифорова (гл. III, IV, X). London, 1980. P.144.

³ Чому конспірологічна пропаганда успішна і що з цим робити: вразливість аудиторії та спротив антизахідній, прокремлівській дезінформації в Україні / П.Померанцев та ін. *Arenaresearch.org* : веб-сайт. URL: <https://arenaresearch.org/wp-content/uploads/2021/06pdf>. (дата звернення: 18.04.2022).

людей до висновку про безглуздість їхньої політичної активності оскільки в політиці все вирішують учасники таємної змови, а громадяни – всього лише маріонетки в чийхось руках...»¹. У спеціальному дослідженні Н.С. Ярош, В.В. Артюхова зазначають, що «до соціально-політичних умов наслідування теорії змов належить ситуація аномії, що характеризується відсутністю довіри між індивідами та органами влади»².

Однак, інколи конспірологічні наративи можуть впливати і на здоров'я нації. Так, під час пандемії Covid-19 активно велася інформаційно-психологічна війна з метою викликати страх, несприйняття і отримання переваги у розробці вакцини. Окрім, посилення «теорії змов»: поява вакцини супроводжувалася тим фактом, що провідні організації охорони здоров'я, такі як Фонд Білла Гейтса чи ВООЗ будуть причетні до її виробництва чи розповсюдження, тож конспірологічний матеріал твердо доповнився тезами, що окремі особи не лише створили вірус, але й планують на ньому добре заробити.

Не менш небезпечною була й ідея «Великого перезавантаження/обнуління» та думки експертів на кшталт Люка Монтан'є породила теорію змови QAnon, яка стверджує, що глобальні фінансові еліти і світові лідери навмисно спланували пандемію, штучно вивели коронавірус в лабораторії, щоб створити умови, які дозволять реструктурувати уряди світу. Прихильники теорії змови особливу увагу приділяють концепції «Великого перезавантаження», стверджуючи, що головною метою цього перезавантаження є глобальний політичний і економічний контроль шляхом встановлення тоталітарного режиму і, як наслідок, Нового світового порядку»³.

¹ Курілло В.Є. Латентна політика : навчальний посібник, 2-е вид., перероб. і доп. Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2017. С.67.

² Ярош Н.С., Артюхова В.В. Теоретична модель поведінкових наслідків віри у теорії змови. *Вісник Харківського національного університету імені В.Н.Каразіна. Серія «Психологія»*. 2021. Випуск 70. С.78-85.

³ Морозов А.Ю. Футурологічні та конспірологічні виміри ковід-епідемії. *Суспільно-політичні процеси в умовах пандемії: особливості та виклики* : тези доповідей Всеукр. наук.-практ. конф., м. Київ, 16 квітня 2021 р. Київ, 2021. С.70-73.

Лише на перший погляд конспірологічні теорії мають комічне забарвлення, їх реальні наслідки – трагічні. Так, духовний лідер Ірану аятолла Алі Хаменеї 22 березня 2020 р. заявив у зверненні до нації, що Covid-19 є біологічною зброєю американців і різко відкинув пропозицію США про допомогу зі словами: «Ніхто вам не вірить»¹. Неурядова організація «Лікарі без кордонів» змушені були покинути Іран, оскільки в очах тамтешнього керівництва вони ніхто інші, як «західні шпигуни». У січні 2021 р. він також заборонив увіз вакцини із США і Великобританії². Деякі іранці, очевидно, заплатили життям за такі рішення.

Не менш небезпечними були чутки щодо методів лікування Covid-19, особливо популярним було «лікування» гідроксихлорохином – протималярійним препаратом. Прикрим, на наш погляд, є й те, що появі таких заголовків сприяла підтримка подібних методів першими особами передових держав. Наприклад, такі методи лікування неодноразово і публічно підтримував колишній Президент Америки Дональд Трамп. 21 березня 2020 р. у своєму Twitter із аудиторією у 84 млн. осіб, політик написав, що гідроксихлорохин, якщо його приймати із антибіотиком азитромицином, може стати «одним із найважливіших факторів, здатних змінити правила гри в історії медицини», і що його варто «негайно використати». На наш погляд, під час ситуації високої тривожності і низької впевненості, якою є пандемія, авторитетним особам, віральність повідомлень яких у соціальних мережах є доволі високою варто радити своїм підписникам використовувати ефективні і науково доведені методи лікування, забезпечувати їх інформацією спеціалістів у галузі охорони здоров'я.

¹ Supreme Leader: US officials are charlatans and terrorists. *Islamic republic news agency* : веб-сайт. URL: <https://en.irna.ir/news/83723720/Supreme-Leader-US-officials-are-charlatans-and-terrorists> (дата звернення: 08.02.2021).

² Прищепа Я. Іран заборонив імпортувати американської та британської вакцини. *Суспільне*|| *Новини* : веб-сайт. URL: <https://suspilne.media/94450-iran-zaboroniv-import-amerikanskoi-ta-britanskoi-vakcini/> (дата звернення: 08.02.2021).

2.3. Інформаційно-технічна війна: теоретичні засади.

Набагато більшу складність викликає розуміння «інформаційно-технічної війни» («кібервійни»). Перспектива глобальних «кібервійн» – «віртуальний соціум повинен бути готовий до організованих політичних акцій та запобігання реальній загрозі виникнення «кібервійни»¹ – відкрила нові сценарії загроз, які тепер існують паралельно із можливістю ядерного знищення людства: за цією логікою є загроза знищення цивілізації через руйнування критичної інфраструктури.

Ідейне поле у цьому контексті можна умовно розділити на два табори: 1) кібервійна існує; 2) кібервійна – це певна умовність, так, у Таллінському мануалі, яке присвячене цьому явищю, робиться уточнення, що «кібервійна» вживається у чисто описовому, а не нормативному сенсі², а те, що Таллінський мануал є академічним, а не міжнародно-правовим актом, дозволяє дійти висновку, що «кібервійна» поки що не стала війною у розумінні міжнародного права, а є природнім становищем інформаційного суспільства, що можна охарактеризувати тезою Т.Гоббса «боротьба всіх проти всіх».

Небезпечної «мілітаризації» кіберпростору, на наш погляд, ще не досягнуто, а часте використання терміна «кібервійна» для позначення всіх політично-мотивованих кібератак видається дещо перебільшеним, хоча, кожен такий випадок безсумнівно вказує на вразливість життя суспільства у цифрову епоху. Крім того, складно не погодитися із Ю.В.Завгородньою, яка підкреслює, що «кіберпротиборство є невід’ємною складовою цифровізованого розвитку суспільства»³.

¹ Прохоренко А.М. Концепт інноваційних політичних технологій та особливості впровадження їх в Україні: дис...докт.філософії : 052. Одеса, 2021. С.165.

² Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. 2017. P.18.

³ Завгородня Ю. В. Захист прав суб’єктів політики в умовах кіберпротиборства. *Права людини в період збройних конфліктів : Зб. матеріалів Міжнародної науково-практичної конференції присвяч. 25-річчю Національного університету «Одеська юридична академія»* (м. Одеса, 18 листопада 2022 р.) / Нац. ун-т «Одеська юридична академія» ; каф. міжнародного та європейського права НУ «ОЮА» : у 2 т. Одеса, 2022. С. 531-534.

Дефінітивний апарат концепції інформаційно-технічної війни можна звести до таких основних ідей.

По-перше, це війна між суверенними державами, яка ведеться за допомогою кіберзброї (не кінетично). Так, О.О. Мережко кібервійною вважає «використання Інтернету і пов'язаних з ним технологічних та інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній, інформаційній безпеці та суверенітету іншої держави»¹. Підтримку такий підхід знайшов у роботах Р.В.Бараненко, А.Ю.Задорожної², С.О.Чернишенка³.

По-друге, широке розповсюдження кіберзлочинності і кібершпигування, яке потенційно може перетворитися на повноцінну війну у будь-який момент, «надзвичайне становище», яке стає новим «нормальним» розмиває межі поняття «кібервійни». Кібервійна як становище у кіберпросторі тісно межує із кіберзлочинністю, кібершпигуванням, є доволі балансуєчим поняттям, із нечіткими межами – дещо відмінне від двох названих явищ, і об'єднувальне водночас. Справді, розділити кіберзлочинність і кібервійну вкрай важко: акти кіберзлочинності є діями окремих осіб, а кібервійна – залучає держави, які є або спонсорами або об'єктом нападу. Термін «кібервійна» неоднорідний і не піддається легкому розумінню з огляду на існуюче правове регулювання.

По-третє, кібервійна може бути частиною збройного конфлікту, як міжнародного, так і внутрішнього. Частіше акт, який називають кібервійною, не відповідає повною мірою розумінню війни, яка протипоставляється «миру», а є чимось серединним. Дж.Лукас описує кібервійну як «постійну, «безкінечну» війну

¹ Мережко А.А. Конвенция о запрещении использования кибервойны в глобальной информационной сети информационных и вычислительных ресурсов (Интернете). *Політичний менеджмент. Політик* : веб-сайт.URL: <http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57>. (дата звернення: 21.04.2022).

² Бараненко Р.В., Задорожна А.Ю. Кібервійна як новий вид протистояння держав. *Південноукраїнський правничий часопис*. 2017. №1. С.53-56.

³ Чернышенко С.А. Кибервойна: теория и практика. *Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія»*. Серія: Політологія. 2015. Вип.248. С.37-41.

– війну без правил, «війну всіх проти всіх»... розмиваючи «просту» злочинну діяльність, це такий стан війни, який все важче відрізнити від миру»¹. К.Ашраф відзначає: «загальноприйнятого визначення кібервійни не існує. Існує багато часто суперечливих визначень, починаючи з неіснування кібервійни і закінчуючи кібервійною як екзистенційною загрозою... неоднозначність визначень затрудняє послідовне обговорення кібервійн, обмежує теоретичні уявлення і нівелює зусилля із розробки політики. Дійсно, Хьюз і Коларик виявили, що із 159 статей про кібервійну 103 (65 %) не містять чіткого визначення кібервійни»².

Двоїста природа технологій, що з одного боку зближують і об'єднують світ, а з іншого – мають потенціал воєнного застосування і держави, які переважатимуть в інноваціях, відповідно, отримують стратегічні переваги. Загроза, що створена кібервоїнами робить цю війну триваючою і у мирний час.

Під інформаційно-технічною війною ми розуміємо будь-який тип інформаційного впливу із застосуванням інформаційної зброї, метою якого є вплив на функціонування інформаційної системи шляхом незаконного доступу до інформаційної системи, здолання системи захисту, обмеження доступу законних користувачів з можливістю подальшого несанкціонованого збору, копіювання, перехоплення, блокування або видалення інформації.

Об'єктом інформаційно-технічної війни є інформаційно-технологічна система, суб'єктом – кібервоїн (хакер), який прагне задовольнити своє его або отримати фінансову винагороду; отримати визнання в очах своїх колег, задовольнити цікавість; для нього участь в інформаційно-технічній війні може виступати і як перевірка власного інтелекту, і як виклик державам; або ж, навпаки, це може бути виконання конкретного замовлення окремих компаній, переслідуючи

1

Lucas G. [Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare](https://philpapers.org/rec/LUCEAC-2). *PhilPapers* : веб-сайт. URL: <https://philpapers.org/rec/LUCEAC-2> (дата звернення: 21.04.2022).

² Ashraf C. Defining cyberwar: towards a definitional framework. *Defense&Security Analysis*. 2021. Volume 37, issue 3. URL: <https://www.tandfonline.com/doi/full/10.1080/14751798.2021.1959141> (дата звернення: 01.03.2023).

мету грошового прибутку, чи іноземних держав, для досягнення ними конкурентної переваги (наприклад, економічної) тощо.

До особливостей її ведення можна віднести економію ресурсів і фінансів – на відміну від розробок збройних технологій, інформаційні технології не вимагають значних фінансових ресурсів. Комп'ютер, доступ до Інтернету, експертиза інформаційних систем і доступ до важливих мереж можуть бути єдиним «озброєнням»; проблему тактичного попередження і оцінки атак; розмиті кордони – значення географічних меж нівелюється під впливом зростання ролі інформаційної інфраструктури, протиборство відбувається у віртуальному просторі – кіберпросторі.

Кіберпростір – єдиний створений людиною простір, який вона сама і може змінити. Його використання у контексті інформаційно-технічної війни характеризується: 1) анонімністю; 2) атакою «звідусіль» і швидко, тому що він виходить за географічні межі і фізичне місцезнаходження; 3) власною метрикою, яка вимірює його ефективність; 4) додатковою вразливістю для національної безпеки; 5) здатністю підірвати традиційне розуміння міжнародних відносин, силовій політики і засадничі політичні концепції; 6) неефективністю механізму відповідальності за протиправні дії. У ст.1 ЗУ «Про основні засади забезпечення кібербезпеки», кіберпростір визначається як «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних».

Від інформаційно-технічної війни слід відрізнити явище інформаційного тероризму (кібертероризму). Ми не будемо вдаватися у детальну проблематику розуміння «тероризму», відмітимо, лише що у сама його концепція є дуже складною: «ще у 80-х роках XIX ст. А. Шмідт склав список із 109 визначень тероризму з метою узагальнити цей матеріал і вивести загальноприйняте

визначення тероризму. Зусилля вченого виявилися марними, тому що після нього ще багато дослідників намагалися зробити те саме, але безуспішно, нові визначення призводили до ще більшої плутанини... Тероризм – це соціальне явище, яке виникає і загострюється на ґрунті соціальної, правової, політичної та економічної нестабільності в державі з метою досягнення певних змін (виконання поставлених вимог) на користь злочинців, шляхом застосування чи погрози застосування насильства, яке проявляється у застосуванні зброї, вчиненні вибухів, підпалів, та інших загально небезпечних дій певною особою чи організованою групою осіб»¹. М.А.Польовий підкреслює: «головною сутнісною рисою добре відомого сучасного міжнародного тероризму є залякування населення певної країни (країн) з метою здійснення певного впливу на політичну владу»².

Р.О. Гриник та В.М.Пилипенко, вказують: «що стосується природи кібертероризму, то він якісно відрізняється від загальноприйнятого поняття тероризму, зберігаючи лише стержень цього явища і ознаки»³, натомість, М.М.Вегеша відносить його до терористичних актів, вбачаючи у кібертероризмі «напади на комп'ютерні мережі»⁴.

Визначення природи кібертероризму – питання досі дискусійне, остаточної констатації – чи це один із актів тероризму, як це визначено на законодавчому рівні – відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», кібертероризм являє собою терористичну діяльність, що здійснюється у кіберпросторі або з його використанням, чи абсолютно нове явище досі немає.

Л.І.Кормич, А.І.Кормич відзначають: «Кібертероризм виглядає найтехнологічнішим і не пов'язаним безпосередньо із загибеллю людей. Проте

¹ Біленчук П.Д., Кофанов А.В., Кобилянський О.Л. Міжнародний тероризм: консолідований аналіз забезпечення безпеки. Київ : ННІПС КНУВС, 2009, С.13-14.

² Польовий М.А. Формування глобального громадянського суспільства як чинник розвитку терористичної активності в глобалізованому світі. *Актуальні проблеми політики*. Одеса : Фенікс, 2015. Вип. 56. С.122-129.

³ Гриник Р.О., Пилипенко В.М. Кібертероризм як нова форма міжнародного тероризму. *Актуальні задачі та досягнення в галузі кібербезпеки* : матеріали Всеукр. наук.-практ. конф., м.Кропивницький, 23-25 листопада 2016 р. Кропивницький, 2016. С.61-62.

⁴ Політологія : підручник / за ред. М.М. Вегеша. Київ : Знання, 2008. С.346.

втручання в роботу електронних систем управління за допомогою хакерства і створення комп'ютерних вірусів може обумовити надзвичайно небезпечні ситуації і привести до непередбачуваних наслідків. Такі дії здатні руйнувати фінансові системи, системи військового управління, управління екологічними об'єктами тощо»¹.

Як й інформаційно-технічна війна, кібертеракт не має державних меж, кібертерорист може рівною мірою створити загрозу інформаційним системам, розташованим у будь-якій точці земної кулі. Кібертероризм – це розвиток терористичних можливостей, які забезпечуються новими технологіями, реалізуються у кіберпросторі, це своєрідна «терористична декаль» у віртуальне середовище. Сьогодні не складно говорити про інформаційно-технічну атаку, яка наносить істотну шкоду і впливає на критично важливу інфраструктуру, однак, ми вважаємо, що можна висувати лише теорію кібертероризму, оскільки, досі немає реального прикладу терористичних дій у кіберпросторі, який би підтвердив гіпотезу його існування, а пояснення на кшталт «сучасний інформаційний тероризм можна охарактеризувати як множину інформаційних війн та спецоперацій, пов'язаних із національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав»² і поділ «інформаційний тероризм поділяють на: інформаційно-психологічний тероризм (контроль над ЗМІ для поширення дезінформації, чуток, демонстрації могутності терористичних організацій); інформаційно-технічний тероризм (завдання збитків окремим елементам і всьому інформаційному середовищу загалом: руйнування елементної бази, створення

¹ Кормич Л.І., Кормич А.І. Новий формат загроз міжнародного тероризму: час мереж та технологій. *Актуальні проблеми політики*. 2019. Вип. 63. С. 6-19.

² Смачило Т.В., Кривцун А.Р. Феномен інформаційного тероризму як загрози міжнародній безпеці. *Молодий вчений*. 2017. №11 (51). С.124-127.

перешкод на лініях зв'язку, штучне перенавантаження вузлів комунікації та інше)»¹ тільки примножують плутанину.

Така теза знаходила відгук у зарубіжних дослідників ще на початку століття, так, у 2004 році Г.Вейман написав: «Кібератаки на критично важливу інфраструктуру не рідкість, але вони не проводяться терористами і не прагнуть нанести збитки, які можна було б кваліфікувати як кібертероризм»². Вважаємо її актуальною досі. При цьому, терористична «війна ідей», яка ведеться у тому числі в кіберпросторі може охоплюватися поняттям «пропаганда» і бути складовою інформаційно-психологічної війни – у цьому аспекті відкидання зв'язку кіберпростору і терориста було б помилковим.

Таким чином, кібертероризм – це ще один термін, що виник разом із розвитком детериторіалізованого віртуального простору, де велика кількість загроз і ще більша кількість вразливостей і швидко проник у державну політику безпеки, наукові видання, газети тощо.

Цифрові розробки, стрімкий розвиток технологій відкривають більше можливостей для дестабілізаційного впливу, а кіберпростір – це нове місце конфлікту, що ставить перед державами серйозні виклики стосовно їх суверенітету. Зміни, що принесла цифрова епоха із її інноваційними інструментами в усі сфери соціального, економічного, політичного, культурного життя з інколи глобально-тривожними наслідками потребували відповіді законодавства. І.М. Милосердна слушно зазначає, що «у ХХІ ст. ефективна та надійна міжнародна безпека може бути тільки загальною і усеосяжною. Така безпека повинна охопити усі держави і

¹ Бойченко О.В. Медіа-тероризм: особливості сучасних ознак інформаційної безпеки. *Інтегровані інтелектуальні робототехнічні комплекси (ІРТК-2009)* : друга міжнародна наук.-практ. конф., м.Київ, 25–28 травня 2009 р. Київ : НАУ, 2009. С. 230–232.

² Weimann G. Cyberterrorism How Real Is the Threat? Special report. *United State institute of peace*. 2004. URL: <https://www.usip.org/sites/default/files/sr119.pdf> (дата звернення: 30.04.2022).

регіони, а також враховувати усі чинники, які впливають на міжнародну систему: військові, політичні, економічні та інші»¹.

У своїх звітах міжнародні спільноти виражають занепокоєність з приводу тривожних тенденцій у вигляді кібернападів: так, експертами Комітету з питань цифрової трансформації ООН відмічено: «Складні (гібридні) загрози розмивають традиційну лінію розмежування між миром та збройним конфліктом, ставлять під сумнів звичайний розподіл відповідальності між цивільним та військовим секторами. Через високу швидкість технологічної еволюції вкрай ускладнюється прогнозування майбутніх головних загроз»², а експерти НАТО констатують: «Вздовж периферії НАТО і за її межами утворилася дуга небезпеки та нестабільності... Кібернапади становлять очевидний виклик безпеці Альянсу і можуть бути не менш згубними для сучасних суспільств, ніж напади з застосуванням звичайних видів зброї. В Уельсі ми дійшли згоди про те, що кіберзахист є частиною головного завдання НАТО – колективної оборони. Зараз, у Варшаві, ми знову підтверджуємо оборонний мандат НАТО і визнаємо кіберпростір сферою операцій, в якому НАТО має захищати себе так само ефективно, як вона це робить у повітрі, на землі та на морі... Ми вітаємо зусилля щодо розробки добровільних міжнародних норм відповідальної поведінки держав та заходи зміцнення довіри стосовно кіберпростору»³. З огляду на слова експертів НАТО зазначимо, що кібервійні чи окремим кібератакам протиставляється «кіберзахист», який розуміється як «сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак,

¹ Милосердна І.М. Чинники та напрями формування ефективної системи міжнародної безпеки в сучасних умовах. *Правове життя сучасної України* : у 3 т. : матеріали Міжнар. наук.-практ. конф. м. Одеса, 15 трав. 2020 р., Одеса : Гельветика, 2020. Т. 1. С. 213-216.

² Олексюк Л. Кращі практики управління кібербезпекою : оглядовий звіт. *United Nations Development Programme* : веб-сайт. URL : https://www1.undp.org/Report_on_Cybersecurity_04.pdf (дата звернення: 02.11.2021).

³ Заява за результатами саміту у Варшаві. *North Atlantic treaty organization*. URL : https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=uk (дата звернення: 02.11.2021).

ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем» (п.7 ст.1 ЗУ «Про основні засади забезпечення кібербезпеки України»). Кіберзахист є складовою політики інформаційної безпеки. Використання кіберпростору стало частиною досягнення національних інтересів: оборонна і наступальна діяльність офіційно входить до стратегічних документів найбільш впливових учасників міжнародних відносин. Тим не менше, діяльність у кіберпросторі регулюється не лише національними нормативними актами, але й нормами міжнародного права. Наприклад, попри складність повноцінного теоретичного осмислення, на міжнародному рівні 22 грудня 2018 р. Генеральною Асамблеєю ООН було прийнято резолюцію «Заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки» (A/73/678), разом з тим, за слушним наголосом зарубіжних дослідників: «Кіберпростір не визнає зусиль дипломатії і стіл переговорів, звісно, не є його складовою частиною»¹.

Різке зростання комп'ютерних атак за участю і державних, і недержавних суб'єктів є реальною міжнародною загрозою, крім того, збільшення кількості кібератак, що ставлять під загрозу нормальне функціонування критичної інфраструктури є однією із підстав міждержавного напруження а відтак, за вірним наголосом науковців: «сучасні інформаційні загрози підкреслюють нагальну потребу у співпраці між державами для попередження постійних загроз в інтернеті, забезпечення кращого розслідування, затримання і переслідування зловмисних агентів, подолання проблем кібербезпеки, адже сучасні суспільства глобально взаємопов'язані, а кібератаки можуть призвести до значних економічних і соціальних збитків»².

¹ Mohee A. *Cyber war: The hidden side of the Russian-Ukrainian crisis*. *SocArXiv* : веб-сайт. URL: <https://osf.io/preprints/socarxiv/2agd3/> (дата звернення 01.03.2023).

² Трофіменко О.Г., Прокоп Ю.В., Логінова Н.І., Задерейко О.В. Кібербезпека України: аналіз сучасного стану. *Захист інформації*. 2019. Том 21. № 3. С. 150-157.

Заяви про кібервійну лунають і на рівні окремих держав. Наприклад, у 2019 р. міністерка Збройних Сил Франції Флоранс Парлі констатувала: «Кібервійна почалася». Аби протистояти кібератакам, Франція розробила доктрину кібервійни, яка передбачає не лише оборонні, але й наступальні дії (те саме зробили і США)¹. У Франції до 2025 року планують набрати більше 1000 кібер-бійців (комбатантів)².

Зростання кібератак, і у кількісному, і у якісному (серйозність впливу) аспектах дозволяє констатувати відмінну від звичайної кіберзлочинності природу – серйозність і розмір, яке виходить за межі інформаційно-комунікаційних технологій, а глибоко, тривало і системно впливає на всі аспекти життєдіяльності суспільства, державних та міждержавних інституцій, пагубна динаміка зростає.

Наявність широкого доктринального пласта, яким характеризується теорія і практика інформаційно-технічної війни зумовлює необхідність виділення її класифікаційних моделей. За словником «класифікація – розподіл предметів на класи, зроблений таким чином, що кожен клас займає відносно інших класів точно визначене і міцно закріплене місце»³. Це особливий випадок застосування логічної операції поділу об'єму поняття, класифікація означає певне упорядкування, а складність теорії інформаційних війн, яку можна віднести до «теорії множин» особливо потребує раціональної організації її розрізнених елементів.

Першу класифікаційну модель вважаємо визначальною – її *критерієм* виступає *об'єкт спрямування* інформаційно-технічної війни. За посяганням на об'єкт інформаційно-технічну війну можна розділити на:

1) інформаційні системи органів державної влади та місцевого самоврядування;

¹ Samama P. Comment la France se prepare a une cyberguerre mondiale. *BFM business*. 2019. URL: [bit.ly/45JII5o](https://www.bfm.com/fr/economie/cybersecurite/article-comment-la-france-se-prepare-a-une-cyberguerre-mondiale) (дата звернення: 13.12.2021).

² Trujillo E. Cyberdefense: «La cyberguerre s'apparente avant tout a une guerilla». *BFM business*. 2020. URL: [bit.ly/3Rh2GuA](https://www.bfm.com/fr/economie/cybersecurite/article-la-cyberguerre-s-apparente-avant-tout-a-une-guerilla) (дата звернення: 13.12.2021).

³ Павлов В.І., Лебедєв В. О. Словник найбільш уживаних термінів з філософії, логіки, етики, естетики та релігієзнавства. Харків : УкрДУЗТ, 2019. С.45.

2) інформаційні системи критично важливих об'єктів інформаційної інфраструктури;

3) комплексні атаки.

Попри захищеність комп'ютерних систем органів державної влади та місцевого самоврядування доступ до них часто стає метою кіберсуб'єктів. Такі дії не можуть виключати актів кіберзлочинності, наприклад, отримання особистої інформації з метою подальших шахрайських дій до яких можна віднести випадок із українськими громадянами А.Радченком та О.Єременком, яким у США було висунуто звинувачення у шахрайстві із цінними паперами із використанням електронних засобів – із Системи електронного збору, аналізу і пошуку даних Комісії із цінних паперів США за допомогою скоординованих кібератак, фішингу і зараження комп'ютерних систем шкідливим ПЗ, було викрадено тисячі файлів, у тому числі квартальну та річну звітність, конфіденційну фінансову інформацію, однак, у деяких випадках вони все ж є спробою порушити сталість роботи органів влади за допомогою інструментів інформаційно-технічної війни. Відомі атаки на органи законодавчої влади поки що більше відносяться до одиничних атак, а не до інформаційно-технічної війни, або є складовими скоординованих і тривалих кібероперацій у випадку комплексних нападів (на декілька об'єктів). Так, у червні та серпні 2017 року відбулася спроба отримання несанкціонованого доступу до облікових записів політиків палат парламенту Сполученого Королівства. Державна служба її Величності звинуватила Іран¹. У жовтні 2020 р. подібне сталося із політиками у парламенті Норвегії. Офіційно звинувачення було висунуто Росії², а у

1

Iran blamed for Parliament cyber-attack. 2017. BBC. URL: <https://www.bbc.com/news/uk-41622903> (дата звернення: 12.12.2021).

2

Norway blames Russia for cyber-attack on parliament. BBC. URL: <https://www.bbc.com/news/world-europe-54518106> (дата звернення: 12.12.2021).

березні 2021 р. напад на електронну систему норвезького парламенту відбувався із Китаю¹.

Кібератаки на органи виконавчої влади зазвичай мають більш серйозне стратегічне значення, оскільки більшість потенційно цікавої для кібервоїнів інформації – фінансової, у сфері оборони, розвідки, шпигування за діяльністю уряду, доступ і опублікування конфіденційної урядової інформації (у 2017 р. було опубліковано конфіденційні урядові документи Філіпін, включно із стенограмою розмови президента Родріго Дутерте і президента США) зосереджено саме в органах виконавчої влади. Наприклад, у 2009 р. було проведено низку кібероперацій під назвою «Operation Troy», які було спрямовано проти Південної Кореї та США. Серед уражених об'єктів був сайт Білого дому США, Пентагону, Міністерство оборони Південної Кореї, Міністерство державного управління і безпеки Південної Кореї, Національна розвідувальна служба Південної Кореї. У грудні 2016 року було здійснено масштабний напад, у тому числі на Міністерство фінансів України, Пенсійний фонд України: «унаслідок цієї кібератаки було знищено частину інформації, а також виведено з ладу обладнання. У зв'язку з цим сталися затримки з бюджетними виплатами на сотні мільйонів гривень. Для виведення з ладу серверів державних фінансових установ зловмисники використовували «KillDisk» (програма для знищення файлів з комп'ютерів (серверів), принцип роботи якої полягає у знищенні або перезаписі критично важливих системних файлів), а також троянську програму «BlackEnergy»². Принагідно відмітимо, що з метою запобігання знищенню інформації Проектом Закону України «Про внесення змін до деяких законів України» № 4378 пропонується «законодавче врегулювання питання щодо здійснення резервного

1

Buli N. Norway says cyber attack on parliament carried out from China. *Reuters*. URL: <https://www.reuters.com/world/china/norway-says-march-cyber-attack-parliament-carried-out-china-2021-07-19/> (дата звернення: 08.12.2021).

² Кібератаки Російської Федерації: Хронологія. Міністерство оборони України : офіційний веб сайт. URL: <https://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federaczii-hronologiya.html> (дата звернення: 09.12.2021).

копіювання інформації та відомостей державних електронних інформаційних ресурсів державними органами, військовими формуваннями, утвореними відповідно до законів України, державними підприємствами, установами та організаціями, а також питання щодо централізованого зберігання Державною службою спеціального зв'язку та захисту інформації України таких резервних копій»¹.

Критично важливі об'єкти інформаційної інфраструктури у національному законодавстві, згідно п. 16 ст.1 ЗУ «Про основні засади забезпечення кібербезпеки України» визначаються як «підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей». Недоліком визначення поняття є його оціночні судження: «велике значення», «негативний вплив». Не уточнення підстав дозволяє віднести до цієї категорії велику кількість підприємств.

Відповідно до п.19 ст.1 ЗУ об'єкт критичної інформаційної інфраструктури визначається як «комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури». У спеціальному законі «Про критичну інфраструктуру» під критичною інфраструктурою розуміються «об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких

¹ Комітет з питань цифрової трансформації рекомендує Верховній Раді прийняти у другому читанні і в цілому законопроект щодо здійснення резервного копіювання інформації та відомостей державних електронних інформаційних ресурсів державними органами. *Верховна Рада України* : офіційний веб портал парламенту України. URL: https://www.rada.gov.ua/news/news_kom/216206.html (дата звернення: 09.12.2021).

може завдати шкоди життєво важливим національним інтересам» (п.7 ст.1). Крім того, цим законом виділено чотири категорії критичності об'єктів: I категорія критичності – особливо важливі об'єкти, які мають загальнодержавне значення, значний вплив на інші об'єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації державного значення; II категорія критичності – життєво важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення; III категорія критичності – важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення; IV категорія критичності – необхідні об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення. Загалом національну інфраструктуру можна розділити на цивільну та військову.

Таллінський мануал визначає критично важливу інфраструктуру як «фізичні чи віртуальні системи і активи, що знаходяться під юрисдикцією держави, які настільки життєво важливі, що їх вивід із ладу чи знищення може завдати збитків безпеці, економіці, охороні здоров'я чи навколишньому середовищу»¹. В.В.Музика відзначає: «загалом до критичної інфраструктури держави найчастіше відносять об'єкти та активи таких секторів як: сектор енергетики, сектор фінансів, сектор транспорту, сектор водопостачання; урядовий сектор; оборонний сектор; сектор реагування на надзвичайні ситуації та сектор охорони здоров'я»².

Попри те, що ЗУ «Про критичну інфраструктуру» у ч.4 ст.9 передбачає 18 пунктів «важливих функцій та/або послуг порушення яких призводить до негативних наслідків для національної безпеки України» ми підтримуємо більш оптимізований підхід, принагідно відмітимо, що деякі із цих функцій видалися сумнівними Головному юридичному управлінню, «враховуючи, що

¹ Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge : Cambridge University Press, 2017. P.213.

² Музика В.В. Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення: дис. ... доктора філософії : 081. Одеса, 2021. С.175.

законопроектом віднесено до таких послуг, зокрема дослідницьку діяльність, то із положень законопроекту не вбачається, чи вважатиметься збій, як це визначено законопроектом, у дослідницькій діяльності (і якій саме дослідницькій діяльності?) збоєм життєво важливої функції та/або послуги?»¹.

Кібератаки протягом останніх десяти років спіткали ЄС, США, більшість країн-членів НАТО. У них нападали на критичну інфраструктуру, нейтралізували важливі мережі на декілька годин і днів: залізничні лінії, аеропорти, військові бази – лише короткий список потенційних цілей кібернападів. Невпинний глобалізаційний процес передбачає неможливість обмеження підходів до захисту критичної інфраструктури лише національним рівнем, однак планування її захисту, зокрема, з боку кіберзагроз ускладнюється тим, що дати однозначне визначення «критичній інфраструктурі», а тим більше конкретний перелік її об'єктів поки що неможливо, тому, кожна держава визначає свій власний перелік виходячи із директиви національної безпеки.

За типом приналежності об'єкта критичної інфраструктури або за галузевим спрямуванням інформаційно-технічну війну, що характеризується істотною шкодою для життєво важливих послуг, стабільності політичної системи і безпеки держави можна об'єднати у такі групи:

1. Фінансова система (згідно законодавчого розподілу сюди можна віднести фінансові та банківські послуги) найбільш узагальнено фінансову систему визначають як «сукупність різноманітних видів фондів фінансових ресурсів, які є у розпорядженні держави. Вона має внутрішню будову та організаційну структуру. Внутрішня будова складається зі сфер та ланок і репрезентована такими складовими: державні фінанси, фінанси суб'єктів господарювання, міжнародні фінанси та фінансовий ринок (забезпечувальна сфера). До складу організаційної

¹ Зауваження Головного юридичного управління до проекту Закону України про критичну інфраструктуру. Верховна Рада України : офіційний веб портал парламенту України. URL: bit.ly/484IYId (дата звернення: 18.11.2021).

структури входять органи управління у сфері бюджету, контрольно-регулювальні, фінансові інститути та цільові фонди»¹. У процесі здійснення і управління фінансовою системою інтенсивно використовуються інформаційні технології: розвиваються нові форми банківського і фінансового посередництва, онлайн-страхування та управління страховими ризиками, звичними є безготівкові платежі, онлайн-платформи для кредитування чи інвестування в інноваційні проєкти (краудфандинг), активно розвивається алгоритмічна торгівля. Цифрові фінансові перетворення отримали спеціальне позначення – «FinTech», а пандемія COVID-19 пришвидшила їх розвиток.

Звичайні атаки на фінансову систему проводяться за допомогою різних методів, таких як крадіжка облікових даних через фішинг, атак за типом відмова в обслуговуванні (DDoS), що перевантажує систему мільйонами одночасних запитів і робить використання фінансових послуг неможливим чи зламування, наприклад, у 2011 році було викрадено дані, номери рахунків та контакти одного з найбільшого міжнародного банку – *Citibank*, однак, для констатації саме інформаційно-технічної війни потрібні великі збитки і масштабність. Зазвичай, головною метою кібернападів є корислива мета. Так, у 2015 і 2016 рр. було атаковано міжнародну систему міжбанківських платежів SWIFT. Над кібернападом працювала ціла хакерська група. Викрадення облікових записів працівників Центрального банку Бенгладешу у SWIFT призвело до викрадення 101 млн. доларів² (20 млн. було повернуто) у банку Нью-Йорка, де був відкритий рахунок Бенгладешського банку (розміщено міжнародні резерви). У позовній скарзі «Bangladesh Bank проти Rizal Commercial Banking Corporation та ін.» від 31 січня 2016 року до Окружного суду США Південного округу Нью-Йорка вказувалося, що це «масштабна багатолітня змова з метою проведення одного з найбільшого пограбування в історії», а відповідальність

¹ Орел В. М. Фінансова система як невід’ємна складова економічного процесу країни. *Український журнал прикладної економіки*. 2016. Том 1. № 1. С. 141-152.

² Ecuadorean Bank Loses \$12 million via SWIFT. *Trendmicro*. URL: bit.ly/3P9LJ2w (дата звернення: 18.12.2021).

покладали на «північнокорейських хакерів, що об'єдналися із спільниками на Філіппінах»¹. Провадження було закрито рішенням 20 березня 2020 р. з огляду на транскордонність справи – переведення коштів відбулося на рахунки у Філіппінах, для того, щоб констатувати неспроможність місцевого суду вирішити такого масштабу справу за такий строк достатньо навіть того факту, що Філіппіни відомі своїми законами про банківську таємницю – зокрема, Законом Республіки №1405 заборонено розкривати відомості про депозити за запитами у будь-якій банківській установі під загрозою тюремного ув'язнення строком до 5-ти років². З огляду на загальний осуд такого підходу влітку 2021 року розпочалося реформування банківської системи Філіппін. Основною причиною відмови у задоволенні позовних вимог стала непідсудність викладених у заяві вимог Окружному суду США Південного округу Нью-Йорка³. Принагідно відмітимо частоту появи саме північнокорейських слідів у різних кіберопераціях, зокрема, окремі джерела⁴ говорять вказують на те, що черв'як-вимагач WannaCry (від якого постраждали користувачі близько 150 країн світу) – шкідливе програмне забезпечення, що спочатку блокує комп'ютер, а потім вимагає викуп у криптовалюті для його розблокування теж інформаційна зброя родом із Північної Кореї.

Складні методи призводять до викрадення грошових коштів в особливо великих розмірах чи даних, а деякі зупиняють роботу, що також супроводжується великими збитками. Так, програма вимагач NotPetya (Petya.A, ExPetr), яка шифрує дані і не дає можливості їх розшифрувати, ефективно знищуючи дані у 2017 р.

1

Bangladesh Bank vs. Rizal Commercial Banking Corporation, et al. – Complaint in the United States District Court for the Southern District of New York. *National security archive*. URL: <https://nsarchive.gwu.edu/media/18204/ocr> (дата звернення: 04.12.2021).

² An act prohibiting disclosure of or inquiry into, deposits with any banking institution and providing penalty therefor: Republic Act № 1405. *The LawPhil project*. URL : https://lawphil.net/statutes/repacts/ra1955/ra_1405_1955.html (дата звернення: 04.12.2021).

³ Case 1:19-cv-00983-LGS Bangladesh bank against Rizal commercial banking corporation at al. URL: bit.ly/3PxBkz2 (дата звернення: 05.12.2021).

⁴ Nakashima E. The NSA Has Linked the WannaCry Computer Worm to North Korea. *Washington Post*. URL: wapo.st/3R9X19v (дата звернення: 18.12.2021).

нанесла великі економічні збитки підприємствам та установам, серед яких були і фінансові установи – зокрема особливо сильно постраждали «Ощадбанк», «Укргазбанк», «Укрсоцбанк», «ТАСкомбанк» etc., а саме розповсюдження вірусу розпочалося із оновлення програми бухгалтерської звітності М.Е.доc. Відмітимо, що з метою захисту інформації та кіберзахист у платіжних системах Правлінням НБУ було прийнято Постанову «Про затвердження Положення про захист інформації та кіберзахист у платіжних системах».

Технологічний та інформаційний прогрес призвів не лише до трансформації традиційних банківських систем, але й до виникнення нових цифрових криптовалютних платформ. Поява і розвиток Bitcoin.org, LiteCoin, Ethereum, Ripple призвів до посилення атак, які, з огляду на збитковість можуть підпадати під розуміння інформаційно-технічної війни, попри потужні системи захисту, кібервійни знаходять вразливість і слабкість у функціонуванні цих цифрових сервісів. У 2018 році 14 атак на криптобіржі спричинили збитки на суму 882 млн. доларів¹.

Спрямування кібервійни не обмежується метою відслідковування дій органів влади, викраденням конфіденційної інформації чи порушенням роботи об'єктів критичної інфраструктури, одним із таких – є прибуток.

2. Промисловість, зокрема, енергозабезпечення (в тому числі постачання теплової енергії), водопостачання та водовідведення, продовольче забезпечення; хімічна промисловість.

Дослідженню впливу кібервійни, що в окремих випадках є складовою гібридної війни приділяється увага не лише на національному рівні. Міжнародні утворення спрямовують свої зусилля на захист критично важливої інфраструктури. Зокрема, Радою науки та технологій НАТО проведено дослідження «Енергетична

¹

14 cyber attacks on crypto exchanges resulted in a loss of \$882 million. *Finyear*. URL: https://www.finyear.com/14-cyber-attacks-on-crypto-exchanges-resulted-in-a-loss-of-882-million_a40041.html (дата звернення: 04.12.2021).

безпека в епоху гібридних війн»: «гібридна війна спрямована на підриг довіри до громадянського суспільства і демократичних засад, у першу чергу шляхом кібератак на критично важливу інфраструктуру, у тому числі енергетику... У цьому аспекті вона несе у собі потенційну загрозу суверенітету, оскільки дає країнам, терористичним організаціям і злочинцям відносну анонімність за допомогою недорогого і високодохідного методу впливу на політику і політику інших держав»¹. Про підвищену увагу до галузі енергетики свідчить і регулярне звітування про групи ризиків², а у спеціальних дослідженнях робиться вказівка на ретельний підхід до захисту енергетичної галузі: «кібератаки на ПЕК є серйозною загрозою для багатьох країн. Суть енергетичних інтересів держави, в кінцевому підсумку, зводиться до побудови надійної системи безпеки, в тому числі і від кібератак...»³; «стратегія забезпечення повноцінного функціонування Регулятора ринків енергетики та комунальних послуг... [полягає у тому числі] в підвищенні кіберзахисту інформаційної системи НКРЕКП»⁴.

Особлива увага енергетиці приділяється з огляду на те, що стабільна робота – розподіл, виробництво, передача і зберігання електроенергії є гарантією забезпечення не лише технологічно розвиненого суспільства, але й життєздатності держави.

Рівень збитковості у 2017 р. за допомогою вірусу NotPetyavirus дав зрозуміти, що успішна кібератака може викликати аварійне становище – вірусом були вражені комп'ютерні системи «Укренерго», «Київенерго» etc., однак масштабні напади на енергетичні комплекси відбувалися і раніше. Так, у 2010 р. в Ірані на заводі із

¹ Dupuy A.C., Nussbaum D., Butrimas V., Granitsas A. Energy security in the era of hybrid warfare. *NATO*. URL: bit.ly/3sNIUwo (дата звернення: 16.12.2021).

² Final Report - Study on cyber security in the energy sector of the Energy Community. *Blueprint Energy Solutions GmbH*. URL: <https://energy-community.org> (дата звернення: 16.12.2021).

³ Жуйкова К.В., Гулак Г.М. Формалізація моделі загроз енергетичної безпеки. *Молодий вчений*. № 11 (38), 2016. URL: <http://molodyvcheny.in.ua/files/journal/2016/11/26.pdf> (дата звернення: 18.12.2021).

⁴ Омельченко В., Чекунова С., Білявський М. Енергетика України: виклики та ініціативи. *Razumkov Centre*. URL: https://razumkov.org.ua/uploads/article/2020_energy_initiatives.pdf (дата звернення: 16.12.2021).

збагачення урану із ладу вийшло 1368 центрифуг, і хоч, офіційно іранський уряд винуватця вірусу Stuxnet, на який вказували спеціалісти не визнав, однак, на найвищому рівні атаки на об'єкт визнавалися, а у втручанні звинувачували США. Час потрібен вірусу від перших заражень комп'ютерів до цілих цехів склав один рік. Виведення центрифуг із ладу призвело до переносу введення в експлуатацію АЕС «Бушер» і відсунуло ядерну програму країни на два роки. Відмітимо, що, попри те, що окремі випадки використання кіберзброї відомі уже з 1980-х саме ця подія вважається науковцями як така, що констатувала поповнення збройного арсеналу і продемонструвала як комп'ютерна програма може призводити не лише до серйозних збитків, але й мати серйозний політичний вплив. У 2015 р. відбулося масштабне виведення із ладу трьох енергопостачальних компаній України. Кібервоїни використовували троянську програму Black Energy. Про постійну загрозу енергетиці свідчать і заяви посадових осіб СБУ: «Загалом за 2018 р. було заблоковано близько 400 кібератак, деякі з них за своїми наслідками могли бути не менші ніж вірус Petya A. Зокрема і атака на енергетику, вірус Grey energy, який був послідовником вірусу Black energy...»¹.

З метою забезпечення кіберзахисту АЕС Міжнародне агентство із атомної енергії (МАГАТЕ) у 2021 р. розробило перший практичний посібник із комплексного вирішення питань комп'ютерної безпеки «Комп'ютерна безпека для фізичної ядерної безпеки»².

На фоні швидкого оцифрування вразливим до кібератак також є гідротехнічне обладнання, особливо у частині роботи насосних систем і дистанційного керування. Кібервоїни можуть використовувати недосконало налаштовані міжмережеві екрани для проникнення у центр управління водопровідних станцій, збільшувати тиск у

¹ Мурашко А. У 2018 році українські фахівці заблокували близько 400 кібератак. *Інформаційне агентство «Українські Національні Новини»*. URL: bit.ly/3LcX3d2 (дата звернення: 12.02.2019).

² Now Available: IAEA Guidance on Computer Security for Nuclear Security. *IAEA*. URL: bit.ly/3rb0oCv (дата звернення: 06.12.2021).

проводах для того, аби ті лопали, або, навпаки – зменшувати тиск, що призведе до недостатньої подачі води, очищена вода може змішуватися із стічними водами, що може призвести до зараження бактеріями. Однак, деякі кібератаки мають значно вищий рівень небезпеки, ніж виведення із ладу гідротехнічного обладнання – шляхом зміни хімічних властивостей (зміна рівня гідроксиду натрію) води на водоочисній станції вони ставлять під загрозу безпечність її споживання. Спроба такої кібератаки, а по факту – отруєння води шляхом збільшення концентрації хімічної речовини, відбулася у лютому 2021 року на систему водопостачання м.Олдсмар (Флорида, США).

До водопроводів також підключені системи, які можуть стати об'єктами кібератак. Наслідки кібератак особливо серйозні, коли вони вражають важливі сфери повсякденного життя людей.

Продовольче забезпечення теж сфера потенційного ризику інформаційно-технічної війни, хоча поки що все обмежувалося одноразовими атаками: наприклад, у червні 2021 р. програма-вимагач порушила виробництво м'яса однієї із найбільшій компаній «JBS» у Північній Америці та Австралії, однак, такі атаки можуть призводити до зростання цін на продукти.

3. Транспортне забезпечення. У липні 2021 р., наприклад, кібернапад було здійснено на залізничні дороги в Ірані – на табло було розміщено інформацію про затримку чи відміну потягів.

4. Охорона здоров'я, зокрема, медичні заклади, фармацевтична промисловість, стає функціонування біолабораторій, виготовлення вакцин. Кібератаки на заклади охорони здоров'я несуть у собі дві загрози: 1) можливість викрадення конфіденційних даних пацієнтів; 2) блокування роботи комп'ютерних систем. Відомі напади здійснювалися за допомогою програм-вимагачів, що призводило до сповільнення роботи закладів охорони здоров'я (WannaCry у Великобританії, Ryuk у США). А у 2020 р. в Німеччині під час вторгнення програми-вимагача у систему університетської клініки Дюсельдорфа жінка

померла через необхідність перевезення її в іншу клініку з огляду на кібернапад, який паралізував роботу системи. У ЗМІ зазначалося, що це «може бути перша смерть напряду пов'язана із кібератакою на лікарню»¹. На підвищення смертності через втручання програм-вимагачів, зокрема, у лікарняні системи вказує і дослідження Ponemon Institute, зокрема у звіті «Ponemon Research: вплив програм-вимагачів на охорону здоров'я під час COVID-19 і після нього» за участю 597 медичних організацій (у т.ч. інтегровані мережі доставки, регіональні системи охорони здоров'я, лікарні etc.) вказано, що «програми-вимагачі призводять до зростання смертності пацієнтів»².

У 2020 р. різного роду нападам піддавалися і фірми – розробники вакцини проти COVID-19. Занепокоєння міжнародними атаками, спрямованих на медичні заклади розпочалося у травні 2020 р., коли ФБР США і Міністерство національної безпеки США офіційно звинуватили Китай у спробі використати комп'ютерне шпигування (вторгнення у чужі комп'ютерні системи з метою збору інформації) для крадіжки даних про вакцину проти Covid-19. Такі дії: 1) роблять спробу незаконного отримання інтелектуальної власності, пов'язаної із вакциною, її тестуванням, дослідженнями (очевидно, що інформація про вакцину стане менш цінною, коли вакцина отримає патент), яка має велику цінність – як результат і потенційний прибуток; 2) ставлять під загрозу виготовлення безпечних, ефективних варіантів вакцинації.

Небезпека інформаційно-технічної війни полягає у складній ідентифікації і класифікації можливих вразливостей, робота комп'ютерної системи залежить від вбудованих технічних факторів і прикладного програмного забезпечення.

1

Westman N. Woman dies during a ransomware attack on a German hospital. *The Verge*. URL: <https://www.theverge.com/2020/9/17/21443851/death-ransomware-attack-hospital-germany-cybersecurity> (дата звернення: 12.01.2022).

² Ponemon Research Report: The Impact of Ransomware on Healthcare During COVID-19 and Beyond. Censinet. URL: <https://www.censinet.com/ponemon-report-covid-impact-ransomware/> (дата звернення: 12.01.2022).

Збитки від інформаційно-технічної війни включають вкрадені кошти та ушкоджені системи. За видами реакції на інформаційно-технічну війну можна виділити:

- 1) прийняття збитків;
- 2) укріплення інфраструктури, аби попередити подальші або повторні напади;
- 3) відмова від цифрових інструментів і повернення до традиційних систем.

Очевидно, що забезпечення стійкості конструкцій є найбільш бажаним способом реагування, який потребує критичної оцінки, зокрема розуміння природи загроз й виправлення комп'ютерної вразливості (використання простих паролів, відсутність постійно оновлюваного антивірусу, відсутність резервного копіювання даних) і мережевої вразливості.

2.4. Інструментарій інформаційно-технічної війни.

Розвинені технології у вигляді доступних соціальних мереж, можливість майже миттєвих онлайн-транзакцій, й загальна автоматизація процесів стали невід'ємними елементами життя людей. Зростання цифрової взаємодії, важливість обміну інформацією, й численні варіанти її використання надають технологіям безсумнівну цінність, а високотехнологічні гаджети пропонують більш високий рівень обробки інформації і її використання. Однак, із стрімкою технологічною еволюцією прогресують й можливості інформаційно-технічної війни, ризики, що пов'язані із використанням інформаційно-технічної зброї. А.Ф.Брентлі відзначає, що «невелика держава, яка володіє кіберзброєю може мати більше влади, ніж велика держава без кіберзброї»¹.

¹ Brantly A.F. Military and intelligence cyber decision-making: a dissertation Doctor of Philosophy. Georgia, 2012. URL: https://getd.libs.uga.edu/pdfs/brantly_aaron_f_201212_phd.pdf С.118 (дата звернення: 12.12.2021).

Розглянемо інформаційно-технічну зброю (кіберзброю) більш детально. Поняття кіберзброї складне у тлумаченні, адже його помилково було б визначати суто як «смертоносний кіберпросторовий пристрій» або «кіберпросторовий засіб, руйнівний для речей і людей», тому що це визначення беззмістовне. Однак, як і уся теорія інформаційних війн, поняття кіберзброї є дискусійним. Р.В.Гришук з цього приводу відзначає: «кібернетична зброя... нині розробляється, досліджується та застосовується урядами близько 140 держав світу... Незважаючи на це, ні на регіональному, ні на міжнародному рівнях немає однозначного розуміння того, що ж саме слід розуміти під КЗ та як потрібно здійснювати її класифікацію. Термінологічна та правова невизначеність стосовно категорії КЗ, що склалася на сьогодні у світовому масштабі, породжує перед суспільством ряд проблем як організаційного, так і технологічного характеру»¹.

Тім Стівенс у роботі «Кіберзброя: сила і керування невидимим» під кіберзброєю розуміє «шкідливі програмні об'єкти, які використовуються для нанесення шкоди комп'ютерним мережам і системам. Вони загрожують цілісності і функціональності цифрових систем, які забезпечують глобальні канали зв'язку і обміну, що може серйозно вплинути на соціальний, економічний і політичний порядок»². У праці «Кіберзброя: нова архітектура глобального управління» науковець вказав на таку особливість кіберзброї, у порівнянні із традиційною як «відсутність традиційної фізики – це комп'ютерний код, який існує лише в інформаційних структурах, таких як Інтернет»³.

¹ Гришук Р.В. Кібернетична зброя: класифікація, базові принципи побудови, методи та засоби застосування й захисту від неї. *Сучасна спеціальна техніка*. 2016. № 3 (46). С.94-101.

² Stevens T. Cyberweapons: power and the governance of the invisible. *ResearchGate*. URL: https://www.researchgate.net/publication/320293035_Cyberweapons_power_and_the_governance_of_the_invisible (дата звернення: 06.12.2021).

³ Stevens T. Cyberweapons: an emerging global governance architecture. *ResearchGate*. URL: https://www.researchgate.net/publication/312188394_Cyberweapons_an_emerging_global_governance_architecture (дата звернення: 06.12.2021).

У наукових роботах виокремлюються різні групи інформаційно-технічної зброї. У своїй роботі В.Г. Бабенко серед груп виділяє: мережеву кіберзброю, попередньо встановлену кіберзброю, проникаючу кіберзброю, електромагнітну зброю, комунікаційну кіберзброю. Відмітимо, що під проникаючою кіберзброєю розуміється «цілеспрямована зміна акустичного, оптичного та інших середовищ з відповідною модифікацією сигналів, що надходять на зовнішні сенсорні датчики високотехнологічної зброї. За допомогою цих впливів забезпечуються перебої в роботі бойової техніки, яка атакує, або повне знищення керуючих комп'ютеризованих блоків цієї техніки»¹, до того ж, окремо виділяється електромагнітна зброя. Із таким підходом до групування кіберзброї можна погодитися лише частково, у зв'язку з тим, що: по-перше, відбувається змішування кібервійни, яка у найбільш простому розумінні спрямована на досягнення цілей у кіберпросторі, і електромагнітною війною, яка спрямована на контроль електромагнітного спектра чи атаку противника з його допомогою у традиційному конфлікті, те ж стосується і радіоелектронної боротьби, яка, за наведеним автором групуванням також повинна була бути включена до поняття «кіберзброї». У першому розділі нами було визначено, що універсальна роль інформації і різні способи її використання призвели до того, що з'явилися різні підходи до вживання терміна «інформаційна війна». Широта цих підходів варіюється від класичної радіоелектронної боротьби до кібервійни. Однак, між кібервійною й іншими формами є фундаментальна різниця, попри схожість функцій на стратегічному рівні, ці категорії розрізняються, якщо розглядати їх інструменти, методи, військове застосування і цілі. По-друге, кіберзброя відрізняється від засобів високоточного технічного озброєння. Якщо останнє переважно використовується проти сухопутних військ чи фізичної інфраструктури комп'ютерних мереж, то кіберзброя

¹ Бабенко В. Г. Основні групи кіберзброї та особливості її застосування. *Актуальні задачі та досягнення у галузі кібербезпеки* : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. Кропивницький : КНТУ, 2016. С. 23–24.

– це засіб інформаційних технологій, яка використовуються з метою безпосереднього впливу на глобальні комп'ютерні мережі (конфіденційність, цілісність, доступність інформації). Де конфіденційність означає збереження санкціонованого обмеженого доступу і розкриття інформації, у тому числі способи захисту конфіденційності і службової інформації. Цілісність означає захист від неналежної зміни чи знищення інформації. Доступність означає забезпечення швидкого і надійного доступу до інформації і її використання.

Л.Свенсон виділяє три категорії інформаційної зброї: «1) синтаксична зброя націлена на операційну систему комп'ютера, включає шкідливий код, такий як віруси, черв'яки, троянські коні, DDOS і шпигунське програмне забезпечення; 2) семантична зброя, яка складається із мінливої інформації, яка надходить у комп'ютерну систему; 3) змішана зброя, яка об'єднує синтаксичну та семантичну зброю для атак як інформації, так й інформаційної системи комп'ютера, що призводить до більш серйозної атаки»¹.

В збройному арсеналі інформаційно-технічної війни чотири основних методи. Першим є атаки спрямовані на перевантаження ресурсу запитами, аби вичерпати їх фільтрувальну здатність – такі дії призводять або до сповільнення, або до зупинки роботи інформаційної системи. До таких видів інформаційно-технічних атак належать: DoS (відмова в обслуговуванні); DDoS (розподілена відмова в обслуговуванні); DRDoS (відмова в обслуговуванні із розподіленим відображенням); зустрічається SYN-флуд атака, однак, вона визнається «морально застарілою»², оскільки уже існують ефективні способи її здолання; вилкова (подвійна) бомба. Ці атаки не приводять кібервоїна до отримання доступу до

¹ Swanson L. *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict*, 32 Loy. L.A. Int'l & Comp. L. Rev. 303. 2010. URL: <https://digitalcommons.lmu.edu/ilr/vol32/iss2/5/> (дата звернення: 15.12.2021).

² Прокопчук А., Баранов А. Сетевая атака SYN-флуд. *Institutional Repository Dnipro University of Technology*: веб-сайт. URL: <http://ir.nmu.org.ua/bitstream/handle/123456789/1881/SYN-FLOOD.pdf?sequence=1&isAllowed=y> (дата звернення: 14.07.2021).

інформації у системі і не викликають втрати чи крадіжки даних, а блокують роботу мереж і сервісів, роблять їх недоступними.

Другим є метод міжсайтового скриптингу (XSS) пов'язаний із вразливістю веб-сайтів. Кібервоїн вставляє шкідливий код або скрипт в базу даних веб-сайта. У літературі¹ прийнято класифікувати XSS-атаки:

За способом впливу:

1. Активна – не вимагає будь-яких дій зі сторони користувача;
2. Пасивна – спрацьовує у разі, якщо користувач вчиняє певні дії («клік», наведення вказівника миші тощо).

За вектором впливу:

1. Відбита (відображена) XSS є найбільш розповсюдженою, зазвичай не передбачає викрадення даних, а працює у комплексі з іншими атаками і методами – зокрема, соціальної інженерії і перетворюється у так звану XFS-атаку, яка спрямована на викрадення даних користувача, наприклад, шляхом запису натискання клавіш;

2. Збережена XSS-атака у свою чергу поділяється на два види:

а) Stealing cookies (викрадення cookies). Відмітимо, що згідно п. 30 Регламенту Європейського парламенту і ради (ЄС) (General Data Protection Regulation)² «фізичні особи можуть бути пов'язані з онлайн-ідентифікаторами за допомогою їхніх пристроїв, додатків, інструментів чи протоколів, зокрема IP-адрес, ідентифікаторів «cookie» (реп'яшків) або інших ідентифікаторів, таких як мітки радіочастотної ідентифікації. Це може залишити підказки, які, особливо в поєднанні з унікальними ідентифікаторами та іншою інформацією, отриманою з

1

Див.наприклад, комплексне дослідження Shende Dinesh Ankush. XSS Attack Prevention Using DOM based filtering API: dissertation. URL: <https://core.ac.uk/download/pdf/53189097.pdf> (дата звернення: 16.11.2021).

² Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). *Офіційний веб-портал Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 12.12.2021).

серверів, можна використати для створення профілів фізичних осіб та їхньої ідентифікації». У загальному, cookie визначаються як «текстові файли, які сервер веб-сторінки може зберігати на жорсткому дискові комп'ютера у вигляді певної інформації про користувача». Вони збирають різні види даних з метою розпізнавання користувача для подальших відвідин сайту, покращення цільової реклами, отримання кількісних показників відвідування сайтів etc. Певні типи файлів Cookie використовуються для створення унікального ідентифікатора сеансу, щоб користувачі могли залишатися у системі, наприклад, Гугл, Фейсбук. Stealing cookies дозволяє входити в облікові записи сторонньої особи, переглядати історію запитів, перечитувати повідомлення, вилучати списки контактів наприклад, з метою подальшого фішингу чи розсилання електронних листів, крадіжки даних платіжної або депозитної системи (наприклад, крадіжка даних через China UnionPay, депозит Alipay), або товарів із кошика онлайн-магазинів. У 2020 р. з'явилася програма Cookiethief, отримавши файли cookie хакер може підключатися до облікових записів Facebook з метою викрадення особистих даних або використати обліковий запис для подальшого фішингу, заразивши шкідливим ПЗ ще більше користувачів.

3. Комплексна – XSS Based Trojan Horse теж відбувається за допомогою метода соціально-технічної інженерії, необхідно завантажити троянську програму;
3) XSS-атака, заснована на DOM-моделі.

4. Clickjacking, на відміну від прямих атак на сервери, є похідним від XSS-атак. При відвідуванні цього сайту користувачем Інтернету, його дії, такі як знімки екрана, збір конфіденційних даних фіксуються, можливий подальший віддалений доступ і керування комп'ютером постраждалого користувача Інтернету.

Третім є метод соціально-технічної інженерії. В науковій літературі частіше визначається поняття «соціальна інженерія». Так, у контексті інформаційної безпеки соціальна інженерія використовується для позначення несанкціонованого доступу до інформації, не пов'язаного із зламуванням програмного забезпечення із

метою обманути людей для отримання паролів до системи чи іншої інформації, яка може порушити безпеку системи¹. Таким чином цей метод одночасно спрямований і на технічні засоби, разом з тим, оскільки недостатньо лише атаки на мережевий суб'єкт, необхідно задіяти і людину, якій ці технічні засоби належать, будучи єдністю соціального і технологічного доцільним видається визначення саме методу соціально-технічної інженерії (наприклад, фішинг залежить не лише від хакерських можливостей, але й від уміння змусити жертву довіряти кібервоїну).

До форм соціально-технічної інженерії відносяться:

1. Фішингові листи; у загальному, фішинг – спроба виманити особисту інформацію в користувача Інтернету. Зазвичай для фішингу застосовуються електронні листи, оголошення та фіктивні сайти, за дизайном дуже подібні до тих, які часто відвідує користувач². Листи приходять від підприємств, установ, організацій чи окремих осіб, яким жертва довіряє (наприклад, банк, відомі фірми на кшталт DHL, платформи електронної комерції як-от Amazon) із пропозицією перейти за вказаним у листі посиланням, відкрити доданий до листа файл або відповісти на повідомлення. У липні 2021 р. було повідомлено про отримання користувачами листів із посиланням на фальшивий веб-сайт Президента України, з якого завантажувався вірус³. Відзначимо, що кібервоїн докладає максимум зусиль для правдоподібності: у полі «Кому» жертва може бачити тисячі інших електронних адрес, таким чином, вважаючи, що лист надіслано від організації, із якою вона працює і якій довіряє; використовуються візуальні елементи організації (шрифт, логотип etc.). Однак, дедалі частіше зусилля кібервоїнів спрямовані на те, щоб звести до мінімуму «соціальний» аспект – залежність від довіри користувача.

¹ Дашко Д.А.Мешков В.И.Социальная инженерия с точки зрения информационной безопасности. *Institutional Repository NTU Dnipro Polytechnic* : веб-сайт. URL: bit.ly/469HURL (дата звернення: 02.08.2021).

² Обачність.Пильність.Захист.Ввічливість.Сміливість : посібник із цифрового громадянства та безпеки. URL: <https://nus.org.ua/wp-content/uploads/2018/08/PRESS.pdf>. (дата звернення: 18.07.2021).

³ Маскировался под сайт Президента. Госпечсвязи заблокировала фишинговый сайт. *Гордон*: веб-сайт. URL: bit.ly/3Pvycnc (дата звернення: 20.07.2021).

Для досягнення цієї цілі «фішери» використовують: підроблення адресної стрічки URL; атаки за типом «фармінг», метою якого є переправлення жертви із легального веб-сайту на шахрайський прихованим способом; шпигунський фішинг – шпигунське програмне забезпечення, яке виступає у ролі кейлогера, що записує натискання клавіш на клавіатурі і передає своєму розробнику логін/пароль та іншу необхідну інформацію, коли виявляє, що користувач відвідує сайт (банку, магазину etc.), якому довіряє. На відміну від «класичного» фішингу, який може бути швидко виявлений і припинений правоохоронними органами, шпигунський може працювати місяцями, доки жертва не почне розуміти, що безпека її технічних засобів і особистих даних під загрозою.

Мета фішингових атак різна: крадіжка особистої інформації, встановлення шкідливого програмного забезпечення, контроль за персональним комп'ютером тощо.

2. Спам-листи – атака, із якою стикаються мільйони людей – невідомі адресату користувачі розсилають небажані листи на різні теми. ЗУ «Про електронні комунікації»¹, який набув чинності 01 січня 2022 р. визначає спам у п.118 ст.2 як «електронні, текстові та/або мультимедійні повідомлення, що без попередньої згоди (замовлення) користувачів неодноразово (більше п'яти повідомлень одному абоненту) надсилаються на їхні адреси електронної пошти або кінцеве (термінальне) обладнання, крім повідомлень постачальника електронних комунікаційних послуг щодо надання ним електронних комунікаційних послуг або повідомлень від органів державної влади чи органів місцевого самоврядування з питань, що належать до їх повноважень». Позитивною новелою цього закону стало й те, що ст. 120 «Захист кінцевих користувачів від спаму» «забороняється умисне масове розсилання електронних, текстових та/або мультимедійних повідомлень без згоди (замовлення) кінцевих користувачів (спаму)».

¹ Закон про електронні комунікації ст.2 2020 (Верховна рада України). Офіційний сайт Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/1089-20> (дата звернення: 27.07.2021).

Попри наявність легального визначення зміст поняття «спам», з урахуванням його багатогранності, легше зрозуміти, визначивши основні характеристики: 1) надсилається в електронному вигляді, однак, не обов'язково обмежується електронною скринькою, а, наприклад, може надсилатися за допомогою SMS або месенджерів; 2) особа відправника зазвичай прихована за заголовком листа або вигадана – спамери рідко використовують власні облікові записи, таким чином атаки складніше відфільтровувати і викрити невідомого відправника; 3) електронна адреса або номер мобільного телефону використовується без згоди власника; разом з тим 4) відправник не має діючої адреси або іншого контакту, на який користувач може надіслати повідомлення із вимогою припинення розсилання спаму; 5) може містити незаконні (шахрайство, порнографія) елементи або бути спрямованим на встановлення шкідливого програмного забезпечення; 6) розсилається масово, інколи декілька разів (повторно). Метою спам-повідомлення може бути завантаження вкладення користувачем-адресатом чи перехід за посиланням, яке містить шкідливе програмне забезпечення; агресивний маркетинг; шахрайство; продаж особистої інформації.

Характеризуючи соціально-технічну інженерію як метод інформаційно-технічної війни слід відзначити, що професіоналізм кібервоїнів повсякчас зростає, а дії кібервоїнів часто бувають структуровані – фішинг і спам «воюють» разом як піхота й артилерія: роль спамера полягає у зборі електронних адрес для створення списку потенційних жертв і розсилання їм спам-листів із закликом відвідати ту чи іншу компанію/організацію/магазин тощо; фішер займається пошуком «вразливих» серверів. Електронні листи формулюються таким чином, щоб переконати отримувача відкрити вкладення чи перейти на спеціально створений сайт. Фішер використовує зібрані дані для купівлі товарів, переведення сум, чи як «міст» для подальших атак.

Четвертий метод – встановлення шкідливого програмного забезпечення без згоди власника. Метою встановлення шкідливого програмного забезпечення може

бути: відслідковування і пересилання даних облікового запису (імена користувачів, паролі); зміна, шифрування чи знищення даних; інтеграція у мережу ботів і їх незаконне використання для DDoS-атак; несанкціоноване віддалене керування ІТ-системою.

Попри те, що функціональні можливості шкідливого програмного забезпечення відрізняються, воно в усіх випадках використовує інформаційно-технічну систему для цілей, на які законний користувач не давав згоди: крадіжка повідомлень у месенджерах; доступ і перевірка до закладок й історії браузерів; запис аудіо; запис телефонних розмов; зйомка через фронтальну чи задню камеру; крадіжка фото і відео; моніторинг місцезнаходження за GPS; крадіжка sms-повідомлень; крадіжка телефонних контактів і даних журналів виклику; відслідковування натискання клавіш; перевірка файлів на жорсткому диску; перегляд застосунків на робочому столі; крадіжка номерів карт, паролів, іншої особистої інформації.

Джерела розповсюдження можна розділити на дві категорії: 1. Перший і найбільш популярний спосіб це установка самим користувачем, шкідлива програма може міститися у легальному ПЗ, часто безкоштовному. 2. Перехід за посиланнями, яка містить код установлення шкідливого програмного забезпечення відбувається примусове установлення шкідливого програмного забезпечення.

До видів шкідливого програмного забезпечення відноситься:

1. Шпигунське програмне забезпечення – повністю невидимі комп'ютерні програми, які встановлюються з метою передачі інформації про користувача третім особам без його згоди. Шпигунське ПЗ – одна із найбільш зростаючих загроз інформаційній безпеці. Шпигування часто передуює іншим формам кіберзагроз. Встановлення цієї програми сповільнює роботу комп'ютера і часто відповідальне за впливання нав'язливої реклами. Зазвичай воно використовується для «агресивного» Інтернет-маркетингу. Ця програма відслідковує поведінку при переглядів веб-сторінок– аби дізнатися про звички споживача, його переваги з

метою оптимізації цільової реклами, рідше – з метою заволодіння особистими даними для їх незаконного використання і відображає рекламу. Цікаво, що є цілі компанії, які продають шпигунське програмне забезпечення виключно урядам різних країн¹. Кібершпигування використовується для викрадення промислових секретів з метою недобросовісної конкуренції чи стратегічної переваги (зразки військового обладнання).

Наявність у IT-системі шпигунського програмного забезпечення знижує продуктивність і якість роботи комп'ютера. Прикладом такого програмного забезпечення є «CoolWebSearch», яке замасковане під рекламне ПЗ і здатне самостійно встановлюватися на комп'ютер, відомими шпигунськими програмами є Gator, PurityScan. Наприклад, програма 180 Solutions надає рекламодавцям повну інформацію про відвідувані веб-сайти. HuntBar (а / к / а WinTools) чи Adware.Websearch розповсюджується Traffic Syndicate і встановлюється через завантаження ActiveX на його партнерські сайти. Це приклад того, як одне шпигунське ПЗ встановлює інші шпигунські ПЗ.

Відмінним, за змістом, але часто схожими за цілями із шпигунським програмним забезпеченням є «бекдори» – це форма атак, за якої у систему вбудовуються сторонні алгоритми, що дозволяє отримати несанкціонований доступ і можливість управління системою. Відомі бекдори BackDoor.DNS.ep, BackDoor.Cotx, BackDoor.Skeye.1 etc. Бекдори можуть бути компонентами шкідливого програмного забезпечення – наприклад, «серед компонентів ESPECTER (шкідливого програмного забезпечення – курсив наш) бекдор, який містить великий набір команд і можливості автоматичного перехоплення даних, включно із

¹

[Marczak B., Scott-Railton J., Berdan K., Razzak B.A., Deibert R., Hooking C. Another Mercenary Spyware Vendor Comes into Focus. The citizen lab. URL: https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/](https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/) (дата звернення: 05.11.2021).

викраденням документів, зчитування натисків клавіатури і періодичне створення знімків екрана жертви. Усі зібрані дані зберігаються у прихованому каталозі»¹.

2. Вірусне програмне забезпечення, відзначимо, що під комп'ютерним вірусом розуміється «програма, що розмножується та поширюється самочинно. При цьому комп'ютерний вірус може порушувати цілісність інформації, програмне забезпечення та режим роботи обчислювальної техніки»²:

- 1) макровірус це різновид вірусів, що розповсюджується через документи застосунків, які мають засоби для виконання макрокоманд (Word, Excel);
- 2) поліморфний – це різновид вірусів, які застосовують різноманітні способи шифрування власного тіла. У разі зараження чергового файлу алгоритм шифрування змінюється випадковим чином. При цьому дуже важко виділити сигнатуру – характерну послідовність байтів у коді вірусу³;
- 3) стелс-віруси маскують свою присутність в місці існування шляхом перехоплення звернень операційної системи (ОС) до уражених файлів, секторам і переадресовують ОС до незаражених ділянок інформації. Вірус є резидентним, маскується під програми ОС, може переміщатися в пам'яті⁴;
- 4) троянський кінь зазвичай маскується під законне програмне забезпечення. Свого часу він маскувався, наприклад, під оновлення Adobe Flash. У подальшому троянські коні можуть відкривати ботнет аби відкривати дорогу програмам-користувачам, наприклад, відомим є Kilim. Спрощеною формою троянського коня є «вірус-крапельниця», «програма-укол»; 5) логічна бомба; 6) комп'ютерний

1

Буткит UEFI как инструмент для кибершпионажа. Eset. ERL: <https://eset.ua/ru/news/view/913/butkit-UEFI-kak-instrument-dlya-kibershpiionazha> (дата звернення: 01.12.2021).

² ДСТУ 3396. 2-97. Захист інформації. Технічний захист інформації. Терміни і визначення. Київ : Держстандарт України, 1998. 16 с. 3. Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека. Термінологічний навчальний довідник. Київ : Издатель ООО «Д. В. К.», 2002. С. 4.

³ Технології захисту інформації : лекція. С.10. *Ужгородський національний університет*: веб-сайт. URL: <https://www.uzhnu.edu.ua/uk/infocentre/get/4186> (дата звернення: 29.10.2021).

⁴ Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. С. 75.

черв'як є пасивною програмою, яка розповсюджується без втручання користувача, так, Koobface викрадає інформацію. Як і троянські коні здатні створювати ботнет.

До вірусного програмного забезпечення можна віднести:

а) програми-вимагачі, які блокують системи і вимагають викуп за розблокування під загрозою оприлюднення або видалення даних, найчастіше оплату вимагають за дешифрувальний ключ. Існують різні види програм-вимагачів:

а) програма-шантажист – вона не блокує сам жорсткий диск, а блокує доступ до нього;

б) програми-вимагачі, які блокують дані, цей вид має великий потенціал нанесення збитків зацікавленим особам, оскільки це шифрування складно здолати, крім того, сплата грошової суми, яка вимагається часто не призводить до розблокування зараженої системи;

в) програми-очисники найбільш небезпечні з усіх «вимагачів», адже, у них відсутня функція розблокування і відновлення даних недоступне у системі навіть після сплати грошової суми; дані стають непридатними для використання і знищуються остаточно. Одним із найбільш шкідливих серед програм-вимагачів є програми-вимагачі GandCrab, Cerber, Conti, Ryuk тощо. Відомою також є програма REvil, створена однойменною хакерською групою. У жовтні 2021 р. з'явилося повідомлення про припинення діяльності цього угруповання, що було відповідальне за атаки на одного з партнерів Apple, компанію Quanta, постачальника м'яса JBS S.A., владу Техасу, ІТ-компанію Kaseya та багато інших гучних інцидентів. Деякі із них встановлюються за допомогою інших інструментів, наприклад, CryptXXX розповсюджується через троянського коня Bedep.

г) програми для крадіжки інформації, такими, наприклад, є AZORult – програма для крадіжки інформації, яка використовує різні цифрові ідентифікатори; njRAT – інструмент віддаленого доступу, який записує натискання клавіш (кейлогінг) і надає третім особам доступ до мікрофону і камери.

г) рекламне – призначене для того, аби на екрані користувача з'являлося якомога більше реклами. Лише на перший погляд може здатися, що ця реклама потрібна суто для того, аби привернути увагу (а частіше – подратувати користувача) – часто перехід за рекламним посиланням може привести до веб-сайту, що містить шкідливе програмне забезпечення.

З метою приховування шкідливого програмного забезпечення використовуються маскувальники – руткіти (RootKit). Самі руткіти не є шкідливими для комп'ютерної системи, натомість, вони маскують свої сліди або від антивірусного програмного забезпечення, або від засобів захисту від руткітів, що дозволяє зловмиснику тривалий час працювати віддалено¹.

Зусилля кібервоїни спрямовані на системне вторгнення, яке може призвести до знищення інформації, незаконного отримання інформації, несанкціонованої зміни даних можуть супроводжуватися фінансовою вигодою. Крім того, за допомогою методів інформаційно-технічної війни можуть бути виконані такі завдання як: 1) контроль доступу (ідентифікація, аутентифікація та авторизація); 2) порушення цілісності інформаційної системи; 3) закриття доступу власнику.

Отже, інформаційно-технічна зброя націлена на збір конфіденційної інформації, доступ до мережі, може погіршувати роботу мережі, у тому числі призводити до відмови роботи усього сервісу, погіршувати або змінювати роботу одного чи декількох вузлів мережі, активізувати шкідливий код.

Висновки до 2 розділу

Інтегральне розуміння інформаційних війн передбачає два її спрямування, два види – інформаційно-психологічну та інформаційно-технічну.

¹ [Muthumanickam K., Ilavarasan E.](#) CoPDA: Concealed process and service discovery algorithm to reveal rootkit footprints. *Malaysian Journal of Computer Science* 28(1):1-15, 2015. URL: bit.ly/3sJM3gI (дата звернення: 11.11.2021).

До елементів, що формують політичну платформу інформаційно-психологічної війни, перш за все, належить теорія комунікації, однак, основою будь-якого спілкування є мова, а відтак, при дослідженні інформаційно-психологічної війни неможливо ігнорувати лінгвістичні аспекти, які найбільш яскраво проявляються у пропагандистських, дезінформаційних текстах. Інформаційно-психологічна війна, що може знаходити своє вираження у політичному дискурсі найбільш яскраво знаходить своє відображення у масовій пропаганді.

Серед найчастіше вживаних мовностилістичних засобів інформаційно-психологічної війни: риторичні (мовні) фігури; ідеологеми; міфологеми; інфологеми; метафори; пейоративи; неологізми; евфемізми; гіперболізація. В окремих випадках інформаційно-психологічна війна супроводжується наявністю певної символіки, гасел із стилістичними і риторичними властивостями і специфічними способами звернення.

Адресантами інформаційно-психологічної війни можуть бути як державні, так і недержавні суб'єкти. Адресатами інформаційно-психологічної війни є маси, оскільки інформаційно-психологічна війна – складова політичних комунікацій і масових комунікацій.

Об'єктом впливу інформаційно-психологічної війни є психічна діяльність людини чи груп людей. Метою інформаційно-психологічної війни можна вважати виклик певних емоційних реакцій для досягнення конкретних поведінкових результатів. До каналів або засобів інформаційно-психологічної війни можуть відноситися: 1) Інтернет-ресурси: сайти, блоги, соціальні мережі; 2) візуальні і звукові носії: телебачення, радіо, кінотеатр, документальні фільми, пісні, новини, ток-шоу; 3) промови: концерти, особисті зустрічі із великою аудиторією, політичні події; 4) мистецтво: картини, плакати; 5) преса і література: брошури, книги, газети, журнали.

Підходи до наповнення інструментарію інформаційно-психологічної війни не характеризуються догматизмом, а мають декілька версій та інтерпретацій. На наш погляд, до методів інформаційно-психологічної війни слід віднести *дезінформацію*, яка є більш широким терміном, ніж популярний *fake news*, пропаганду та теорії змов, хоча теоретичні підходи до розуміння і переліку методів ще підлягатимуть глибокому аналізу, оскільки досі спостерігається семантична плутанина у різних термінах та значеннях.

Не меншу складність викликає розуміння «інформаційно-технічної війни» («кібервійни»). Перспектива глобальних «кібервійн» – відкрила нові сценарії загроз, які тепер існують паралельно із можливістю ядерного знищення людства: за цією логікою, існує загроза знищення цивілізації через руйнування критичної інфраструктури.

Ідейне поле у цьому контексті можна умовно розділити на два табори: 1) кібервійна існує; 2) кібервійна – це певна умовність, так, у Таллінському мануалі, яке присвячене цьому явищю, робиться уточнення, що «кібервійна» вживається у чисто описовому, а не нормативному сенсі.

Небезпечної «мілітаризації» кіберпростору, на наш погляд, ще не досягнуто, а часте використання терміна «кібервійна» для позначення всіх політично-мотивованих кібератак видається дещо перебільшеним, хоча, кожен такий випадок безсумнівно вказує на вразливість життя суспільства у цифрову епоху.

Серед особливостей кібервійни виділимо наступні: 1) це війна між суверенними державами, яка ведеться за допомогою кіберзброї; 2) кібервійна як становище у кіберпросторі тісно межує із кіберзлочинністю, кібершпигуванням, що робить розмитим її межі; 3) кібервійна може бути частиною збройного конфлікту, як міжнародного так і внутрішнього.

Об'єктом кібервійни є інформаційно-технологічна система. Суб'єктом є кібервоїн (хакер), який прагне задовольнити своє еґо або отримати фінансову винагороду; отримати визнання в очах своїх колег, задовольнити цікавість; для

нього участь в інформаційно-технічній війні може виступати і як перевірка власного інтелекту, і як виклик державам; або ж, навпаки, це може бути виконання конкретного замовлення окремих компаній, переслідуючи мету грошового прибутку, чи іноземних держав, для досягнення ними конкурентної переваги (наприклад, економічної) тощо.

Серед особливостей інформаційно-технічної війни можна виділити: економію ресурсів і фінансів; наявну проблему тактичного попередження і оцінки атак; розмиті кордони – значення географічних меж нівелюється під впливом зростання ролі інформаційної інфраструктури, протиборство відбувається у віртуальному просторі – кіберпросторі, який характеризується: анонімністю, швидкою атакою «звідусіль» і є додатковою вразливістю для національної безпеки держави.

До збройного арсеналу інформаційно-технічної зброї, яка націлена на збір конфіденційної інформації, доступ до мережі, може погіршувати роботу мережі, у тому числі призводити до відмови роботи усього сервісу, погіршувати або змінювати роботу одного чи декількох вузлів мережі, активізувати шкідливий код належить чотири основних методи. Першими є атаки спрямовані на перевантаження ресурсу запитами, аби вичерпати його фільтрувальну здатність – такі дії призводять або до сповільнення, або до зупинки роботи інформаційної системи. Другим є метод міжсайтового скриптинг (XXS) пов'язаний із вразливістю веб-сайтів. Третім є метод соціально-технічної інженерії. Четвертий метод – встановлення шкідливого програмного забезпечення без згоди власника.

РОЗДІЛ 3. СПЕЦИФІКА ІНФОРМАЦІЙНОЇ ВІЙНИ РФ ТА УКРАЇНСЬКІ СПОСОБИ ПРОТИДІЇ

2014-2022 рр. стали для України особливо випробувальними на інформаційному фронті, а із 24 лютого 2022 р. інформаційна війна стала невід’ємною складовою повномасштабної російсько-української війни. Росія розгорнула її у безпрецедентних масштабах – і внутрішніх, спрямованих на власне населення, і зовнішніх – з метою впливу на суспільну думку в Україні та відчайдушних пошуків союзників за кордоном. Так, пропаганда шириться через офіційні кремлівські канали, такі як Russia Today і Sputnik, які ведуть мовлення і публікують твіти на декількох мовах (із початком повномасштабного вторгнення це стало робити дещо складніше, оскільки ряд країн заблокували мовлення). Ці канали не лише повторюють прокремлівські тези, але й звертаються до усіх тих, хто підтримує політику Росії за кордоном.

Крім того, ще до повномасштабного вторгнення Росія часто крім пропаганди та дезінформації використовувала з метою впливу на іноземну аудиторію м’яку силу. Прикладом м’якої сили може слугувати російська медична допомога Італії, Сербії під час пандемії Covid-19. Задача у неї була двояка: продемонструвати схильність Росії і підтримати ідею про нездатність європейських лідерів зупинити кризу у галузі охорони здоров’я разом з тим звернувши увагу на те, яке значення Росія має у цьому типі міжнародного кризового управління.

Найбільш помітним наданням гуманітарної допомоги Росії стала доставка медичного обладнання у північну Італію в березні 2020 р. під лозунгом «Із Росії з любов’ю». Російські ЗМІ показали кадри проїзду військової техніки: в Італію було відправлено військових спеціалістів Міністерства оборони РФ. Російські ЗМІ широко трансливали дві символічні сцени: з одного боку, консультація італійських і російських офіцерів в одному штабі італійської армії під Римом, з іншого боку, колонна російської військової техніки маршрутом Рим-Бергамо. Цей захід, безпрецедентний для країни НАТО можна розцінювати по-різному:

ніби простий вираз російської допомоги, яка підпадає під дію м'якої сили, і в той же час демонструє візуально жорстку силу. Якоюсь мірою це і засіб впливу на італійський уряд, аби досягнути більшої схильності до російських інтересів, особливо у відношенні європейських санкцій проти Росії. Італійська щоденна газета «*LaStampa*» припустила, що справжньою метою була розвідка, у зв'язку з чим, розгорнувся цілий спір із офіційним представником Міністерства оборони Росії, який зазначив, що видання у цій статті «маніпулює русофобними фейками»¹.

Щодо України стратегія інформаційної війни реалізовується сучасними способами – широким простором можливостей інформаційно-психологічної війни: повторенням пропагандистських наративів, інколи ізольованих, логічно нееквівалентних та нераціональних суджень ЗМІ та армією політичних ботів, які покликані впливати на чутливих і довірливих людей (фейки – їх основний інструмент). Частим стало активне розповсюдження дезінформації – дезінформаційна практика покликана спотворити історію: тут і специфічне російське бачення історичної належності Криму, міти про «один народ», «заснування Одеси Катериною II», і стирання дистанції між війною та миром: від «нас там нет» у 2014 р. до «Захід почав першим» у 2022 р., аби інші засумнівалися у власному правильному розумінні.

Крім офіційної пропаганди та інших використовуваних методів, варто виділити декілька категорій акторів інформаційно-психологічної війни, які сприяють більш аргументованій популяризації тез на фоні російсько-української війни: 1) це добре відомі, «хороші» росіяни, які стоять на сторожі умиротворення, як спадкоємці пацифістів часів холодної війни; сюди ж можна віднести тих, хто наївно, щиро (чи ні) вважають, що переговори із Росією дозволять взяти ситуацію

¹ Le accuse di Mosca e la nostra risposta. *La Stampa*. URL: bit.ly/3ZejW5F (дата звернення: 02.02.2021).

під контроль. Вони вважають себе реалістами і прагматиками, але їх реалізм зводиться до неможливості боротися із «другою армією світу» (цей політичний міт уже розвінчано). Їх пропаганда спрямована на те, щоб посіяти сумніви в ліберальних цінностях і відмінити санкції «хорошим» росіянам, які самі є жертвою тоталітарного режиму, «нічого не можуть зробити», але не повинні страждати і нести відповідальність за дії режиму; 2) «помірковані», що балансують між двома сторонами, для них недоліки завжди врівноважуються, а «захід не завжди правильно вчиняв із Росією»; 3) не можна не згадати тих, чий антиамериканізм і сентиментальна ностальгія за СРСР влучно доповнюють лінію інформаційно-психологічної війни.

Про усіх них ми знаємо з Інтернету, який став справжньою платформою інформаційно-психологічної війни, адже, в інформаційній війні ефективність заснована на обміні, а не на приховуванні інформації. Фактором ефективності пропагандистського чи дезінформаційного повідомлення є його видимість у мережі, яка зазвичай досягається віральністю. В основі видимості два фактори: ранжування повідомлення у пошукових системах або його закріплення у соціальних мережах (наприклад, телеграм-каналах) та його цитування іншими сайтами і користувачами, які діляться контентом у соціальних мережах, що сприяє його швидкому розповсюдженню – контент стає віральним. І ось уже велика частина Інтернет-спільноти спостерігає за істерикою бабусь із Загонів Путіна і хлопцем з Хмельницького, який «вважає, що Україна повинна бути у складі РФ, СРСР або Російської імперії – як вийде»¹.

На разі платформа розгортання інформаційно-психологічної війни може варіюватися від популярних (велика кількість підписників) блогів до майже

¹ На Хмельниччині СБУ викрила прихильника Шарія на закликах до підтримки окупантів. Служба безпеки України: Youtube-канал. URL:

https://www.youtube.com/watch?v=sxeYbWehGoA&ab_channel=%D0%A1%D0%BB%D1%83%D0%B6%D0%B1%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8 (дата звернення: 04.03.2023).

анонімних. Однак, інформація із «камерного блогу» може швидко розповсюдитися і віртуальне сарафанне радіо рознесе потрібне для звернення до емоцій широкого кола користувачів Інтернету повідомлення.

Інтернет дозволяє для кожного адресата створювати свій контент: 1) для послаблення волі ворога, створюються веб-сайти чи сторінки у соціальних мережах, спрямовані на громадян держави, із якими ведеться боротьба, часто їх мета – посіяти жак, наприклад, розповсюджуючи контент у вигляді відео страт чи нападів, демонстрація зброї; 2) робота із схильною аудиторією ведеться із наголосом на потенційну цінність отримання результату, такого як забезпечення громадської безпеки; вказівкою на тих, кого варто боятися; 3) робота із «нейтральною» аудиторією забезпечується масштабуванням потрібної інформації, яке відбувається за лінгвістичним критерієм: різні мови – більше впливу.

Разом з тим, суттєвою перевагою Інтернету є можливість документування поля бою у режимі реального часу, у тому числі, цивільним населенням. Facebook, Twitter, YouTube, Telegram відкривають можливості для масової комунікації, а отже і протидії інформаційній агресії Росії.

Можливості оборони в інформаційно-психологічній війні РФ – питання, що намагалося знайти своє вирішення у науковій літературі: Г.В. Сасин ще у 2015 р. у своїй науковій роботі відзначала, що «Для захисту інформаційного простору та національної безпеки України необхідним є: зміна інформаційної політики (як зовнішньої, так і внутрішньої) ...просування української інформації на територію агресора, використовуючи при цьому сучасні технології; здійснення обмеження російської інформації...контроль іноземних ЗМІ, які акредитовані та функціонують на території України; сприяння розвитку вітчизняних інтернет-ресурсів...; збільшення якості та кількості українського продукту (цікаві телепрограми, друкована продукція тощо); здійснення діяльності в інформаційному та віртуальному просторі...; контроль донесення правдивої інформації до споживача...; блокування інтернет-ресурсів, які є загрозливими для інформаційної безпеки держави;

стимулювання наукових досліджень щодо державної інформаційної політики та безпеки; вдосконалення рівня підготовки фахівців у галузі інформаційної безпеки»¹.

У дослідженнях приділялася увага і протидії окремим методам інформаційно-психологічної війни. Так, наприклад, *В.І.Маляренко констатувала, що: «...універсальних рецептів боротьби з фейками досі не існує. Загальновизнаним залишається орієнтація на те, що еталоном захисту від деструктивної пропаганди та маніпуляції свідомістю людини є передусім міцність демократичних традицій кожного суспільства...»*. На думку М.В.Маркової, «в арсеналі сучасної людини існують різноманітні способи протидії ІПВ, серед яких максимально простими є критичне осмислення інформації, формування навичок позитивного мислення, інтелектуальна й фізична активність...»².

На наш погляд, протидія інформаційній агресії РФ полягає не тільки у безвтомному і невпинному виправленні брехні і спростуванні сфабрикованих наративів, а також просування послідовного і позитивного дискурсу, заснованого як на правді, так і на цінностях, що принципово розрізняють демократію і диктатуру, демонструють привабливість проукраїнської моделі. Недостатньо реагування, потрібні нові правила, власний проукраїнський дискурс, по суті, розгортання інформаційної війни проти РФ не лише в аспекті оборони, але й контрнаступу. Розглянемо, що уже втілено на другому році повномасштабної російської агресії, адже, парадокс полягає у тому, що країна на яку напали повинна робити більше, ніж агресор, аби продемонструвати свою правоту.

По-перше, відбувається невпинне виправлення і встановлення фактів щодо російського вторгнення. Так, названі російськими пропагандистами фейками страшні події у Бучі 2022 р., документування військових злочинів Росії, зроблено українською владою разом із західними партнерами.

¹ Сасин Г.В. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на кприкладі російської експансії в український простір). *Грані*. 2015. №3 (119). С. 18-23.

² Маркова М.В. Інформаційно-психологічна війна: медико-психологічні наслідки та стратегії протидії. *Проблеми безперервної медичної освіти та науки*. 2016. №4. С.6-10.

По-друге, українські наративи зводяться до: 1) благородної справи самооборони країни; 2) варварства російського вторгнення; 3) нестійкості і необґрунтованості російської військової стратегії. Важливою у цьому аспекті є робота Центру протидії дезінформації при РНБО України (7 травня 2021 року Президент України Володимир Зеленський підписав Указ № 187/2021 «Питання Центру протидії дезінформації», яким затвердив Положення про ЦПД).

Центр протидії дезінформації при РНБО України згідно Указу Президента України № 187/2021 «Питання Центру протидії дезінформації»: «забезпечує протидію як наявним, так і прогнозованим загрозам нацбезпеці та національним інтересам в інформаційній сфері, виявляє та протидіє дезінформації, пропаганді, деструктивним інформаційним впливам і кампаніям, а також має запобігати спробам маніпулювання громадською думкою». Центр займається і просвітницькою роботою, так, на сторінках сайту можна знайти пояснення термінів найбільш придатних до використання щодо російської аудиторії «псевдопатріотизм як деструктивна ідеологія РФ», «псевдоевакуація як механізм терору», «емоційний фейк» тощо; механізмів, наприклад, «ЦПД пояснює, як працює механізм хибної аналогії в дезінформації» та принципів, наприклад, «ЦПД пояснює як працює принцип «психологічного шоку» в дезінформації».

Важливим кроком стало і прийняття закону «Про внесення змін до деяких законодавчих актів України (щодо заборони виготовлення та поширення інформаційної продукції, спрямованої на пропагування дій держави-агресора)» від 3 березня 2022 р., яким було внесено зміни до низки законів України і: «встановлення в них заборон щодо: виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України у 2014 р., у тому числі, шляхом представлення збройної агресії Російської Федерації проти України, як «внутрішнього конфлікту», «громадянського конфлікту», «громадянської війни», заперечення тимчасової окупації частини території України; глорифікації осіб, які здійснювали збройну агресію Російської Федерації проти України у 2014

році... у тому числі, шляхом їх визначення як «повстанці», «ополченці», «ввічливі військові люди»; встановлення санкції для релігійної організації у вигляді припинення діяльності у разі встановлення судом фактів вчинення релігійною організацією дій, спрямованих на: ліквідацію незалежності України, зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності держави...; поширення відомостей, що містять виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, розпочатої у 2014 році тощо».

По-третє, розвінчування підступних принижувальних дискурсів щодо історичних фактів: маси погано знають історію і часто повторюють тези із російської пропаганди.

Робота у напрямі встановлення історичної правди, нагадування фактів, а також систематична відповідь, у тому числі на політичному рівні.

Нагадування фактів відбувається аби протистояти псевдореалістичному дискурсу і показати його небезпеку. Не дивлячись на той факт, що утворення України випередило створення Російського царства на декілька століть, президент Росії регулярно відкидає той факт, що Україна – повноцінна нація. Ці твердження на кшталт «Украину создал Ленин в 1922» стали лейтмотивом у спробах позбавлення України права на незалежність, якщо не на існування. Відзначимо, що навіть політика СРСР була не настільки категоричною і Україна як держава із віковими традиціями визнавалася: так, у газеті «Радянський патріот» 1979 р. є стаття із заголовком «Испытанная в веках. К 325-летию воссоединения Украины с Россией»¹, хоча історія, подана у ній, безумовно, спотворена.

¹ Збанацкий Ю. Испытанная в веках. К 325-летию воссоединения Украины с Россией. *Советский патриот*. 1979. 10 января. С.2.

По-четверте, безумовно, демократії не повинні мовчати перед лицем своїх противників. Лідери повинні реагувати на кожного, хто виступає проти цінностей свободи.

Особа президента В.Зеленського відіграє не останню роль в цій інформаційній війні, адже він регулярно надає правдиву версію війни і розвінчує російські міфи, а його відео із прямих етерів перших днів війни стали символом хоробрості і національної єдності. Інформаційна війна, розв'язана уже проти РФ повинна виявити справжню жертву цієї війни, якою є Україна й агресора, який повинен заплатити за своє вторгнення. Разом з тим, на думку О.Чачко та К.Лінос «війна в Україні вдихнула таку необхідну енергію в міжнародну систему норм та інститутів, яка багато в чому втратила свою силу»¹.

По-п'яте, поступове вирішення питання монументальної пропаганди.

Пам'ятник – один із способів донести ключові політичні ідеї до мас, це політично умотивована ікона, що у руках російської пропаганди покликана заплутати людей, як це було, наприклад, в Одесі із пам'ятником Катерині II, яка символічно закріпила приналежність міста до Росії, що не відповідає дійсності, однак, міцно вплелось у реальність навіть містян. Тому знищення візуальних образів державних діячів, що або дуже умовно, або взагалі не відносяться до країни, або є символом її імперського чи радянського минулого видається одним із ефективних способів протидії російській інформаційно-психологічній війні.

Серйозну проблему для України становлять російські кібератаки і це, крім того, що на окупованих територіях Росія спрямувала інтернет-трафік через власні точки мережевої взаємодії. Л. Машмайер та М.Кавелті, відзначають: «перед вторгненням Росії в Україну ряд експертів передбачали кібервійну: масове використання російських наступальних кіберможливостей, аби «шокувати і залякати» обороноздатність України і підірвати її волю до війни. Деякі навіть

¹ Chachko E., Linos K. International Law After Ukraine: Introduction to the Symposium. *AJIL Unbound*. 2022. Vol. 116. P.124-129.

вважали, що Росії не потрібне вторгнення, що вона може досягнути тих самих результатів завдяки кібервійні. Коли цього не відбулося, ті ж експерти передбачали, що Росія все ж застосує наступальні кіберможливості не лише проти України, але й проти Заходу і його критичної інфраструктури як покарання за санкції і підтримку України...Деякі говорять, що мали рацію і кібервійна тут, за винятком того, що загрозу в Україні стримали і кібератаки було вчасно нейтралізовано»¹.

Потрібно відзначити, що Росія має неабиякий кіберпотенціал і досвід у нанесенні кібератак. Наприклад, атаки за типом DDoS, зокрема, було застосовано в Естонії у 2007 р. при кібернападі на сайти державних і приватних організацій, великих банків та парламент на фоні загострення відносин між Росією та Естонією у зв'язку із перенесенням пам'ятника радянським воїнам (неофіційна назва – «Бронзовий солдат») у Талліні. Естонія – одна із найбільш комп'ютеризованих країн була виведена із ладу. Хоча, країна не понесла втрат чи фізичного руйнування критичної інфраструктури, а лише її блокування, це перший випадок, коли країна член НАТО попросила застосувати ст.5 Договору НАТО після кібератаки на власні цифрові структури.

Російська влада традиційно відкидала усі звинувачення, а Естонія вбачаючи у діях збройний напад, вимагала застосування доктрини взаємного захисту за ст.5 Північноатлантичного Договору: «...збройний напад на одну або кількох із них (сторін Договору) у Європі чи у Північній Америці вважатиметься нападом на них усіх: і, відповідно, вони домовляються, що в разі здійснення такого нападу кожна з них, реалізуючи своє законне право на індивідуальну чи колективну самооборону, підтверджене Статтею 51 Статуту Організації Об'єднаних Націй, надасть допомогу тій Стороні або Сторонам, які зазнали нападу, і одразу здійснить,

¹ Maschmeyer L., Cavelty M. Goodbye Cyberwar: Ukraine as a reality check. *Policy perspectives*. 2022. Vol.10/3. URL: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/549252/PP10-3_2022-EN.pdf?sequence=2&isAllowed=y (дата звернення: 01.03.2023).

індивідуально чи спільно з іншими Сторонами, такі дії, які вважатимуться необхідними, включаючи застосування збройної сили, з метою відновлення і збереження безпеки у Північноатлантичному регіоні»¹. Застосування цієї статті відбувається у разі, якщо на критичну інфраструктуру члена НАТО нападуть і є підстави uważати, що під загрозою атаки може опинитися увесь військово-політичний альянс, у випадку з Естонією – відкинулося. Така позиція цілком обґрунтована, адже проблема цього документа у історичному періоді його прийняття – 1949 р., коли стратегічні загрози країнам-членам НАТО як і всім іншим державам були відмінними від існуючих сьогодні, у кібер-еру, а значення «збройного нападу» було цілком традиційним, зрозумілим і полягало у прямій загрозі територіальній цілісності країни зі сторони іншої країнами за допомогою збройних сил.

У 2008 р. на території столиці Естонії з'явився Центр співробітництва у сфері кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence) зі статусом військової організації, а документ «Таллінський мануал», попри те, що не має обов'язкової юридичної сили і є політично нейтральним, слугує важливим інструментом для політичних експертів, правників у практиці застосування міжнародного права у кіберопераціях².

У Вікіпедії стаття під назвою «Російсько-українська кібервійна» показує хронологію із 2013 р., а 28 лютого 2023 р. СБУ повідомила, що «російські хакери здійснюють кожного дня у середньому понад десять кібератак на Україну»³; типовими є також повідомлення на кшталт: «Кібератаки росіян були перенаправлені з військових цілей на комерційний, енергетичний, фінансовий,

¹ Північноатлантичний договір : міжнародний документ від 04.04.1949. *Офіційний портал Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/950_008#Text (дата звернення: 02.12. 2021).

² Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge : Cambridge University Press, 2017. 598 p.

³ Росія здійснює на Україну понад 10 кібератак за добу – СБУ. *Укрінформ: мультимедійна платформа іномовлення України*. URL: <https://www.ukrinform.ua/rubric-ato/3676108-rosia-zdijsnue-na-ukrainu-ponad-10-kiberatak-za-dobu-sbu.html> (дата звернення: 28.02.2023).

телекомунікаційний і державний сектори»¹; «42 кіберзлочини проти медіа Кібератаки, піратство, погрози, атаки на сторінки медіа в соціальних мережах... Інформаційна війна поширюється в Інтернеті. За рік було зафіксовано щонайменше 42 кіберзлочини. Останню кібератаку, яка була націлена на сайт українського інформаційного агентства «Укрінформ», пов'язують з хакерами, пов'язаними з ГРУ, російською службою військової розвідки»²; «Фахівці Держспецзв'язку протягом 2022 р. зареєстрували в Україні понад 2 тисячі кіберінцидентів та ще більшу кількість кібератак... ми зазнаємо постійних кібератак і достатньо ефективно протидіємо»³. Хоча, тези зарубіжних науковців дещо песимістичніші, ось що пише з цього приводу А.Мохі: «Уцілому, українські атаки носили рудиментарний характер й мали обмежений ефект. Україна страждає через відсутність досвіду в області кібербезпеки, поганого регулювання, обмежених можливостей реагування і відсутності координації між різними відомствами...З іншого боку – російський ведмідь, який перенасичений високоорганізованими, ефективними, передовими дослідницькими центрами фінансових і людських ресурсів кібербезпеки...»⁴.

Така інтенсивність може бути і складовою асиметричних кампаній, що спрямовані на буквальний завал противника брехливими атаками, аби вони виснажували ресурси, зниження здатності ресурсів працювати належним чином і відволікти їх увагу від важливих функцій, для захисту яких вони працювали, дослідники Стівен Дефібо та Донна Шеффер у дослідницькій роботі «Чи може

1

Росія за допомогою кібератак намагається тероризувати українців – Politico. УНІАН: інформаційне агентство. URL: unian.ua/techno/communications/rossiya-pri-pomoshchi-kiberatak-pytaetsya-terrorizirovat-ukraincev-politico-12106917.html (дата звернення: 06.03.2023).

² Україна. Рік інформаційної війни в цифрах. Reporters sans frontiers: веб-сайт. URL: https://rsf.org/sites/default/files/medias/file/2023/02/Un%20an%20guerre%20information_UKR.pdf (дата звернення: 06.03.2023).

³ Росія здійснює на Україну понад 10 кібератак за добу – СБУ. Укрінформ: мультимедійна платформа іномовлення України. URL: <https://www.ukrinform.ua/rubric-ato/3676108-rosia-zdijsnue-na-ukrainu-ponad-10-kiberatak-za-dobu-sbu.html> (дата звернення: 28.02.2023).

⁴ Mohee A. Cyber war: The hidden side of the Russian-Ukrainian crisis. SocArXiv : веб-сайт. URL: <https://osf.io/preprints/socarxiv/2agd3/> (дата звернення 01.03.2023).

теорія виснаження надати розуміння кібервійни?» проводять паралелі між тактикою виснаження у традиційній війні і кібервійні. На прикладі російсько-української війни простежується правильність тези науковців про те, що «існує чіткий зв'язок між звичайною війною і кібервійною. У деяких випадках видно інтеграцію кібервійни поруч із звичайною тактикою або як прелюдію до неї...».

Протидія інформаційно-технічній агресії РФ, яка, за влучним формулюванням у Стратегії кібербезпеки залишається «одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури»¹, відбувається завдяки суб'єктам національної системи кібербезпеки, основними з яких згідно ст. 8 ЗУ «Про основні засади забезпечення кібербезпеки України» є: Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, крім того, Указом Президента України від 7 червня 2016 р. № 242/2016 затверджено Положення про Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України, який здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку...(ч.2 ст.5 ЗУ «Про основні засади забезпечення кібербезпеки України»). Серед основних завдань Центру здійснення аналізу: стану кібербезпеки; результатів проведення огляду національної системи кібербезпеки; стану

¹ Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни»: затверджено указом Президента України від 26 серпня 2021 року №447/2021. *Верховна рада України: офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#n7> (дата звернення: 01.03.2023)

готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам, здійснення заходів щодо профілактики і боротьби з кіберзлочинністю тощо.

Відмітимо, що 28 липня 2022 р. було прийнято ЗУ «Про внесення змін до деяких законів України щодо забезпечення формування та реалізації державної політики у сфері активної протидії агресії у кіберпросторі», яким на Державну службу спеціального зв'язку та захисту інформації України покладено завдання «створення та забезпечення функціонування системи активної протидії агресії у кіберпросторі та створення та забезпечення функціонування Центру активної протидії агресії у кіберпросторі». Крім того, у 2023 році було прийнято ряд підзаконних нормативно-правових актів у сфері політики інформаційної безпеки, серед них виділимо: Постанову Кабінету Міністрів України «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» від 04.04.2023 р. №299, Постанову КМУ «Деякі питання функціонування Національного центру резервування державних інформаційних ресурсів» від 07.04.2023 р. №311, Постанову КМУ «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» від 16.05.2023 р. №570.

У контексті протидії кібервійні позитивним є збір людей і ефективна робота у кіберпросторі – ІТ армія.

У звіті із кібербезпеки відзначено: «За декілька років до російського вторгнення 24 лютого 2022 року в українських урядових колах крутилася принципова ідея створення кібердобровільної армії. Частково цим обговоренням сприяв успіх Кіберпідрозділу Кайтселіта Естонії та інші організації по всьому світові...ІТ-армія України – це гібридна конструкція, ні цивільна, ні військова, ні державна, ні приватні, два аспекти роботи: 1) заклик до дії, який мобілізує будь-кого, хто готовий брати участь у

скоординованих DDoS-атаках проти Росії 2) внутрішня команда, яка складається із українських сил оборони і розвідки задля експериментів і проведення більш складної кібероперації проти конкретних російських цілей носить наступальний характер»¹.

У кіберконфлікт залучено недержавні угруповання, більшість із яких – на стороні України, вони теж вважаються складовою ІТ-армії.

Висновки до 3 розділу

Процеси і спрямування сучасного світу знаходяться у розпорядженні інформаційно-комунікаційної та інформаційно-технічної сфер, важливість яких продовжує зростати, а нові, швидкі, інтенсивні відносини з інформацією не лише зручність і доступність, але й постійне напруження і загроза. Інформаційні війни не розмежовують воєнний і мирний час, стають тотальними, всеохоплюючими слугами політики де кожен вербує союзника, а кордони не зупиняють можливості їх розповсюдження.

Положення інформаційно-психологічної війни РФ невідривні від соціокультурного й історичного контексту, адже, часте звернення епох і виявлення їх ключових моментів виявляється доречним в сучасній ситуації – для мас і їх настроїв вербальні форми слугують ключами для викривлення когнітивного світу. Доповнюють картину популізм і емоційний пафос, який багато у чому перевищує раціональний контекст, медіа-хаос із гучними дисоснансними голосами й інколи відновленням уже підзабутих приспівів про «8 років бомбили Донбас», пропаганда – ірраціональна та софістична, із свідомим відкиданням чи ігноруванням фактуальності.

¹ Soesanto S. The IT army of Ukraine: structure, tasking, and eco-system. Cyberdefense report. Zurich. 2022. *ENT library*. URL: <https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/552293/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf?sequence=2&isAllowed=y> (дата звернення: 01.03.2023).

Інформаційно-психологічна війна РФ змушує російське населення діяти у певному напрямкові, залучаючи механізми переконання – ідеологічні та організаційні, артикулюється на основі «логіки» правдоподібності, а не істини.

Крім офіційної пропаганди та інших використовуваних методів, варто виділити декілька категорій акторів інформаційно-психологічної війни, які ведуть свою діяльність через соціальні мережі, що стали справжньою платформою інформаційно-психологічної війни.

Актори інформаційно-психологічної війни сприяють більш аргументованій популяризації тез на фоні російсько-української війни. До них відносяться добре відомі, «хороші» росіяни; сюди ж можна віднести тих, хто вважають, що переговори із Росією дозволять взяти ситуацію під контроль. Їх пропаганда спрямована на те, щоб посіяти сумніви в ліберальних цінностях і відмінити санкції «хорошим» росіянам, які самі є жертвою тоталітарного режиму, «нічого не можуть зробити», але не повинні страждати і нести відповідальність за дії режиму; «помірковані», що балансують між двома сторонами, для них недоліки завжди врівноважуються, а «захід не завжди правильно вчиняв із Росією».

Український спротив інформаційній агресії РФ зосередився на таких аспектах як невпинне виправлення неправдивої інформації, зокрема, і розвінчування підступних принижувальних історичних дискурсів і встановлення фактів щодо російського вторгнення, що є спільною роботою української влади і західних партнерів. Важливою у цьому аспекті є робота Центру протидії дезінформації при РНБО України (7 травня 2021 р. Президент України Володимир Зеленський підписав Указ № 187/2021 «Питання Центру протидії дезінформації», яким затвердив Положення про ЦПД), який, серед іншого займається і просвітницькою роботою, поясненням пропагандистських та дезінформаційних термінів та механізмів.

Важливим кроком стало прийняття Закону «Про внесення змін до деяких законодавчих актів України (щодо заборони виготовлення та поширення

інформаційної продукції, спрямованої на пропагування дій держави-агресора)» від 3 березня 2022 р.

Особа президента В.Зеленського відіграє не останню роль в цій інформаційній війні, адже він регулярно надає правдиву версію війни і розвінчує російські міфи, а його відео із прямих етерів перших днів війни стали символом хоробрості і національної єдності. Інформаційна війна, розв'язана уже проти РФ повинна виявити справжню жертву цієї війни, якою є Україна й агресора, який повинен заплатити за своє вторгнення.

Важливим є поступове вирішення питання монументальної пропаганди, адже, пам'ятники – один із способів донести ключові політичні ідеї до мас, це політично умотивована ікона, що у руках російської пропаганди покликана заплутати людей. Тому знищення візуальних образів державних діячів, що дуже умовно, або взагалі не відносяться до країни, чи є символом її імперського чи радянського минулого видається одним із ефективних способів протидії російській інформаційно-психологічній війні.

Однак, з огляду на масштаби, потрібно визнати, що РФ – країна не лише воїнів інформаційно-психологічного фронту, адже, серйозну проблему для України становлять російські кібератаки і це, крім того, що на окупованих територіях Росія спрямувала інтернет-трафік через власні точки мережевої взаємодії.

Зазначене вище однозначно свідчить, що час ізольованих мереж минув. На зміну цьому утворилося динамічне і складне середовище із інтелектуальних технологій і конвергованих мереж для переходу від однієї системи до іншої, що робить небезпечним кібератаку навіть на один пристрій. Найбільш небезпечними є комплексні російські кібератаки, що здатні паралізувати не лише функціонування систем державного управління і забезпечення основних послуг для громадян, але й мають потенційно руйнівні наслідки за типом збою критично важливої інфраструктури, атомних станцій, диспетчерських вишок, аеропортів, системи громадського транспорту.

Потрібно відзначити, що Росія має неабиякий кіберпотенціал і досвід у нанесенні кібератак, а кіберполітика стала новим способом ведення політики: діяльність держав стає усе більше віртуальною, а нерівний доступ до кіберсектора відображає розподіл потужностей держав на міжнародному рівні. Наслідки російської кіберактивності все ж менш відчутні, ніж результати традиційних військових дій: реалії російсько-української війни вкотре це підкреслюють, однак, забезпечення національної безпеки держави неможливе без звернення уваги на ризики, пов'язаних з можливостями інформаційно-технічної війни.

ВИСНОВКИ

1. Концепція інформаційної війни у контексті психологічної парадигми відома здавна, а сучасні методи інформаційно-психологічної війни дивовижно схожі на античні, з тією лише різницею, що тепер вони більш масштабні, глобальні і пагубні.

Тематичні дослідження інформаційних війн тривають у вітчизняній і зарубіжній науковій думці. Слід відзначити, що вони носять міждисциплінарний характер: до осягання теоретичних основ досліджуваного феномену звертаються політологи, психологи, соціологи, історики, медики.

Глибоке пізнання основ інформаційної війни попри різні погляди на її змістовне наповнення відбувається шляхом дослідження форм та методів.

Окремою науковою площиною стало вироблення способів протидії російській агресії на інформаційному фронті і у аспекті психологічної парадигми, і з точки зору інформаційно-технічної боротьби.

2. Об'єднана концепція інформаційних війн, що передбачає вивчення інформаційно-психологічного й інформаційно-технічного аспекту порівняно нечасто стає предметом наукових досліджень, оскільки більшість науковців тяжіють до психологічної парадигми, однак, на наш погляд, саме інтегральний підхід дає найбільш повне розуміння інформаційних війн.

На основі поліпарадигмального (комплексного, інтегрального підходу) пропонується розуміння інформаційних війн як комбінації людських або технологічних дій, призначених для присвоєння, видалення чи зміни інформації, що призводить до пошкодження або знищення критичної інфраструктури, порушення сталої роботи органів державної влади, економічних збитків у великих розмірах або порушення адекватного ментального сприйняття явищ і подій шляхом нав'язування певного бачення реальності. Попри об'єднувальне поняття, інформаційна війна має суттєву детермінацію, функціональну спрямованість на отримання різних

результатів. Вважається, що «інформаційна боротьба» й «інформаційне протиборство» можуть виступати синонімами «інформаційної війни», оскільки за критеріями ідентифікації понять якими можуть виступити історія, теорія і практика стає зрозумілим, що вони не мають історичних та категоріальних відмінностей і є однаковими з точки зору розгляду їх як політичного і соціального явища.

4. Невід'ємним атрибутом інформаційних війн є інформаційна зброя. Вона, на відміну від традиційного озброєння, не передбачає особливих умов зберігання і не виходить із ладу. Інформаційна зброя – інструмент, який, залежно від спрямування інформаційної війни може виражатися у певних методах. Збройний арсенал інформаційно-технічної війни програмно-математичний, а зброя інформаційно-психологічної війни вербальна або невербальна, у будь-якому разі – комунікативна.

5. Історичний досвід дозволяє побачити динаміку інформаційних війн та окремих її елементів, крім того, це дає розуміння сучасного стану і можливість уявити майбутні ризики.

Ретроспективна орієнтація дозволяє виокремити наступні періоди розвитку інформаційних війн. Перший етап розпочинається ще у архаїчні (стародавні часи). Важливе значення у можливості ведення перших форм інформаційно-психологічної війни мало створення писемності. Інформаційно-психологічна війна у давні часи була невід'ємною складовою військового конфлікту – її дію було спрямовано на підняття бойового духу, здатності активно чинити опір, зменшення власних матеріальних та фізичних втрат чи послаблення волі ворога. Це найбільш тривалий етап, який охоплює і часи Середньовіччя, коли поява друку дозволила розповсюджувати газети, листівки, і Добу Просвітництва. Другий етап простягається із сер. XIX ст., яке охоплювалося появою нових способів доставки інформації, що пов'язано із винайденням електрики (фотографії, телеграфу, радіо тощо). Третій етап розпочинається із поч. XX ст., яке охоплювалося войовничістю й існуванням біполярного світу холодної війни.

Спочатку територію сучасної України охопила революція, яка розгорнулася масштабними пропагандистськими гаслами. Кожна з воєн XX століття мала своє ідеологічне оформлення, ідеологічну мотивацію, яка могла виражатися як в офіційному визначенні війни вищими політичними та ідеологічними інститутами, так і в безпосередніх гаслах, що використовувалися в пропагандистській роботі. Протягом XX століття з'являються персональні комп'ютери і перші випадки кібератак. На цьому етапі можна говорити про зародження форм інформаційно-технічної війни. Активно застосовувалися і теоретично досліджувалися засоби інформаційно-психологічної війни, найчастіше – один з найпоширеніших її методів – пропаганда. Цей етап простягнувся на століття. Четвертий етап розпочався з поч. XXI ст. і триває до теперішнього часу: кібервійна утвердилася як нове деструктивне явище, а методи інформаційно-психологічної війни з огляду на масштабну цифровізацію стали справжньою політичною інфекцією.

6. У рамках комплексного підходу до розуміння інформаційних війн, єдину складну структуру простіше сприймати за двома спрямуваннями: їх розділяють на два види – інформаційно-психологічну та інформаційно-технічну.

Інформаційно-психологічна війна – це інструмент впливу політичної, військової, економічної, ідеологічної дії, логічне застосування якого дозволяє: 1) впливати на формування громадської думки (у т.ч. викликати інакомислення, невдоволення чи навпаки – підтримку у населення); 2) захистити національні інтереси шляхом зниження морального духу, бойової ефективності ворогів; 3) впливати на поведінку іноземних держав, неурядових організацій, окремих груп чи осіб. Її можна розглянути як процес взаємодії, що містить усі елементи комунікаційної моделі Лассвела: 1) хто або що є джерелом (наприклад, ЗМІ); 2) яку інформацію/контент містить; 3) через які канали він передається; 4) на яку аудиторію розрахований; 5) якого ефекту/результату вдалося досягнути.

Інформаційно-психологічну війну не слід ототожнювати із маніпулюванням, оскільки останнє її супроводжує, але не зливається. Крім того, попри

систематичний характер інформаційно-психологічної війни, маніпулювання використовується ще частіше не лише на маси, але й у міжособистісних стосунках, починаючи від торгівлі і закінчуючи внутрісімейними відносинами.

Інформаційно-психологічна війна сьогодні – складова технологічного Всесвіту. Мережа Інтернет дозволила розвивати нові форми обміну контентом, які сильно впливають на судження людей: блоги, форуми, соціальні мережі, сайти тощо, які оснащені системою оцінки аудиторією повідомлення, що разом із можливістю залишення коментарів дозволяє отримувати швидкий зворотній зв'язок, відслідковувати реакцію споживачів контенту й корегувати пропагандистський та/чи дезінформаційний вектор.

Проблема активності розгортання інформаційно-психологічного фронту в Інтернеті посилюється ще й тим, що користувачі більше довіряють думці окремих блогерів чи дописам у телеграм-каналах, ніж офіційним сайтам чи традиційному ЗМІ (телевізор, радіо), які тепер самі часто ретранслюють відео-, фото-матеріали із соціальних мереж.

До ключових аспектів пропаганди як основного методу інформаційно-психологічної війни відноситься: 1) односторонність аргументів; 2) виправдання результатами; 3) байдужість до логічних роздумів і доказової бази; 4) емоційна мова і переконливі визначення; 5) «квазіодноголосся»; 6) створення накопичувального повідомлення у ЗМІ.

7. Кібервійна, на наш погляд, складова доктрини вірогідності, яка поки що не витримує суворих перевірок, однак у науці відповідь на запитання щодо її існування значною мірою – питання інтерпретації та вільної конкуренції двох основних ідей: 1) кібервійна існує; 2) кібервійна – це певна умовність.

Під інформаційно-технічною війною ми розуміємо будь-який тип інформаційного впливу із застосуванням інформаційної зброї, метою якого є вплив на функціонування інформаційної системи шляхом незаконного доступу до інформаційної системи, здолання системи захисту, обмеження доступу законних

користувачів з можливістю подальшого несанкціонованого збору, копіювання, перехоплення, блокування або видалення інформації.

Об'єктом кібервійни є інформаційно-технологічна система. Суб'єктами інформаційно-технологічної війни можуть бути: недержавні (індивідуальні, субнаціональні, корпоративні) суб'єкти, до яких відносяться кібервоїни, які або самостійно ведуть кібервійну (надають «послуги») за винагороду від окремих держав або продають своє шкідливе програмне забезпечення (зазвичай, успішне ведення кібервійни потребує значних фінансових і кадрових ресурсів, які просувають політичні цілі держави-замовника, а зростаюча доступність анонімних ресурсів і обміну інформацією забезпечують ефективне співробітництво і швидкий обмін інформацією) або державні – окремі держави мають можливість самостійно використовувати складну кіберзброю для досягнення політичних цілей.

8. Ключові аспекти воєнної політики РФ включають не лише традиційне поле бою, але й інформаційно-психологічну та інформаційно-технічну війну.

Інформаційна війна РФ – постійний акт насильства, що слугує різним політичним цілям: ведеться в освітній, соціальній, оборонній, духовній сферах. Стратегія реалізовується сучасними способами – широким простором можливостей інформаційно-психологічної війни та масштабними кібератаками.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Акінчиць Н.Г. Політичний дискурс як об'єкт наукового аналізу. *Культура народів Причорномор'я*. 2007. № 107. С. 72-76.
2. Антонюк В.В. Інформаційна війна в структурі сучасного геополітичного протиборства: нові контексти та інтерпретації. *Державне управління: удосконалення та розвиток* : електронний журнал. URL: http://www.dy.nayka.com.ua/pdf/7_2021/35.pdf (дата звернення: 04.03.2023).
3. Бабенко В.Г. Основні групи кіберзброї та особливості її застосування. *Актуальні задачі та досягнення у галузі кібербезпеки* : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. Кропивницький : КНТУ, 2016. С. 23–24.
4. Бараненко Р.В., Задорожна А.Ю. Кібервійна як новий вид протистояння держав. *Південноукраїнський правничий часопис*. 2017. №1. С.53-56.
5. Біленчук П.Д., Кофанов А.В., Кобилянський О.Л. Міжнародний тероризм: консолідований аналіз забезпечення безпеки. Київ : ННПСК КНУВС, 2009. 72 с.
6. Білоконенко Л.А. Пейоративна й інвективна лексика в міжособистісному конфлікті. *Філологічні студії : Науковий вісник КНУ* : зб. наук. праць. 2012. Вип. 7. Ч. 2. С. 119–127.
7. Бовгиря О.О., Кирилюк М.А. Евфемізми як засіб маніпуляції в німецькому політичному дискурсові. *Філологічні науки: історія, сучасний стан та перспективи досліджень* : матеріали науково-практичної конференції, м. Львів, 20-21 вересня 2019 р. Херсон : Видавництво «Молодий вчений», 2019. С.35-38.
8. Бойченко О.В. Медіа-тероризм: особливості сучасних ознак інформаційній безпеці. *Інтегровані інтелектуальні робототехнічні комплекси (ПРТК-2009)* : друга міжнародна наук.-практ. конф., м.Київ, 25–28 травня 2009 р. Київ : НАУ, 2009. С. 230–232.

9. Браніцька Т.Р., Кащенко Н.В., Кухар І.Г. Культурна дипломатія як спосіб комунікації в інтересах національної безпеки України. *МАУП* : веб-сайт. URL: <https://maup.com.ua/assets/files/expert/16/13.pdf> (дата звернення: 14.03.2022).
10. Бурскин П. Итоги войны 1916 г. *Утро России: ежедневная газета*. 1917. 1 января.
11. Буткит UEFI как инструмент для кибершпионажа. *Eset*. URL: <https://eset.ua/ru/news/view/913/butkit-UEFI-kak-instrument-dlya-kibershpiionazha> (дата звернення: 01.12.2021).
12. Валюшко І.О. Еволюція інформаційних війн: історія і сучасність. *Історико-політичні студії*. 2015. № 2. С. 127-134.
13. Валюшко І.О. Основні виклики і загрози в епоху інформаційних війн. *Науковий вісник Дипломатичної академії України*. 2016. Вип. 23(2). С. 142-147.
14. Вауліна Ф.В. Політична міфотворчість у сучасній Україні. *Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Питання політології»*. 2015. Вип. 14. С. 106-111.
15. Великий тлумачний словник сучасної української мови : 250000 / уклад. та голов. ред. В. Т. Бусел. Київ ; Ірпінь : Перун, 2005. – VIII. 1728 с.
16. Верголяс О.О. Правове забезпечення спеціальних інформаційних операцій: дис. ... канд.юрид.наук : 12.00.07. Київ, 2020. 287 с.
17. Війни інформаційної епохи: міждисциплінарний дискурс : монографія / за ред. В.А. Кротюка. Харків : ФОП Федорко М. Ю., 2021. 558 с.
18. Вітман К.М., Кормич А.І. Відеоблоги як інноваційний засіб політичної комунікації. *Актуальні проблеми політики* : зб. наук. пр. 2021. Вип.68. Одеса : Видавничий дім «Гельветика». С. 52-57.
19. Воротинський В.В. Чутки як інструмент політичного маніпулювання в Інтернеті (на прикладі ситуації в Україні 2014 – початку 2015 років). [*Сучасне суспільство*](#). 2015. Вип. 2(1). С. 4-12.

20. Гібридна війна і журналістика. Проблеми інформаційної безпеки : навчальний посібник / за заг. ред. В. О. Жадька ; ред.-упор. : О.І. Харитоненко, Ю.С. Полтавець. Київ : Вид-во НПУ імені М. П. Драгоманова, 2018. 356 с.
21. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення. *Вісник НАДУ*. 2015. №1. С. 136-141.
22. Грачиков Г. Их облик, их нравы. В атмосфере жестокости и насилия. *Советский патриот*: Орган центрального комитета ДОСААФ СССР. 1979. 10 января. С.2.
23. Гриник Р.О., Пилипенко В.М. Кібертероризм як нова форма міжнародного тероризму. *Актуальні задачі та досягнення в галузі кібербезпеки* : матеріали Всеукр. наук.-практ. конф., м.Кропивницький, 23-25 листопада 2016 р. Кропивницький, 2016. С.61-62.
24. Гришук Р.В. Кібернетична зброя: класифікація, базові принципи побудови, методи та засоби застосування й захисту від неї. *Сучасна спеціальна техніка*. 2016. № 3 (46). С.94-101.
25. Грінберг М. Символи ненависті: довідник / укл.М.Петров.Українська Гельсинська спілка з прав людини : веб-сайт. URL: https://helsinki.org.ua/wp-content/uploads/2021/02/Prev-Hate_Symbols_A4.pdf (дата звернення: 18.03.2022).
26. Дашко Д.А., Мешков В.И. Социальная инженерия с точки зрения информационной безопасности. *Institutional Repository NTU Dnipro Polytechnic* : веб-сайт. URL: bit.ly/469HURL (дата звернення: 02.08.2021).
27. Денисюк Ж.З. Пропаганда та контрпропаганда в контексті стратегій державної інформаційної політики. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління*. 2021. Том 32 (71). № 2. С.46-51.
28. Джадт Т. Після війни. Історія Європи від 1945 року / пер. з англ. К.Заремби. Київ : Наш формат, 2020. 928 с.

29. Джиджора Є. Теорія змови як пропагандистська модель комунікації (як вишки 5G пов'язані з коронавірусом та «вакцинами Білла Гейтса»). *Діалог: медіа-студії*. 2020. № 26. С.37-51.
30. Дзьобань О.П. Філософія інформаційних комунікацій : монографія. Харків : Майдан, 2012. 224 с.
31. Для Русской Армии. *Киевлянин : литературная и политическая газета Юго-Западного края*. 1914. 27 июля. С.2.
32. Добровольська Г. Семантичні групи метафор в українському політичному дискурсі. *Філологічні студії*. 2017. С.30-34.
33. Доклад А.Жданова (22 сентября 1947 г.). *CVCE.eu.*: веб-сайт. URL: https://www.cvce.eu/content/publication/1997/10/13/914edbc9-abdf-48a6-9c4a-02f3d6627a24/publishable_ru.pdf (дата звернення: 17.05.2022).
34. ДСТУ 3396. 2-97. Захист інформації. Технічний захист інформації. Терміни і визначення. Київ : Держстандарт України, 1998. 16 с. 3. Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека. Термінологічний навчальний довідник. Київ : Издатель ООО «Д. В. К.», 2002. С. 4.
35. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ : НІСД, 2014. 328 с.
36. Е-боротьба в інформаційних війнах та інформаційне право : монографія / В.М. Брижко та ін. ; за ред. д.е.н., проф., члена-кореспондента АПрН України М. Швеця. Київ : НДЦПІ АПрН України, 2007. 234 с.
37. Жуйкова К.В., Гулак Г.М. Формалізація моделі загроз енергетичної безпеки. *Молодий вчений*. № 11 (38), 2016. URL: <http://molodyvcheny.in.ua/files/journal/2016/11/26.pdf> (дата звернення: 18.12.2021).
38. Завгородня Ю. В. Захист прав суб'єктів політики в умовах кіберпротистояння. *Права людини в період збройних конфліктів : Зб. матеріалів Міжнародної науково-практичної конференції присвяч. 25-річчю Національного університету «Одеська юридична академія»* (м. Одеса, 18 листопада 2022 р.) / Нац. ун-т «Одеська юридична

академія» ; каф. міжнародного та європейського права НУ «ОЮА» : у 2 т. Одеса, 2022. С. 531-534.

39. [Задорожна М.І.](#) Державне управління в умовах гібридної війни: маніпуляція суспільною свідомістю. *Публічне адміністрування: теорія та практика*. 2017. Вип. 2 (18). С.1-17. URL: http://nbuv.gov.ua/UJRN/Patp_2017_2_9 (дата звернення: 18.03.2022).

40. Закіров М. Міф як засіб інформаційного впливу та інструмент політичної комунікації. *Наукові праці Національної бібліотеки України імені В. І. Вернадського*. 2017. Вип. 48. С. 630-644.

41. Закон про електронні комунікації. *Верховна Рада України* : офіційний веб портал парламенту України. URL: <https://zakon.rada.gov.ua/laws/show/1089-20> (дата звернення: 27.07.2021).

42. Зауваження Головного юридичного управління до проекту Закону України про критичну інфраструктуру. *Верховна Рада України* : офіційний веб портал парламенту України. URL: bit.ly/484IYId (дата звернення: 18.11.2021).

43. Захаренко Л.М., Давидова О.В. Психотехнології ведення перемовин із правопорушниками : метод. рекомендації / за заг. ред. О. І. Мотляха. Київ : Освіта України, 69 с.

44. Заява за результатами саміту у Варшаві. *North Atlantic treaty organization*. URL:https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=uk (дата звернення: 02.11.2021).

45. Збанацкий Ю. Испытанная в веках. К 325-летию воссоединения Украины с Россией. *Советский патриот*. 1979. 10 января. С.2.

46. Звоздецька О. Дезінформація як загроза національній безпеці Європейського Союзу: проблеми та підходи. *Історико-політичні проблеми сучасного світу*, 2021. Т. 43, С. 30–39.

47. Інформаційно-психологічна боротьба у воєнній сфері : монографія / Г.В. Пєвцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, А.О. Феклістов, К.І. Хударковський. Харків: Вид. Рожко С.Г., 2017. 276 с.
48. Історія інформаційно-психологічного протистояння : підруч. / Я.М.Жарков, Л.Ф.Компанцева, В.В.Остроухов В.М.Петрик, М.М.Присяжнюк, Є.Д.Скулиш; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д.Скулиша. Київ : Наук.-вид. відділ НА СБ України, 2012. 212 с.
49. Калініченко Б.М. Інформаційна війна: чинники ескалації і засоби протидії [Електронний ресурс] / Національний педагогічний університет імені М.П. Драгоманова. Київ, 2020. 294 с.
50. Кібератаки Російської Федерації: хронологія. *Міністерство оборони України* : офіційний веб сайт. URL: <https://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federaczii-hronologiya.html> (дата звернення: 09.12.2021)
51. Кіслов Д.В. Інформаційні війни : монографія. Київ : Київ. нац. торг.-екон. ун-т, 2013. 300 с.
52. [Кіца М.О.](#) Фейкова інформація в українських соціальних медіа: поняття, види, вплив на аудиторію. *Наукові записки Української академії друкарства*. 2016. № 1. С. 281–287.
53. Клемперер В. LTI. Язык третьего рейха. Записная книжка филолога. *Almenda.org* : веб-сайт. URL: bit.ly/3r5Ai3I (дата звернення: 18.02.2022).
54. Климов В. К войне! К победе. *Утро России*. 1917. 8 марта.
55. Ключник Р.М. Дискурс протесту та політична коректність: до питання про евфемізми у політичній комунікації. *Регіональні студії*. 2018. № 13. С.30-35.
56. Ковальова О. Політичний дискурс: сучасні лінгвістичні інтерпретації. *Актуальні питання гуманітарних наук*. 2020. Вип.27. Т. 2. С.101-107.
57. Комітет з питань цифрової трансформації рекомендує Верховній Раді прийняти у другому читанні і в цілому законопроект щодо здійснення резервного копіювання інформації та відомостей державних електронних інформаційних

ресурсів державними органами. *Верховна Рада України* : офіційний веб портал парламенту України. URL : https://www.rada.gov.ua/news/news_kom/216206.html (дата звернення: 09.12.2021)

58. Кормич Л.І., Кормич А.І. Новий формат загроз міжнародного тероризму: час мереж та технологій. *Актуальні проблеми політики*. 2019. Вип. 63. С. 6-19.

59. Косенко Ю.В. Основи теорії мовленнєвої комунікації : навч. посібник. Суми : Сумський державний університет, 2013. 292 с.

60. Краснопольська Т.М. Політичний трайбалізм: прояви на пострадянському просторі та загрози для України. *Правові та інституційні механізми забезпечення розвитку України в умовах європейської інтеграції* : матеріали Міжнародної науково-практичної конференції, м. Одеса, 18 травня 2018 р. Одеса : Видавничий дім «Гельветика», 2018. С. 216-220.

61. Краснопольська Т.М., Милосердна І.М. Цифрові технології в механізмі взаємодії громадянського суспільства та держави. *Актуальні проблеми політики* : зб. наук. пр. 2021. Вип.67. Одеса. С. 68-74.

62. Кривенко С.-В.О. Семантична парадоксальність політичного дискурсу (теоретико-методологічний аналіз) : дис. ...канд.політ.наук : 23.00.01. Львів, 2016. 216 с.

63. Кройтор А.В. Технології маніпуляції у конструюванні інформаційного порядку денного. *Актуальні проблеми політики* : зб. наук. пр.2018. Вип. 62. С. 36-43.

64. Ктитарова Н.К. Загальне мовознавство : навчальний посібник для студентів вищих навчальних закладів. Дніпродзержинськ : Дніпродзержинський державний технічний університет, 2009. 144 с.

65. Кульба Я.Є. Масові настрої: генеза та особливості функціонування. *Inforum: science for the future*. URL: <https://www.inforum.in.ua/conferences/15/19/116> (дата звернення: 17.03.2022).

66. Курбан О.В. Інформаційні кампанії у соціальних онлайн-мережах: типологія та класифікація. *Поліграфія і видавнича справа*. 2017. № 1. С. 172–182.
67. Курілло В.Є. Латентна політика : навчальний посібник 2-е вид., перероб. і доп. Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2017. 360 с.
68. Лактіонов О.М., Хомуленко Т.Б. Політична психологія та іміджеологія: навчально-методичний посібник. Харків, 2009. 94 с.
69. Ландэ Д.В. Моделирование репутации, информационного влияния и управления. *Деструктивна пропаганда: шляхи протидії та проблеми відповідальності* : матер. наук.-практ. конф., м. Київ, 21 травня 2015 року. Київ : ТОВ «ІВА», 2015. С. 56-62.
70. [Левченко О.](#) Форми ведення інформаційної боротьби: практичний підхід до понятійного апарату. *Наука і оборона*. 2013. № 3. С. 21-26.
71. Леньо П.Ю. «Ленініана» на Закарпатті: дослідження радянської монументальної пропаганди (1944-1991). *Науковий вісник Ужгородського університету*. 2020. Вип 1 (42). С.397-412.
72. Лефтеров В., Третьякова Т. До проблеми психологічного тиску на учасників кримінального провадження під час проведення слідчих еспериментів та допитів. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія «Психологічні науки»*. 2019. № 3(14). С. 159-169.
73. Лисенко В. Чутки – активний засіб модифікації суспільної думки. *Політичний менеджмент*. 2004. №6. С.96-102.
74. Литвиненко О.В. Інформаційні впливи та операції: теоретико-аналітичні нариси : монографія. Київ: НІСД, 2003. 240 с.
75. Літопис Руський. *Ізборник* : веб-сайт. URL: <http://izbornyk.org.ua/litop/lit01.htm>. (дата звернення: 16.04.2020).
76. Луцишин Г., Гончарук А. Особливості розвитку культурної дипломатії України в сучасних умовах. *Academic Journals and Conferences* : веб-сайт. URL:

<https://science.lpnu.ua/sites/default/files/journal-paper/2017/nov/6654/lucishin.pdf> (дата звернення: 14.03.2022).

77. Лютий Т. В. Мова та ідеологія. *Магістеріум. Історико-філософські студії*. 2016. Вип. 65. С. 14-22.

78. Макаренко Є. Проблема міфу в системі сучасної політичної науки. *Наукові записки Інституту політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України*. 2012. Вип. 4. С. 289-299.

79. Макаренко Л.П. Еволюція форм та методів ведення інформаційної війни. *ResearchGate* : веб-сайт. URL: bit.ly/3PaKa9g (дата звернення: 23.04.2022).

80. Максимчук О.В., Бондар С.С. Роль мас-медіа у формуванні політичних міфів. *Актуальні проблеми політики*. 2020. Вип.65. С.49-54.

81. Мамонтова Е.В. Псевдоморфоз як техніка символізації у державотворчій практиці Доби Відродження. *Актуальні проблеми політики*. 2018. Вип.61. С.34-45.

82. Мамонтова Е.В., Краснопольська Т.М. Гібридні форми сучасної політики : навчально-методичний посібник для здобувачів третього (освітньо-наукового) рівня вищої освіти. Одеса, 2021. 52 с.

83. Маркова М.В. Інформаційно-психологічна війна: медико-психологічні наслідки та стратегії протидії. *Проблеми безперервної медичної освіти та науки*. 2016. №4. С.6-10.

84. Марунченко О.П. Інформаційна війна в сучасному політичному просторі : дис. ... канд. політ. наук : 23.00.02. Одеса, 2012. 209 с.

85. Марута Н.О., Маркова М.В. Інформаційно-психологічна війна як новий виклик сучасності: стан проблеми та напрямки її подолання. *Український вісник психоневрології*. 2015.Т. 23, Вип. 3 (84).С. 21–28.

86. Маскировался под сайт Президента. Госспецсвязи заблокировала фишинговый сайт. *Гордон*: веб-сайт. URL: bit.ly/3Pvycnc (дата звернення: 20.07.2021).

87. Мережко А.А. Конвенция о запрещении использования кибервойны в глобальной информационной сети информационных и вычислительных ресурсов (Интернете). *Політичний менеджмент. Політик*: веб-сайт.URL: <http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57>. (дата звернення: 21.04.2022).
88. Милосердна І.М. Імідж політичного лідера як категорія PR-технології. *Актуальні проблеми політики* : зб. наук. пр. 2019. Вип.64. Одеса : Фенікс. С. 118-133.
89. Милосердна І.М. Комунікація та зворотний зв'язок у структурі кібернетичного механізму політичного управління. *Актуальні проблеми політики* : зб. наук. пр. 2019. Вип. 63. Одеса : Фенікс. С.153-165.
90. Милосердна І.М. Чинники та напрями формування ефективної системи міжнародної безпеки в сучасних умовах. *Правове життя сучасної України* : у 3 т. : матеріали Міжнар. наук.-практ. конф. м. Одеса, 15 трав. 2020 р., Одеса : Гельветика, 2020. Т. 1. С. 213-216.
91. Морозов А.Ю. Футурологічні та конспірологічні виміри ковід-епідемії. *Суспільно-політичні процеси в умовах пандемії: особливості та виклики* : тези доповідей Всеукр. наук.-практ. конф., м. Київ, 16 квітня 2021 р. Київ, 2021. С.70-73.
92. Мошак Д.С. Сучасні політичні маніпуляції: політико-комунікаційний та політико-технологічний виміри. *Науковий журнал «Політикус»*. Випуск 4, 2020. С.42-46.
93. Мудра І., Сінькова Є. Інструменти інформаційної війни проти України. *Вісник національного університету «Львівська політехніка»: журналістські науки*. 2017. Випуск 1. Номер 883. С.42-47.
94. Музика В.В. Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення: дис. ... доктора філософії : 081. Одеса, 2021. 219 с.

95. Мурашко А. У 2018 році українські фахівці заблокували близько 400 кібератак. *Інформаційне агентство «Українські Національні Новини»*. URL: bit.ly/3LcX3d2 (дата звернення: 12.02.2019).
96. На Хмельниччині СБУ викрила прихильника Шарія на закликах до підтримки окупантів. *Служба безпеки України*: Youtube-канал. URL: https://www.youtube.com/watch?v=sxeYbWehGoA&ab_channel=%D0%A1%D0%BB%D1%83%D0%B6%D0%B1%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8 (дата звернення: 04.03.2023).
97. Нагорна Л.П. Політична мова і мовна політика: діапазон можливостей політичної лінгвістики. Київ : Світогляд. 2005. 315 с.
98. Наумкіна С.М., Гайдаєнко П.Л. Роль харизматичної сигналізації у контексті політичного лідерства в соціальних мережах. *Актуальні проблеми політики* : зб. наук. пр. Одеса : Видавничий дім «Гельветика», 2022. Вип. 69. С. 48-54. DOI <https://doi.org/10.32837/app.v0i69.1301>.
99. Ніколаєнко С., Ніколаєнко Св. Категорія психологічного впливу в психології. *Світогляд - Філософія – Релігія* : зб. наук. пр. 2011. № 1. URL: bit.ly/3PwfU56 (дата звернення: 14.02.2022).
100. Новітня політична лексика (неологізми, okazіоналізми та інші новотвори) / І. Я. Вдовичин, Л. Я. Угрин, Г. В. Шипунов та ін.; за заг. ред. Н. М. Хоми. Львів : «Новий Світ – 2000», 2015. 488 с.
101. Обачність. Пильність. Захист. Ввічливість. Сміливість: посібник із цифрового громадянства та безпеки. *Нова українська школа*: веб-сайт. URL: <https://nus.org.ua/wp-content/uploads/2018/08/PRESS.pdf>. (дата звернення: 18.07.2021).
102. Олексюк Л. Кращі практики управління безпекою: оглядовий звіт. *United Nations Development Programme*. URL: https://www1.undp.org.Report_on_Cybersecurity_04.pdf (дата звернення: 02.11.2021).

103. Омельченко В., Чекунова С., Білявський М. Енергетика України: виклики та ініціативи. *Razumkov Centre*. URL: https://razumkov.org.ua/uploads/article/2020_energy_initiatives.pdf (дата звернення: 16.12.2021).
104. Орел В.М. Фінансова система як невід'ємна складова економічного процесу країни. *Український журнал прикладної економіки*. 2016. Том 1. № 1. С. 141-152.
105. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
106. Павлов В. І., Лебедєв В.О. Словник найбільш уживаних термінів з філософії, логіки, етики, естетики та релігієзнавства. Харків : УкрДУЗТ, 2019. 160 с.
107. Павлов В. НАТО – филиал Пентагона. Международные заметки. *Советский патриот*: Орган центрального комитета ДОСААФ СССР. 1979. 4 апреля. С.4.
108. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал*. 2009, № 5. С.122-135.
109. Пиріг Р. Дипломатія та зовнішня політика в «Артхашастрі». *Зовнішні справи*. 2013. № 7. С. 52-55.
110. Писаренко Л.М. Комунікативна пропаганда та маніпуляція в гаслах та слоганах політичних лідерів. *Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (з нагоди 30-річчя проголошення незалежності України та 25-річчя прийняття Конституції України) : у 2 т. : матеріали міжнар. наук.-практ.конф., м. Одеса, 21 трав. 2021 р. Одеса : Видавничий дім «Гельветика», 2021. Т. 1. С. 712-715.*
111. Північноатлантичний договір : міжнародний документ від 04.04.1949. *Офіційний портал Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/950_008#Text (дата звернення: 02.12. 2021).
112. Пілат М. Інформаційні впливи та інформаційні війни: сутність понять та їхній взаємозв'язок в інформаційну епоху. *Вісник Львівського університету. Серія «Міжнародні відносини»*. 2013. Вип. 32. С. 185-190.

113. Погрібна В.Л., Герасіна Л.М. Інформаційна війна як каталізатор геополітичних змін. *eNULAIR* : веб-сайт. URL: http://dspace.nlu.edu.ua/bitstream/123456789/11320/1/Pogribna_Gerasina_72-75.pdf. (дата звернення: 16.07.2021).
114. Політологія : підручник / за ред. М.М. Вегеша. Київ : Знання, 2008. 556 с.
115. Політологія: сучасні терміни і поняття : короткий навчальний словник-довідник для студентів ВНЗ I-IV рівнів акредитації / укладач В.М. Піча ; наук. редакція Л.Д. Климанської, Я.Б. Турчин, Н.М. Хоми. Львів : Новий Світ – 2000, 2015. 516 с.
116. Полторак В.А., Стадник А.Г. Пропаганда та її місце в процесі ведення інформаційних війн. Основні форми пропагандистського впливу: пряма пропаганда, джінса, пабліситі, пропаганда 2.0. *Epistemological studies in Philosophy, Social and Political Sciences*, 2020, 3 (1) С.126-138.
117. Польовий М.А. Формування глобального громадянського суспільства як чинник розвитку терористичної активності в глобалізованому світі. *Актуальні проблеми політики*. Одеса : Фенікс, 2015. Вип. 56. С.122-129.
118. Почепцов Г.Г. Пропаганда: основные характеристики. *DM media sapiens* : веб-сайт. URL: <https://ms.detector.media/mediaanalitika/post/20334/2018-01-07-propaganda-osnovnye-kharakterystyky/> (дата звернення: 04.03.2023).
119. Почепцов Г.Г. Сміслові та інформаційні війни. *Інформаційне суспільство*. 2013. Вип. 18. С. 21-27.
120. Почепцов Г.Г. Сучасні інформаційні війни. Київ : Вид.дім «Києво-Могилянська академія», 2016. 504 с.
121. Прищепа Я. Іран заборонив імпорту американської та британської вакцини. *Суспільне|| Новини* : веб-сайт. URL: <https://suspiilne.media/94450-iran-zaboroniv-import-amerikanskoi-ta-britanskoi-vakcini/> (дата звернення: 08.02.2021).
122. Прокопович Т. Філософські праці. Вибране. Київ : «Дніпро», 2012. 615 с.

123. Прокопчук А., Баранов А. Сетевая атака SYN-флуд . *Institutional Repository Dnipro University of Technology*: веб-сайт. URL: <http://ir.nmu.org.ua/bitstream/handle/123456789/1881/SYN-FLOOD.pdf?sequence=1&isAllowed=y> (дата звернення: 14.07.2021).
124. Проноза І.І. Інформаційна війна: сутність та особливості прояву. *Актуальні проблеми політики*. 2018. Вип.61. С.76-84.
125. Проноза І.І. Інформаційно-психологічні війни як механізм управління суспільно-політичною свідомістю. *Сучасна українська держава: вектори розвитку та шляхи мобілізації ресурсів* : матеріали П'ятої Всеукраїнської науково-практичної конференції, м. Одеса, 3 квітня 2020 року. Одеса : ПНПУ імені К. Д. Ушинського, Центр соціально-політичних досліджень «Politicus», 2020. С. 46-50.
126. Прохоренко А.М. Концепт інноваційних політичних технологій та особливості впровадження їх в Україні: дис...докт.філософії : 052. Одеса, 2021. 202 с.
127. Психологія спілкування : навч. посіб. / Л.Г. Кайдалова, Л.В. Пляка, Н.В. Альохіна, В.С. Шаповалова. - 2-ге вид., перероб. і допов. Харків : НФаУ, 2018. 140 с.
128. Публічна комунікація та ділова мова в публічному управлінні: конспект лекцій / укл.Шмагун А.В. *Таврійський Національний університет імені В.І.Вернадського* : веб-сайт. URL: bit.ly/3sHDfI5 (дата звернення: 02.02.2022).
129. Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). *Офіційний веб-портал Верховної Ради України*: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 12.12.2021).
130. Росія за допомогою кібератак намагається тероризувати українців – Politico. *УНІАН: інформаційне агентство*. URL: unian.ua/techno/communications/rossiya-pri-

pomoshchi-kiberatak-pytaetsya-terrorizirovat-ukraincev-politico-12106917.html (дата звернення: 06.03.2023).

131. Росія здійснює на Україну понад 10 кібератак за добу – СБУ. *Укрінформ*: мультимедійна платформа іномовлення України. URL: <https://www.ukrinform.ua/rubric-ato/3676108-rosia-zdijsnue-na-ukrainu-ponad-10-kiberatak-za-dobu-sbu.html> (дата звернення: 28.02.2023).

132. Самчинська О.А., Фурашев В.М. Інформаційне насильство, інформаційна маніпуляція та пропаганда: поняття, ознаки та співвідношення. *Інформація і право*. 2021. №1 (36). С.55-65.

133. Сасин Г.В. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір). *Грані*. 2015. №3 (119). С. 18-23.

134. Світова гібридна війна: український фронт / за заг. ред. В.П. Горбуліна. Київ : НІСД, 2017. 496 с.

135. Семенов Г. Бойцы рассказывают о задачах колхозной торговли. Через свободную продажу хлеба кооперации укрепляй колхозы. *Красная звезда*. 1933. 22 декабря. С.1.

136. Сенченко М.І. Латентна світова інформаційна війна. Київ : ФОП Стебеляк, 2014. 384 с.

137. Сербіна Н.Ф., Кучмій О.П. Культурна дипломатія як інструмент зовнішньої політики сучасної європейської держави. *Актуальні проблеми міжнародних відносин*. 2011. Вип. 100 (1). С. 122-131.

138. Словник української мови : в 11 т. / ред. тому: А.А. Бурячок, П.П. Доценко ; АН Української РСР, Ін-т мовознав. ім. О. О. Потебні. Київ : Наукова думка, 1973. Т. 4 : І-М. 840 с.

139. Смачило Т.В., Кривцун А.Р. Феномен інформаційного тероризму як загрози міжнародній безпеці. *Молодий вчений*. 2017. №11 (51). С.124-127.

140. Сніцаренко П.М. Інформаційна операція Збройних Сил України як інтегруюча форма воєнних дій в інформаційному просторі. *Наука і оборона*. 2020. №1. С.37-42.
141. Сніцаренко П.М., Кацалап В.О. Методика оцінювання психологічного впливу. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2018. № 3. С.113-118.
142. Соціальна психологія : навч. посіб. для здобувачів ступеня бакалавра / Н.Ю. Волянчук, Г.В. Ложкін, О.В. Винославська, І.О. Блохіна, М.О. Кононець, О.В. Москаленко, О.І. Боковець, Б.В. Андрійцев. Київ : КПП ім. Ігоря Сікорського, 2019. 254 с.
143. [Стадник А.Г.](#) Інформаційна війна як комунікативна технологія впливу на масову свідомість та громадську думку. *Науково-теоретичний альманах «Грані»*. 2016. № 1. С. 111-115.
144. Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни»: затверджено указом Президента України від 26 серпня 2021 року №447/2021. *Верховна рада України: офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#n7> (дата звернення: 01.03.2023)
145. Сугестивні технології маніпулятивного впливу : навч. посіб. / В.М.Петрик, М.М.Присяжнюк, Л.Ф.Компанцева, Є.Д.Скулиш, О.Д.Бойко, В.В.Остроухов; за заг. ред. Є.Д.Скулиша. 2-ге вид. Київ : ЗАТ «ВІПОЛ», 2011. 248 с.
146. Талышинский Э.Б. Сущность информационной войны в процессах глобализации. *Університетські наукові записки*. 2012. № 2(42). С. 385–389.
147. Твердохліб Ю.М. Інформаційно-психологічні операції у російсько-українській гібридній війні : дис...канд.політ.наук : 23.00.04. Чернівці, 2019. 219 с.
148. Технології захисту інформації : лекція. *Ужгородський національний університет*: веб-сайт. URL: <https://www.uzhnu.edu.ua/uk/infocentre/get/4186> (дата звернення: 29.10.2021).

149. Трофіменко О.Г., Прокоп Ю.В., Логінова Н.І., Задерейко О.В. Кібербезпека України: аналіз сучасного стану. *Захист інформації*. 2019. Том 21. № 3. С. 150-157.
150. Туранський М.О. Інформаційно-психологічне забезпечення операції з анексії Криму Російською Федерацією: історичні передумови та практична реалізація : дис. ... доктора філософії : 032. Львів, 2020. 240 с.
151. Україна. Рік інформаційної війни в цифрах. *Reporters sans frontiers: веб-сайт*. URL: https://rsf.org/sites/default/files/medias/file/2023/02/Un%20an%20guerre%20informatio%20n_UKR.pdf (дата звернення: 06.03.2023).
152. Українська Революція гідності, агресія РФ і міжнародне право / Антонович М.М. та ін. ; упорядкув. і заг. ред. Задорожній О.В. Київ : К.І.С., 2014. 1013 с.
153. Фейки як інструмент впливу на вибори: аналітична доповідь / Дубов Д.В., Корецька І.О., Баровська А.В. та ін. Київ : Національний інститут стратегічних досліджень: центр безпекових досліджень. Школа політичної аналітики НАУКМА. 2020. 209 с.
154. Філософський енциклопедичний словник / Шинкарук В.І. та ін. Київ : Абрис, 2002. 752 с.
155. Фісун А.О. Теоретично-категоріальне осмислення поняття «інформаційна війна» в структурі інформаційно-політичного простору. *Інформаційне суспільство: науковий журнал*. 2011. Вип.13. С.43-48.
156. Фриче В. Раскованный Прометей. *Утро России*. 1917. 8 марта.
157. Фролова І.Є. Дискурсивна стратегія як організуючий конституент вербально-соціальної інтеракції. *Лінгвістика XXI століття: нові дослідження і перспективи*. 2009. № 3. С. 242-249.
158. ЦПД пояснює механізм «заговорювання» в дезінформації. *Центр протидії дезінформації при РНБО України* : веб-сайт. URL: bit.ly/44FzKiQ (дата звернення: 06.03.2023).

159. Цюрупа М. Питання визначення сутності «гібридної війни»: на прикладі збройної боротьби на Сході України (середина 2014-кінець 2015 рр.). *Наукові записки*. Вип. 5-6 (79-80). С.56-65. URL: https://ipiend.gov.ua/wp-content/uploads/2018/07/tsurupa_pytannia.pdf (дата звернення: 18.11.2021).
160. Чернышенко С.А. Кибервойна: теория и практика. *Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія»*. Серія: Політологія. 2015. Вип.248. С.37-41.
161. Чистоклетов Л.Г., Шишко В.Й. Інформаційно-психологічні впливи як невід’ємна складова парадигми інформаційної безпеки. *Науковий вісник Львівського державного університету внутрішніх справ*. 2012. № 2(1). С.183-193.
162. Чому конспірологічна пропаганда успішна і що з цим робити: вразливість аудиторії та спротив антизахідній, прокремлівській дезінформації в Україні / П.Померанцев та ін. *Arenaresearch.org* : веб-сайт. URL: <https://arenaresearch.org/wp-content/uploads/2021/06pdf>. (дата звернення: 18.04.2022).
163. Чорномаз Б.Д. Національна пам’ять як зброя в інформаційній війні. *Науково-теоретичний альманах «Грані»*. 2019. № 22 (11). С. 69-80.
164. Шайгородський Ю. До визначення сутності поняття «політичний міф». *Сучасна українська політика : політики і політологи про неї*. 2009. Вип.16. С. 49-53.
165. Шевців М.Б., Гончарук К.А. Пропаганда, як соціально-політичне явище: проблеми розуміння. *Південноукраїнський правничий часопис*. №1. 2019. С. 119-122.
166. Шпиґа П.С., Рудник Р.М. Основні технології та закономірності інформаційної війни. *Проблеми міжнародних відносин*. 2014. Вип. 8. С. 326-339.
167. Шпилик С. Інформаційна війна, пропаганда та PR: такі схожі й такі різні. *Галицький економічний вісник*. 2014. Том 47. № 4. С. 178-188.

168. Юридическая психология: Терминологический словарь / сост. Бандурка А.М., Венедиктов В.С., Тимченко А.В., Христенко В.Е., Калиновский В.Б. / под ред. Бандурки А.М. Харьков : Тимченко, 2005. 432 с.
169. Яковчук В.С., Малець Б.І., Борзов Ю.О. Інформаційні війни в сучасному світі. *Електронний репозитарій Львівського державного університету безпеки життєдіяльності* : веб-сайт. URL : bit.ly/3Z7i2nj (дата звернення: 20.04.2022).
170. Ярош Н.С., Артюхова В.В. Теоретична модель поведінкових наслідків віри у теорії змови. *Вісник Харківського національного університету імені В.Н.Каразіна. Серія «Психологія»*. 2021. Випуск 70. С.78-85.
171. Яхлаков П. Слава героической Советской Армии. Армия-освободительница. *Колхозная правда*: орган Ново-Ивановского райкома КПБУ и районного совета депутатов Измаильской области. 1949. 22 февраля. С.1.
172. Яцишин М.Ю. Використання сили у кіберпросторі в рамках міжнародного права. *Інформація і право*. 2018. № 4. С. 22-32.
173. «Diversification». *Oxford learner's dictionaries* : веб-сайт. URL: <https://www.oxfordlearnersdictionaries.com/definition/english/diversification?q=diversification> (дата звернення: 22.02.2023).
174. 14 cyber attacks on crypto exchanges resulted in a loss of \$882 million. *Finyear*. URL: https://www.finyear.com/14-cyber-attacks-on-crypto-exchanges-resulted-in-a-loss-of-882-million_a40041.html (дата звернення: 04.12.2021).
175. Ahluwalia V.K. Psychological Warfare: Call out Adversaries' Designs. *CLAWS Journal Winter* . 2020. Vol.13. No 2. URL: bit.ly/466X7D9 (дата звернення: 18.03.2021).
176. Ampere A.M. Essai sur la philosophie des sciences. Paris : Bachelier, 1843. 2nd partie. P. 140–142.
177. An act prohibiting disclosure of or inquiry into, deposits with any banking institution and providing penalty therefor : Republic Act № 1405. *The LawPhil project*.

URL : https://lawphil.net/statutes/repacts/ra1955/ra_1405_1955.html (дата звернення: 04.12.2021).

178. Ashraf C. Defining cyberwar: towards a definitional framework. *Defense&Security Analysis*. 2021. Volume 37, issue 3. URL: <https://www.tandfonline.com/doi/full/10.1080/14751798.2021.1959141> (дата звернення: 01.03.2023).

179. Bangladesh Bank vs. Rizal Commercial Banking Corporation, et al. – Complaint in the United States District Court for the Southern District of New York. *National security archive*. URL: <https://nsarchive.gwu.edu/media/18204/ocr> (дата звернення: 04.12.2021).

180. Baptista J.P., Gradim A. Understanding fake news consumption: a review. *Soc. Sci.* 2020. № 9 (10). URL: <https://doi.org/10.3390/socsci9100185> (дата звернення: 18.03.2022).

181. Bernays E.L. Propaganda. New York, 1928. 159 p.

182. Brantly A.F. Military and intelligence cyber decision-making : a diss. doct. of phil. Georgia, 2012. URL: https://getd.libs.uga.edu/pdfs/brantly_aaron_f_201212_phd.pdf (дата звернення: 12.12.2021).

183. Buli N. Norway says cyber attack on parliament carried out from China. *Reuters*. <https://www.reuters.com/world/china/norway-says-march-cyber-attack-parliament-carried-out-china-2021-07-19/> (дата звернення: 08.12.2021).

184. Case 1:19-cv-00983-LGS Bangladesh bank against Rizal commercial banking corporation at al. URL: bit.ly/3PxBkz2 (дата звернення: 05.12.2021).

185. Chachko E., Linos K. International Law After Ukraine: Introduction to the Symposium. *AJIL Unbound*. 2022. Vol. 116. P.124-129.

186. Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States. *European Parliament* : веб-сайт. URL: bit.ly/45LjOwG (дата звернення: 16.04.2022).

187. Dupuy A.C., Nussbaum D., Butrimas V., Granitsas A. Energy security in the era of hybrid warfare. *NATO*. URL: bit.ly/3sNIUwo (дата звернення: 16.12.2021).
188. Ecuadorean Bank Loses \$12 million via SWIFT. *Trendmicro*. URL: bit.ly/3P9LJ2w (дата звернення: 18.12.2021).
189. Ellul J. Propaganda. *Monoskop.org* : веб-сайт. URL: https://monoskop.org/images/4/44/Ellul_Jacques_Propaganda_The_Formation_of_Mens_Attitudes.pdf (дата звернення: 18.04.2022).
190. Final Report – Study on cyber security in the energy sector of Energy Community. *Blueprint Energy Solutions GmbH*. URL: <https://energy-community.org> (дата звернення: 16.12.2021).
191. Hirst K.K. Behistun Inscription: Darius's Message to the Persian Empire. *ThoughtCo*. URL: <https://www.thoughtco.com/behistun-inscription-dariuss-message-170214>. (дата звернення: 18.09.2021).
192. Iran blamed for Parliament cyber-attack. 2017. *BBC*. URL: <https://www.bbc.com/news/uk-41622903> (дата звернення: 12.12.2021).
193. Joshua H.-C. Stop Talking about Fake News! *PhilPapers* : веб-сайт. URL: <https://philpapers.org/rec/HABSTA> (дата звернення: 16.04.2022).
194. Journalism, «Fake News» & Disinformation: Handbook for Journalism Education and Training. *UNESCO*: веб-сайт. URL: https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf (дата звернення: 14.12.2021).
195. Jung C.G. Psychological Types or The psychology of individuation / translated by Godwin Baynes M.B., Cantab B.C. London. 1946. 694 p.
196. Lasswell H.D. The theory of political propaganda. *The American Political Science Review*. 1927. Vol. 21. P. 627-631. URL: <https://www.jstor.org/stable/1945515> (дата звернення: 08.02.2022).
197. Le accuse di Mosca e la nostra risposta. *La Stampa*. URL: bit.ly/3ZejW5F (дата звернення: 02.02.2021).

198. Libicki M.C. What is information warfare? Washington : National defense university, 1995. 104 p.
199. Lucas G. [Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare](https://philpapers.org/rec/LUCEAC-2). *PhilPapers* : веб-сайт. URL: <https://philpapers.org/rec/LUCEAC-2> (дата звернення: 21.04.2022).
200. Marczak B., Scott-Railton J., Berdan K., Razzak B.A., Deibert R., Hooking C. Another Mercenary Spyware Vendor Comes into Focus. *The citizen lab*. URL: <https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/> (дата звернення: 05.11.2021).
201. Maschmeyer L., Cavelty M. Goodbye Cyberwar: Ukraine as a reality check. *Policy perspectives*. 2022. Vol.10/3. URL: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/549252/PP10-3_2022-EN.pdf?sequence=2&isAllowed=y (дата звернення: 01.03.2023).
202. McCreadie M., Rice R.E. Trends in analyzing access to information. Part I: cross-disciplinary conceptualizations of access. *Information Processing and Management*. 1999. Vol. 35. P. 45-76. URL: bit.ly/4852AMr (дата звернення: 08.09.2022).
203. Mohee A. [Cyber war: The hidden side of the Russian-Ukrainian crisis](https://osf.io/preprints/socarxiv/2agd3/). *SocArXiv*: веб-сайт. URL: <https://osf.io/preprints/socarxiv/2agd3/> (дата звернення 01.03.2023).
204. [Muthumanickam K.](#), [Ilavarasan E.](#) CoPDA: Concealed process and service discovery algorithm to reveal rootkit footprints. [Malaysian Journal of Computer Science](#) 28(1):1-15, 2015. URL: bit.ly/3sJM3gJ (дата звернення: 11.11.2021).
205. Nakashima E. The NSA Has Linked the WannaCry Computer Worm to North Korea. *Washington Post*. URL: wapo.st/3R9X19v (дата звернення: 18.12.2021).
206. Norway blames Russia for cyber-attack on parliament. *BBC*. URL: <https://www.bbc.com/news/world-europe-54518106> (дата звернення: 12.12.2021).
207. Now Available: IAEA Guidance on Computer Security for Nuclear Security. *IAEA*. URL: bit.ly/3rb0oCv (дата звернення: 06.12.2021).

208. Nye J.S. Soft Power. *Foreign Policy*. 1990. № 80. P. 153–171. URL: www.jstor.org/stable/1148580 (дата звернення: 16.11.2021).
209. Plenge J. Deutsche Propaganda. Die Lehre von der Propaganda als praktische Gesellschaftslehre. Bremen, 1922. 86 p.
210. Ponemon Research Report: The Impact of Ransomware on Healthcare During COVID-19 and Beyond. *Censinet*. URL: <https://www.censinet.com/ponemon-report-covid-impact-ransomware/> (дата звернення: 12.01.2022).
211. Popper Karl R. The logic of scientific discovery basic books / пер. с англ. В.Н.Брюшинкина (предисловия гл. I, II, V, VI, VII) и А.Л. Никифорова (гл. III, IV, X). London, 1980. 203 p.
212. Samama P. Comment la France se prepare a une cyberguerre mondiale. *BFM business*. 2019. URL: bit.ly/45JIl5o (дата звернення: 13.12.2021).
213. Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge : Cambridge University Press, 2017. 598 p.
214. Soesanto S. The IT army of Ukraine: structure, tasking, and eco-system. Cyberdefense report. Zurich. 2022. *ENT library*. URL: <https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/552293/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf?sequence=2&isAllowed=y> (дата звернення: 01.03.2023).
215. Stevens T. Cyberweapons: an emerging global governance architecture. DOI:10.1057/palcomms.2016.102. *ResearchGate*. URL: https://www.researchgate.net/publication/312188394_Cyberweapons_an_emerging_global_governance_architecture (дата звернення: 06.12.2021).
216. Sun T. The art of war: the oldest military treatise in the world. *Project Gutenberg* : веб-сайт. URL: <https://www.gutenberg.org/files/132/132-h/132-h.htm> (дата звернення: 18.09.2020).
217. Supreme Leader: US officials are charlatans and terrorists. *Islamic republic news agency* : веб-сайт. URL: <https://en.irna.ir/news/83723720/Supreme-Leader-US-officials-are-charlatans-and-terrorists> (дата звернення: 08.02.2021).

218. Swanson L. The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict, 32 *Loy. L.A. Int'l & Comp. L. Rev.* 303. 2010. URL: <https://digitalcommons.lmu.edu/ilr/vol32/iss2/5/> (дата звернення: 15.12.2021).
219. Trujillo E. Cyberdefense: «La cyberguerre s'apparente avant tout a une guerilla». *BFM business*. 2020. URL: bit.ly/3Rh2GuA (дата звернення: 13.12.2021).
220. Weimann G. Cyberterrorism How Real Is the Threat? Special report. *United State institute of peace*. 2004. URL: <https://www.usip.org/sites/default/files/sr119.pdf> (дата звернення: 30.04.2022).
221. Westman N. Woman dies during a ransomware attack on a German hospital. *The Verge*. URL: <https://www.theverge.com/2020/9/17/21443851/death-ransomware-attack-hospital-germany-cybersecurity> (дата звернення: 12.01.2022).

ДОДАТКИ

Додаток А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні результати дисертації

1. Таркін В.П. Інформаційні війни: теоретичний аспект. *Держава і право. Юридичні і політичні науки*. 2020. Випуск 87. С.285-294. DOI: 10.33663/1563-3349-2020-87-285.
2. Таркін В.П. Окремі аспекти використання методів інформаційно-психологічної війни під час пандемії Covid-19. *Актуальні проблеми політики*. 2021. №67. С.112-117. DOI <https://doi.org/10.32837/app.v0i67.1160>.
3. Таркін В.П. Боротьба у кіберпросторі: інформаційні війни і кібертероризм. *European political and law discourse*. 2021. Volume 8. Issue 4. С.97-105. DOI: 10.46340/eppd.2021.8.4.11.
4. Таркін В.П. Особливості інформаційної війни РФ та український спротив. *Актуальні проблеми політики*. 2023. Вип.71. С.204-210. DOI <https://doi.org/10.32782/app.v71.2023.28>.

Наукові праці, які засвідчують апробацію матеріалів дисертації

5. Таркін В.П. Окремі аспекти успішної пропаганди у поглядах С.П. Чахотина. *Українське суспільство в умовах воєнного стану: сучасні виклики та напрямки розвитку* : матеріали Всеукр. наук. конф. молодих вчених, м. Одеса, 6 червня 2022 р. Одеса : Фенікс, 2022. С. 626-630.
6. Таркін В.П. Пропаганда як метод інформаційно-психологічної війни: політичний контекст. *Правове життя сучасної України: у 3 т.: матеріали міжнар. наук.-практ.конф., м.Одеса, 15 трав.2020 р.* Одеса : Видавничий дім «Гельветика», 2020. Т.1. С.251-254.
7. Таркін В.П. Правове забезпечення інформаційної політики. *Нові завдання та напрями розвитку юридичної науки у ХХІ столітті* : матеріали міжнародної

науково-практичної конференції м.Одеса, 26-27 лютого 2021 року, Одеса : Міжнародний гуманітарний університет, 2021. С.42-45.

8. Таркін В.П. Інформаційно-технічна війна у гонитві вакцинації. *Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (за нагоди 30-ти річчя проголошення незалежності України та 25-ти річчя прийняття Конституції України)* : у 2 т. : матеріали міжнар. наук.-практ. конф., м. Одеса, 21 травня 2021 р. Одеса, 2021. Т 1. С.209-212.

9. Таркін В.П. Дезінформація як метод інформаційно-психологічної війни. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права)* : у 2 т. : матеріали Міжнар.наук.-практ. конф. м. Одеса, 17 червня 2022 р. Одеса : Видавничий дім «Гельветика», 2022. Т. 1. С. 267-270.

10. Таркін В.П. Інтернет – платформа інформаційно-психологічної війни. *Сталий розвиток суспільства та держави: сучасні виклики та перспективи розвитку*: матер. Всеукр. наук. конф. молодих вчених, м.Одеса, 18 листопада 2022 р.) [Електронне видання] / уклад. В.С.Кучерявенко, Л.С.Бондарчук, І.С.Радковська [та ін.]; за ред. М.Р.Аракеяна, К.І. Спасової. Одеса, 2022. С.227-230.

11. Таркін В.П. Окремі аспекти конспірологічних теорій. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень*: матеріали міжнародної науково-практичної конференції, м. Одеса, 19 травня 2023 р. Одеса, 2023. Том 1. С.206-209.

ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

Основні аспекти наукового дослідження обговорювалися на засіданнях та фахових семінарах кафедри політичних теорій НУ «ОЮА». Окремі положення дисертаційного дослідження висвітлювалися на міжнародних та всеукраїнських науково-практичних конференціях та круглих столах: «Правове життя сучасної України» (м. Одеса, 15 травня 2020 р.), «Нові завдання та напрями розвитку юридичної науки у ХХІ столітті» (м.Одеса, 26-27 лютого 2021 р.), «Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (за нагоди 30-ти річчя проголошення незалежності України та 25-ти річчя прийняття Конституції України)» (м. Одеса, 21 травня 2021 р.), «Українське суспільство в умовах воєнного стану: сучасні виклики та напрями розвитку» (м.Одеса, 6 червня 2022 р.), «Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів ХХІ століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права)» (м.Одеса, 17 червня 2022 р.), «Сталий розвиток суспільства та держави: сучасні виклики та напрями розвитку» (м.Одеса, 18 листопада 2022 р.), «Європейські орієнтири розвитку України в умовах війни та глобальних викликів ХХІ століття: синергія наукових, освітніх та технологічних рішень» (м.Одеса, 19 травня 2023 р.).