РОЗДІЛ ІІ. КОНСТИТУЦІЙНЕ ПРАВО; МУНІЦИПАЛЬНЕ ПРАВО

УДК 342.7
DOI https://doi.org/10.24144/2788-6018.2024.03.6

ІНФОРМАЦІЯ ЯК ОБ'ЄКТ НАЦІОНАЛЬНОЇ БЕЗПЕКОВОЇ ПОЛІТИКИ УКРАЇНИ

Венглінський О.О.,
аспірант Харківського національного університету внутрішніх справ
ORCID: 0000-0001-5924-2811

Венглінський О.О. Інформація як об'єкт національної безпекової політики України.

Звертається увага на пріоритетне значення інформації серед об'єктів національної політики безпеки України. Доводиться, що інформаційна свобода вимагає пильного державного контролю та включення інформації до переліку об'єктів національної безпекової політики.

Інформаційні загрози безпеці держави розглядаються як сукупність умов і факторів, які становлять небезпеку життєво важливим інтересам держави, суспільства й особи шляхом негативного інформаційного впливу на свідомість і поведінку громадян, а також деструктивного впливу на інформаційні ресурси та інформаційно-технічну інфраструктуру.

Здійснено поділ інформаційних атак на два види залежно від об'єкта впливу: 1) суто технічні інформаційні атаки, направлені на функціонуванні технічного оснащення інформаційних систем; 2) вплив на свідомість людей за допомогою передачі цільової інформації.

Окреслено три основних мети інформаційної війни: контроль інформаційного простору і забезпечення захисту своєї інформації від ворожих дій; використання контролю над інформаційним простором для проведення інформаційних атак на противника; підвищення загальної ефективності збройних інформаційних функцій. Доводиться, що для запобігання зазначеним негативним наслідкам на державному рівні повинні здійснюватися наступні заходи: 1) розвиток системи постійного моніторингу та аналізу інформаційних потоків для своєчасного виявлення потенційних загроз і реагування на них; 2) запровадження програм підвищення інформаційної грамотності серед громадян з метою зменшення вразливості до інформації маніпулятивного характеру та фейкових новин; 3) співпраця з міжнародними партнерами та обмін досвідом у сфері інформаційної безпеки для підвищення ефективності заходів та вдосконалення стратегій протидії загрозам. Саме ці кроки здатні забезпечити високий рівень інформаційної безпеки, який буде сприяти стабільності, безпеці та захищеності національних інтересів.

Ключові слова: інформація, інформаційна конкуренція, інформаційна інфраструктура, інформаційна війна, інформаційний захист, безпекова політика, кібербезпека.

Venglinsky O.O. Information as an object of Ukraine's national security policy.

Attention is drawn to the priority value of information among the objects of the national security policy of Ukraine. It is argued that information freedom requires careful state control and inclusion of information in the list of objects of national security policy.

Information threats to state security are considered as a combination of conditions and factors that pose a danger to the vital interests of the state, society, and individuals through negative informational influence on the consciousness and behavior of citizens, as well as destructive impact on information resources and information-technical infrastructure.

Two types of information attacks are distinguished based on the object of influence: 1) purely technical information attacks aimed at the functioning of the technical equipment of information systems; 2) influencing people's consciousness through the transmission of targeted information.

Three main goals of information warfare are outlined: control of the information space and ensuring the protection of one's information from enemy actions; using control over the information space to conduct information attacks on the opponent; increasing the overall effectiveness of

armed information functions. It is argued that in order to prevent the above-mentioned negative consequences, the following measures should be taken at the State level: 1) development of a system of continuous monitoring and analysis of information flows for timely detection of potential threats and response to them; 2) introduction of information literacy programmes among citizens to reduce vulnerability to manipulative information and fake news; 3) cooperation with international partners and exchange of experience in the field of information security to increase the effectiveness of measures and improve strategies to counter threats. These steps can ensure a high level of information security that will contribute to stability, security and protection of national interests.

Key words: information, information competition, information infrastructure, information war, information protection, security policy, cybersecurity.

Постановка проблеми. Сучасний світ стрімко крокує у цифрову епоху, де інформаційні технології стають рушійною силою людського розвитку. Інформація пронизала всі сфери життя, перетворившись на цінний ресурс, що визначає конкурентні переваги у будь-якій галузі. Це робить інформаційну безпеку одним із ключових аспектів національної безпеки, особливо в умовах геополітичної напруги та зростання кіберзагроз.

Україна, яка з 2014 року зазнає безпрецедентної інформаційної агресії з боку російської федерації, гостро відчуває нагальність посилення інформаційного захисту. Російські спецслужби активно використовують інформаційні операції, пропаганду та кібератаки, намагаючись дестабілізувати українське суспільство, підірвати довіру до влади та інституцій, посіяти розбрат і хаос. У цих умовах захист інформаційного простору України стає стратегічним завданням, реалізація якого пов'язана з необхідністю створення ефективної та гнучкої системи інформаційної безпеки, здатної протистояти постійно мінливим загрозам. Це потребує комплексного підходу, що охоплює: захист інформаційних ресурсів та інфраструктури від кібератак, протидію інформаційній пропаганді та дезінформації, зростання рівня інформаційної грамотності населення, а також міжнародне співробітництво у сфері кібербезпеки.

Мета дослідження полягає в аналізі системних характеристик інформації як об'єкта національної безпекової політики України в умовах сучасних викликів та загроз, пов'язаних з інформаційною агресією росії.

Стан опрацювання проблематики. Протягом останніх років проблематика інформаційної безпеки набула значної актуальності, ставши ключовим аспектом національної безпеки України в умовах сучасних викликів та загроз, пов'язаних з інформаційною агресією росії. Численні дослідження вітчизняних та зарубіжних вчених, таких як Ю. Горбань, У. Ільницька, О. Левченко, М. Маклуен, Ю. Райхель, В. Хорошко та інші, присвячені проблематиці інформаційної безпеки, свідчать про її багатогранність та складність. Автори цих досліджень аналізують теоретичні засади інформаційної безпеки, вивчають різні аспекти інформаційних загроз, розробляють методи та механізми протидії їм. Однак, у контексті російської агресії, яка ведеться, зокрема, й в інформаційному просторі, дослідження проблематики інформаційної безпеки набуває нових вимірів.

Виклад основного матеріалу. У сучасному світі інформаційна війна стає все більш визначальною. Інформатизація призводить до створення єдиного інформаційного простору, де інформація обмінюється між різними суб'єктами. Однак, це також сприяє зростанню потужності агресивних маніпуляцій. У XXI ст. такі процеси стають серйозною загрозою для інформаційно-психологічної безпеки [1, с. 179-180]. Майкл Шмітт розрізняє широке й вузьке трактування поняття «інформаційна війна». Він зазначає, що характерною особливістю останньої є розгляд інформаційної війни як інформаційних операцій в умовах кризи чи конфлікту [12, с. 366–367].

Зауважимо, що інформаційну безпеку, в аспекті взаємовідношення із загальнодержавною безпекою можливо трактувати у двох варіантах. В одному варіанті тлумачення це самостійний елемент державної оборонної політики та самостійний рівень обороноздатності країни, в іншому варіанті – це елемент певних інших аспектів обороноздатності держави: військової, економічної, політичної обороноздатності тощо. Достатньо повною є наступна дефініція: «*інформаційна безпека* – це стан захищеності важливих інтересів особистості, суспільства і держави, який полягає у мінімізації можливих збитків внаслідок неповної, невчасної або недостовірної інформації, негативного впливу інформації, негативних наслідків функціонування інформаційних технологій та несанкціонованого поширення інформації» [6]. При цьому інформаційні загрози безпеці держави включають негативний вплив на свідомість людей, інформаційні ресурси та інфраструктуру.

Зародження Інтернету надало медійній маніпуляції новітні інструменти соціальної інженерії, що впливають на моделі прийняття рішень завдяки трансформації когнітивної основи сучасної індивідуальності. Інтернет стає чинником, що домінує у визначенні змісту інформації, доступної людям глобально [10]. Користувачі соціальних мереж сприймають інформацію як

створену аналогічними користувачами, тому виявляють високий рівень довіри до представленого контексту, ігноруючи необхідність верифікації правдивості новин і фактів, опублікованих онлайн.

Розвиток подій навколо України демонструє, що країна зіштовхнулася з інформаційною війною та використанням інформаційних операцій. Особливості інформаційного протиборства та воєнного конфлікту характеризуються масштабними бойовими діями регулярних військових формувань та змовою росії з недержавними угрупованнями, що активно діють на території України [7, с. 28].

У сучасному академічному дискурсі Україна ідентифікується як центральна арена першої інформаційної війни, що транслюється в реальному часі, репрезентуючи собою еволюційно розвинену форму «холодної війни», що характеризувалась економічною, ідеологічною та політичною конфронтацією між блоками Сходу (СРСР) та Заходу (США) в період з 1946 по 1989 рік. Аналітична паралель із зазначеною історичною епохою демонструє, що сучасні траєкторії впливу доповнені новітніми інструментами – мас-медіа, інформаційно-комунікаційними технологіями та платформами для негайного доступу до інформації, що уможливлює кваліфікацію цього конфлікту як війни, що ведеться «в прямому ефірі». Інтенсифікація інформаційного впливу в контексті війни «в прямому ефірі» стає інструментом для реалізації згаданої дестабілізації. Основні інформаційні події початку 2022 року, пов'язані з ескалацією військових загроз, свідчать про нову фазу інформаційної війни між росією та Заходом, в якій Україна виступає як основний предмет геополітичного протистояння, використовуючись як інструмент в ширшій стратегії обох сторін. При цьому Україна відстоює власні національні інтереси, зокрема прагнення до євроінтеграції та членства в НАТО, що відповідає амбіціям українського народу, як підтверджується соціологічними дослідженнями, згідно з якими наприкінці 2021 року 62% громадян України підтримали ідею вступу до ЄС, а 58% – до НАТО [9, с. 89]. Цей аналіз репрезентує Україну як визначальний елемент у межах глобальної інформаційної війни, що набуває особливої актуальності в контексті сучасних міжнародних відносин, ідентифікуючи важливість стратегічної комунікації та інформаційної взаємодії як інструментів національної безпеки та оборони.

Інформаційні атаки, на нашу думку, можна розділити на два види, залежно від об'єкта впливу: 1) суто технічні інформаційні атаки, направлені на функціонуванні технічного оснащення інформаційних систем; 2) вплив на свідомість людей за допомогою передачі цільової інформації. В такому випадку інформація вже завдає шкоди не технічному обладнанню, а безпосередньо психіці людини, тобто фактично перетворюється в зброю. Зважаючи на роль інформації у сучасному світі, американець дослідник М. Маклуен зазначав, що війна стає тотальною, коли вона стає війною за інформацію [11]. Він також наголошував, що інформація завжди відігравала важливу роль у війні, але в епоху масових комунікацій її значення зросло ще більше.

Інформаційні війни можуть мати різноманітні цілі: від отримання вигод на політичній арені до воєнної перемоги. Їх важливість полягає у тому, що сучасний світ характеризується високим ступенем залежності від інформації та її швидкого поширення. Інформаційні війни можуть бути проведені як державними структурами, так і недержавними акторами, що робить їх набагато більш небезпечними. Крім того, інформаційні війни можуть мати довготривалий вплив на суспільство, а тому можуть бути використані для зміни суспільного дискурсу та впливу на політичні рішення.

Як підкреслює Ю. Горбань, «антиукраїнська інформаційна кампанія російських ЗМІ, застосування ними новітніх маніпулятивних технологій засвідчили вразливість вітчизняного інформаційного простору. Цей конфлікт став певним каталізатором проблем у двох важливих напрямках нацбезпеки: захисту інформації та боротьби з пропагандою» [3, с. 138]. На жаль, не лише у 2014 році, але й на початок повномасштабного вторгнення 24 лютого 2022 року наша держава фактично не мала належних потужностей для ведення інформаційної та кібернетичної боротьби з державою-агресором, що ускладнило й без того складні обставини в країні.

Думка У. Ільницької підкреслює підвищену актуальність проблем гарантування інформаційної стабільності України через вплив зовнішніх опонентів, які активно маніпулюють інформаційним простором країни. Зокрема, пропагуються ідеї сепаратизму, насильства та національної ворожнечі з метою руйнування національної ідентичності України. Така агресивна інформаційна експансія ставить під загрозу конституційний лад та територіальну цілісність України [4, с. 28].

Питання забезпечення інформаційної безпеки України не обійшов своєю увагою й законодавець. Так, відповідно до Закону України «Про національну безпеку України», національна безпека – це «захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз» [8]. Це охоплює різні сфери суспільства та держави, включаючи освіту, свободу слова, інформаційну та кібербезпеку, захист інформації тощо.

Концепція інформації як важливої складової Закону України «Про національну безпеку» не лише підкреслює її ключову роль у забезпеченні державного суверенітету, але й створює основу для розвитку комплексних механізмів захисту інформації. Це стає необхідною умовою для забезпечення стійкості та безпеки держави, особливо в умовах геополітичних напруг, таких як агресія з боку рф. Відповідно до Закону «Про національну безпеку України», кібербезпека та захист інформаційного простору є пріоритетними завданнями, що потребують інтегрованого підходу та мобілізації ресурсів на всіх рівнях управління.

Ця концепція набуває особливого значення в умовах інформаційної війни та пропагандистських атак. Пропаганда, систематично спрямована на вплив на думку великої кількості людей, стає інформаційною зброєю масового ураження, що використовується нашим ворогом. Це призводить до зростання стратегічної важливості питання захисту інформаційної безпеки держави в умовах війни.

Ще з початком АТО у 2014 році з боку рф почала в геометричній прогресії зростати активність та агресивність інформаційної експансії. Через російські пропагандистські інформаційно-психологічні кампанії, акції, медіазаходи відбувався вплив не лише на суспільну свідомість громадян України, а й на світову громадськість [4, с. 30]. З вторгненням у 2022 році ця ситуація лише погіршилася. Дотепер росія, наприклад, активно просуває у світовій спільноті тези про «геноцид народу Донбасу», й обов'язком України є боротьба з такою дезінформацією, оскільки вона заподіює значну шкоду авторитету нашої держави, та здатна послабити підтримку з боку наших зарубіжних партнерів. Саме тому відстоювання престижу та авторитету нашої країни на міжнародній арені є важливим сегментом інформаційної боротьби.

Інститут національно-стратегічних досліджень США та деякі західні експерти виділяють певне коло структурних елементів інформаційної війни. Одним з основних таких елементів є сплановане ведення психологічної війни. Головною метою якої являється маніпулювання масами. Зазвичай, серед основної мети цих маніпуляцій можна виокремити: внесення в суспільну та індивідуальну свідомість шкідливих ідей та поглядів противника, поширення недостовірної інформації для дезорієнтації та дезінформації, використання образу ворога для індукування страху у власного народу тощо.

Серед цілей, які переслідуються в інформаційній війні, зазвичай виділяють: «контроль інформаційного простору і забезпечення захисту своєї інформації від ворожих дій; використання контролю над інформаційним простором для проведення інформаційних атак на противника; підвищення загальної ефективності збройних інформаційних функцій» [2, с. 91].

Також до послаблення інформаційної стабільності та обороноздатності країни можуть призвести багато факторів, серед яких можна виділити недостатню або відсутню координацію в діях органів державно влади та місцевого самоврядування щодо питань реалізації державної інформаційної політики, освіти та культури, державної політики у сфері кібербезпеки.

Основною причиною недостатньої стабільності суспільства, його вразливості перед загрозою деструктивної пропаганди є перш за все є слабка система освіти, особливо це стосується патріотичного виховання молоді, а також просвітницької роботи з населенням. Тобто, освіченість населення та стійкість його до впливів інформаційних атак є взаємопов'язаними явищами. На сьогодні в Україні помітними є позитивні тенденції у сфері освіти та патріотичного виховання учнів та студентів, це особливо важливо в умовах зовнішньої агресії та внутрішньої нестабільності.

Іншою проблемою інформаційної обороноздатності є недостатня кількість кваліфікованих спеціалістів у сфері кібербезпеки. Створення Департаменту кіберполіції є кроком у напрямку посилення заходів щодо кібербезпеки, але організація знаходиться в стані розвитку й потребує подальших зусиль для ефективного функціонування. Отже, Україна відчуває нестачу ресурсів для забезпечення інформаційної безпеки, і це робить країну вразливою перед сучасними кіберзагрозами.

При несприятливому розвитку подій зазначені недоліки в комплексній системі інформаційного захисту можуть призвести до руйнування інформаційного простору держави, або виникненню конфліктів в суспільстві та хаосу в системі державного управління. Для запобігання зазначеним негативним наслідкам, науковці наголошують на необхідності здійснення таких заходів на державному рівні, як: 1) здійснення превентивних заходів у сфері інформаційної безпеки, спрямованих на попередження можливих зовнішніх та внутрішніх інформаційних загроз; 2) оперативне та ефективне реагування у випадку інформаційної атаки з боку супротивника та активний контрнаступ з метою локалізації та ліквідації інформаційної загрози; 3) створення системи протидії можливим загрозам [4, с. 31]. Ми вважаємо, що розвиток системи постійного моніторингу та аналізу інформаційних потоків для своєчасного виявлення потенційних загроз і реагування на них; запровадження програм підвищення інформаційної грамотності серед громадян з метою зменшення вразливості до інформації маніпулятивного характеру та фейко-

вих новин, а також співпраця з міжнародними партнерами та обмін досвідом у сфері інформаційної безпеки для підвищення ефективності заходів та вдосконалення стратегій протидії загрозам здатні забезпечити високий рівень інформаційної безпеки, який буде сприяти стабільності, безпеці та захищеності національних інтересів України.

Окрім безпосередньо інформаційного тиску з боку росії, О. Левченко зазначає, що негативними чинниками для України в зазначеній сфері є систематичний інформаційний тиск і з боку інших держав та їх союзів (коаліцій), політична нестабільність, а також нестійкість вітчизняного інформаційного простору [5, с. 57]. На нашу думку, означені фактори мають не меншу загрозу ніж безпосередньо агресивна інформаційна кампанія з боку росії, оскільки Україна наразі фактично знаходиться на кордоні між двома різними та значною мірою ворожими інформаційними таборами: західним (ЄС, США та ін.) і східним табором (рф, Близький схід, КНР та ін.).

Проблема нашої держави полягає у тому, що фактично ще нещодавно ми належали до умовно окресленого нами східного інформаційного блоку, але з набуттям незалежності поступово почали переймати західні цінності та західну модель життя. Зміна пріоритетів, зокрема щодо інформаційного простору, призвела не лише до внутрішньополітичної кризи, а й до проблем у зовнішній політиці, оскільки рф сприйняла це як остаточний перехід України у «ворожий табір», після чого й розгорнула найбільш масову інформаційну війну за всю історію незалежності нашої держави. Країни західного інформаційного простору, хоча й підтримали Україну, але виявилися неспроможними ефективно протистояти інформаційному тиску з боку рф.

Такі агресивні інформаційні дії мають прямий негативний вплив на інформаційну обороноздатність України, оскільки країни ЄС є одними з головних союзників у боротьбі з агресією східного сусіда. Ослаблення позицій країн Заходу може безпосередньо позначитися на зовнішній та внутрішній стабільності України. Боротьба з рф розпочалася під гаслами «руху до Європи», і втрата підтримки ЄС може спричинити суспільну та політичну дезорієнтацію України, що зробить її легкою мішенню для ворожої пропаганди.

Тож інформаційна війна стає одним із вирішальних факторів перемоги в сучасних умовах. Це особливо важливо для України, яка веде війну з росією, що переважає у військовому потенціалі та, навіть, має ядерну зброю. Україна має всі шанси досягти успіху в цій війні, якщо зможе ефективно впливати на ситуацію за кордоном та забезпечити підтримку країн Заходу. Рівень політичної підтримки, обсяги наданої допомоги та масштаби запроваджених санкцій проти агресора залежать від того, як за кордоном сприймаються події в Україні. Якщо Україна зможе ефективно впливати на міжнародну думку та переконати країни заходу у своїй правоті, то вона отримає значну підтримку та допомогу в боротьбі з агресором.

Після початку масштабного вторгнення військ росії, всі раніше застосовані методи інформаційної війни значно загострилися, а також з'явилися нові способи впливу на свідомість громадян. Наприклад, обстріли житлових районів, торгових центрів та енергетичної інфраструктури націлені на впливання на моральний стан громадян України з метою їх психологічного виснаження та зниження психологічної готовності до продовження опору. Крім того, психологічний тиск спрямовується і проти українських військових. Відбувається це зокрема за допомогою закликів до військових про те, що з ними буде простіше «домовлятись» аніж з офіційною владою України, які були висловлені лідером росії у його зверненні 24 лютого 2022 року. Також застосовуються показові та особливо жорстокі страти українських військових, які спеціально фільмуються на камеру. Очевидно, що такі дії мають на меті підрив морального стану української армії.

Висновки. Україна зараз знаходиться на перших рядах в інформаційному протистоянні рф та країн західного інформаційного блоку, таких як ЄС та США. В таких умовах особливо важливим є створення нашою державою ефективної та гнучкої системи захисту інформації, з двох складових елементів: по-перше, боротьби з агресивною пропагандою зовнішніх опонентів, по-друге, систему протидії кібератакам. Ці заходи є необхідними для збереження суверенітету та територіальної цілісності України. Особливу увагу варто приділити боротьбі з розповсюдженням неперевірених даних через проросійські медіа, через які агресор чинить особливо інтенсивний тиск на свідомість населення нашої держави, що потенційно несе небезпеку внутрішній стабільності та обороноздатності держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Богуш В., Кривуца В., Кудін А. Інформаційна безпека : Термінологічний навчальний довідник / за ред. В.Г. Кривуци. Київ: ООО «Д.В.К.», 2004. 508 с.
2. Бржевська З.М., Довженко Н.М., Киричок Р.В., Гайдур Г.І., Аносов А.О. Інформаційні війни: проблеми, загрози та протидія. *Кібербезпека: освіта, наука, техніка*. 2019. № 3 (3). С. 88–96. DOI: 10.28925/2663-4023.2019.3.8896.
3. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управлін-*

ня при Президентові України. 2015. № 1. С. 136–141.
4. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Humanitarian vision*. 2016. Vol. 2, No 1. С. 27–32.
5. Левченко О.В. Система заходів протидії інформаційним операціям. *Збірник наукових праць Харківського університету Повітряних Сил*. 2016. Вип. 3 (48). С. 57–60.
6. Панченко О.А. Проблеми правового забезпечення державного управління інформаційною безпекою. *Державне управління: удосконалення та розвиток*. 2019. № 11. DOI: 10.32702/2307-2156-2019.11.3.
7. Пєвцов Г.В., Залкін С.В., Сідченко С.О., Хударковський К.І. Інформаційно-психологічні операції Російської Федерації в Україні: моделі впливу та напрями протидії. *Наука і оборона*. 2015. № 2. С. 28–32.
8. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII (із змін.) // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.
9. Синчак Б. Прямоефірна інформаційна війна та російсько-українська війна 2022-го на медійному плацдармі. *Український інформаційний простір*. 2022. № 2 (10). С. 85–97. DOI: https://doi.org/10.31866/2616-7948.10.2022.269826.
10. Хорошко В., Хохлачова Ю., Прокофьєв М. Концепція застосування інформаційних впливів та протидій інформаційній зброї. *Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні*. 2016. Вип. 1 (31). С. 9–22.
11. McLuhan, M. Understanding Media The extensions of man. London and New York: Routledge, 1964.
12. Schmitt M. Wired warfare: Computer network attack and jus in bello. *International Review of the Red Cross: Journal of International Humanitarian Law*. Vol. 84, No 846. Pp. 121–163.