УДК 342.7
DOI https://doi.org/10.32782/2663-6170/2024.37.26

ОСОБЛИВОСТІ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНИХ УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

FEATURES OF INFORMATION SECURITY POLICY IN THE MODERN CONDITIONS OF MARTIAL ARTS IN UKRAINE

Курсик О.В.,
аспірант кафедри національної безпеки та політології Національного університету «Острозька академія»

Стаття присвячена дослідженню особливостей політики інформаційної безпеки в сучасних умовах воєнного стану в Україні. Визначено, що інформаційну безпеку наділяють важливим значення в процесі забезпечення інтересів кожної країни. Формування розвиненого та захищеного інформаційного простору виступає обов'язковою передумовою для розвитку не лише суспільства, але держави в цілому. Протягом останніх років на світовій арені можна спостерігати якісну трансформацію управлінських процесів, пов'язана із активізацією впровадженням новітніх інформаційно-комунікаційних технологій. Водночас зростає загроза незаконного втручання до інформаційних систем, що посилює важливість результатів подібного втручання. Через це, доволі багато зарубіжних країн прикладають чимало зусиль для вирішення проблеми захисту інформаційних даних. Це зумовлено тим, що ті держави, які не в змозі забезпечити особисту інформаційну безпеку, втрачають конкурентоспроможність на світовій арені, в результаті чого не залучаються до боротьби за розподіл ринків та ресурсів. Тому можливо стверджувати, що однією із причин, через які великі держави перестали існувати була їх неспроможність дієво управляти на своїй території і наявність розбіжностей інформаційної структури з новітніми умовам існування. Відтак, беззаперечно, що існування кожної розвиненої держави пов'язане із системою забезпечення інформаційної безпеки, що вимагає законодавчого відображення функцій та повноважень державних органів влади у даній сфері.

Вже пройшло три роки з початку повномасштабного вторгнення Росії та територію нашої держави. Воєнні дії точаться не лише на полі бою, але водночас має місце й «гібридна війна» в інформаційному просторі. Росія старається зламати авторитетність нашої держави на міжнародній арені тому безперервно поширює інформаційні дані, які породжують та все більше посилюють зневіру у суспільстві, а також несуть репутаційні небезпеки для України. Тому, дана проблематика набуває виняткової актуальності в умовах сьогодення.

Встановлено, що під інформаційною безпекою зазвичай розуміють багатоаспектну сферу роботи, де лише завдяки використанню послідовного та комплексного підходу може досягнути успіху. Визначено, що політика інформаційної безпеки нашої держави в умовах сьогодення відповідає новітнім інформаційним викликам. За рахунок посилення інтеграційних та глобалізаційних процесів можна спостерігати за активізацією впровадження сучасних інформаційних технологій та інструментів, а інформація виступає важливим елементом діяльності країни.

Ключові слова: інформація, інформаційне середовище, інформаційна безпека, національна безпеки, державна політика інформаційної безпеки.

The article is devoted to the study of the features of information security policy in the modern conditions of martial law in Ukraine. It is determined that information security is given important importance in the process of ensuring the interests of each country. The formation of a developed and protected information space is a mandatory prerequisite for the development of not only society, but also the state as a whole. In recent years, a qualitative transformation of management processes has been observed on the world stage, associated with the increased implementation of the latest information and communication technologies. At the same time, the threat of illegal interference in information systems is growing, which increases the importance of the results of such interference. Because of this, quite a few foreign countries are making great efforts to solve the problem of information data protection. This is due to the fact that those states that are unable to ensure personal information security lose their competitiveness on the world stage, as a result of which they are not involved in the struggle for the distribution of markets and resources. Therefore, it can be argued that one of the reasons why great powers ceased to exist was their inability to effectively govern their territory and the presence of discrepancies in the information structure with the latest conditions of existence. Therefore, it is undeniable that the existence of every developed state is connected with the system of ensuring information security, which requires a legislative reflection of the functions and powers of state authorities in this area.

Three years have already passed since the beginning of the full-scale invasion of Russia and the territory of our state. Military actions are taking place not only on the battlefield, but at the same time a "hybrid war" is also taking place in the information space. Russia is trying to break the authority of our state in the international arena, therefore it continuously disseminates information data that generate and increasingly increase distrust in society, and also carry reputational dangers for Ukraine. Therefore, this issue is becoming exceptionally relevant in today's conditions.

It has been established that information security is usually understood as a multifaceted field of work, where only through the use of a consistent and comprehensive approach can success be achieved. It has been determined that the information security policy of our state in today's conditions meets the latest information challenges. Due to the strengthening of integration and globalization processes, it is possible to observe the intensification of the implementation of modern information technologies and tools, and information is an important element of the country's activities.

Key words: information, information environment, information security, national security, state information security policy.

Постановка проблеми. Активізація розвитку інформаційно-комунікаційних технологій в усіх сфери людської життєдіяльності і держави в цілому зумовила зростання потреби у дослідженні проблем забезпечення інформаційної безпеки України. Варто зазначити, що інформаційна безпека виступає невід'ємною складовою національної безпеки, в той час, коли захист суспільства від інформаційних впливів є найбільш пріоритетним завдання будь-якої держави. Зважаючи на чимало конфліктів між державами на світовій арені, зокрема і теперішню російсько-українську війну, захист вітчизняного інформаційного середовища від різноманітних інформаційних небезпек, забезпечення гарантії інформаційної безпеки відіграє все більшої ролі та стають важливими факторами подальшого розвитку нашої держави.

Політика інформаційної безпеки вважається найважливішим засобом управління інформаційними ресурсами в новітньому світі, який повинен зважати не тільки на звичайні умови, але й особливі аспекти у воєнних умовах для забезпечення надійного захисту інформаційних даних та дотримання державних інтересів. Проте, на сьогоднішній день можна з сумом констатувати, що політика інформаційної безпеки нашої країни є недосконалою і тому породжує небезпеки та напади зі сторони ворога.

Аналіз останніх досліджень і публікацій. Дана проблематика висвітлювалася такими ученими як В. Богданович, І. Боднар, В. Виздрик, Б. Ворович, І. Залєвська, А. Колгатин, В. Кривошеїн, С. Лисенко, Є. Марко, О. Мельник, А. Нашинець-Наумова, О. Невельська-Гордєєва, В. Нечитайло, М. Савлюк, О. Троянський, Г. Удренас та іншими.

Виділення невирішених раніше частин загальної проблеми. Не зважаючи на існування низки досліджень даної проблематики, сучасні умови, в яких перебуває наша країна породжують необхідність у розкритті особливостей політики інформаційної безпеки в контексті російсько-української війни.

Формулювання цілей статті (постановка завдання). Мета статті – дослідження особливостей політики інформаційної безпеки в сучасних умовах воєнного стану в Україні.

Виклад основного матеріалу дослідження. Під інформаційною безпекою зазвичай розуміють багатоаспектну сферу роботи, де лише завдяки використанню послідовного та комплексного підходу може досягнути успіху. Головні на даний час проблеми в сфері використання інформаційних систем та технологій, пов'язані переважно із забезпеченням відкритості, цілісності та секретності інформаційних ресурсів тощо. Не варто інформаційну безпеку обмежувати тільки із захистом від незаконного доступу до інформаційних даних, оскільки дане поняття є принципово широким. Це пов'язано з тим, що не тільки незаконний доступ, але й будь-який збій в інформаційній системі може завдати певну шкоду суб'єктам інформаційних відносин. Тому, в сучасних воєнних умовах, питання політики інформаційної безпеки набуває виняткової актуальності.

Початок російсько-української війни можна вважати своєрідним випробуванням всіх органів публічної влади в Україні та обумовила появу багатьох проблем в сфері стратегічних комунікацій. Більшість з них вдалося оперативно розв'язати, проте це не означає, що не треба продовжувати дану роботу.

Для України постала потреба в модернізації інформаційного складника національної безпеки, насамперед українською владою здійснено реформу інформаційного законодавства. Першим нормативно-правовим актом у цій галузі стало рішення РНБО України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної без-пеки України», затверджене 28 квітня 2014 року. Документ містив указівки для вищих органів виконавчої влади розробити проєкти про зміни до законів щодо механізмів протидії інформаційно-психологічному впливу та вжити заходів щодо запобігання кібернетичним загрозам та захисту інформаційних мереж. Автори рішення слушно зазначили, що останнім часом Російська Федерація поширює недостовірну, неповну, упереджену інформацію про Україну, через що намагається маніпулювати суспільною свідомістю в Україні та за її межами. Нова Стратегія національної безпеки, затверджена 2015 року указом Президента України, акцентувала на нагальній потребі вдосконалення ефективності сектору безпеки і оборони, модернізації елементів системи національної безпеки України, що зумовлена окупацією російською федерацією територій України. У цій Стратегії стан інформаційної безпеки України, у зв'язку із загрозами з боку країни-агресора, окреслений як інформаційна війна проти України [1, с. 228].

Сучасний стан забезпечення національної та інформаційної безпеки України потребує розробки науково обґрунтованої державної політики та стратегії в цій галузі, визначення системи національних цінностей, життєво важливих інтересів особистості, суспільства та держави, визначення зовнішніх і внутрішніх загроз цим інтересам, розвитку інформаційної інфраструктури, пошуку ефективних заходів для забезпечення безпеки в усіх її сферах життєдіяльності, налагодження ефективної взаємодії державних органів та належного законодавчого закріплення. Головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні

ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав'язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку [2; 3].

До проблем забезпечення інформаційної безпеки України відносять загрози національним інтересам і національній безпеці в інформаційній сфері: прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації; намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації [4, с. 125].

Як окрему загрозу інформаційній безпеці справедливо виділяють діяльність ЗМІ та захист професійної діяльності журналістів, особливо в умовах війни. Суспільство в цілому і кожен його член має бути обізнаним, виробити інформаційну свідомість, мати доступ до інформації і вміти критично її сприймати. Для формування інформаційної безпеки держава має здійснити низку заходів щодо використання інформації громадянами, а саме: забезпечити доступ до інформації навіть у найвіддаленіших районах, проводити інформаційно-роз'яснювальну роботу з населенням з метою формування їх особистої інформаційної безпеки. При цьому необхідно мати на увазі, що в сучасних умовах на зміну традиційним формам масованої ідеологічної пропаганди приходять глибоко розроблені, багаторівневі й диверсифіковані PR-технології. Такі технології справляють вплив як на раціональному, такі, насамперед, емоційно-психологічному, підсвідомому, ірраціональному рівнях; вони здатні маніпулювати свідомістю широких верств населення, руйнувати традиційні та створювати нові форми, засоби та механізми ідентифікації особистості, колективу, нації [5].

Умови життя нашої країни змушують по-іншому думати про безпеку. Якщо до лютого 2022 року світ навколо нас здавався безпечним, то сьогоднішні виклики становлять набагато більшу небезпеку, ніж у звичайні часи. Об'єктом цього впливу російської пропаганди є не тільки окремі особи, групи осіб, а й цілі народи. Психологічний вплив здійснюється за допомогою засобів масової інформації, основа використання цього впливу перцептивна і поверхнева. Як показують сучасні реалії, масштабні інформаційні атаки, боти та фейкові витвори є ефективними інструментами для заплутування, залякування, маніпулювання та паніки населення. Спеціально створені джерела інформації підсвідомо сприймають інформацію і привчають людину вірити в неї. Тепер Україні доводиться бачити не лише негативну сторону війни. Ця війна є також можливістю створити нову Україну. З цієї точки зору війна відкриває нові перспективи «початку заново» і може бути потужним чинником модернізації. В змісті військових дій зросла значимість інформаційно-технічного протиборства. Перевага поінформованості є важливою для перемоги в повітряних, морських і сухопутних боях. Про це свідчить досвід сучасних збройних конфліктів і локальних війн. Основними заходами щодо забезпечення ефективної діяльності у сфері управління національною інформаційною безпекою є: розробка показників ефективності національної системи захисту інформації; відстежувати та виявляти спалахи нестабільності та загроз; організовувати фундаментальні та прикладні наукові дослідження в галузі захисту інформації; розробка відповідної законодавчої бази [6, с. 198].

Хоча Україна активно проводила політику інформаційної безпеки в довоєнний період, але зараз перед нею постають нові завдання – захист від нових загроз гібридної війни, протидія дезінформації та «фейковим» новинам, збереження інформаційної стабільності суспільства в умовах війни. Війна, що відбувається на теренах нашої держави, характеризується посяганням на інформаційно-кібернетичний простір України, на конституційні основи демократії, незалежності та на інформаційно-психологічну безпеку населення України. Наразі Україна переживає нелегкий період у забезпеченні національної безпеки, проходячи через купу загроз, пов'язаних із гібридною війною, де вміло використовуються прийоми дезінформації та поширюються фейкові новини з метою дестабілізації ситуації в країні. Інформаційне вторгнення, маніпуляції, застосування соціально-психологічного впливу є серйозною загрозою як головним засадам демократичного суспільства, так і особистій інформаційно-психологічній безпеці громадян, у тому числі – загрозою є застосування «fake news» з метою політичного впливу та здійснення політичних завдань [7, с. 127].

В умовах війни політика інформаційної безпеки набуває особливо важливого та критичного значення, оскільки інформація може бути використана відверто або приховано для досягнення військових і політичних цілей. Нижче розглянемо основні аспекти політики інформаційної безпеки держави під час війни:

1. Кібервійна. У сучасних конфліктах інформаційна безпека стає одним з основних аспектів бойових дій, оскільки так звані хакерські атаки можуть істотно впливати на роботу критичної інфраструктури держави, роботу транспорту,

освітнього процесу й інших не менш важливих для перемоги компонентів. Держава повинна бути готовою до відповіді на ворожі кібератаки та захист своєї критичної інфраструктури [8, с. 37]. Коли якісно «контратакувати» й «оборонятися» на кіберполі, то противник може відмовитися від своїх планів у цьому напрямі. І всі свої сили залучатиме до відбиття саме «кіберконтратак».

2. Пропаганда та психологічна війна. Інформація може бути використана для маніпулювання громадською думкою та зміни ставлення до війни. Ворог у доступний спосіб може поширювати власні наративи та пропаганду і, використовуючи політтехнології та психологічні маніпуляції, домогтися того, що громадяни держави, яка піддається нападу, самостійно поширюватимуть таку неправдиву та відверту дезінформацію серед власних друзів (це стосується власне соціальних мереж і пліток). Така робота буде відвертим підіграванням ворогу та його спецслужбам. Держава повинна мати стратегію протидії таким впливам і розвивати контрпропаганду. Для цього потрібна відповідна стратегія та кваліфіковані фахівці з досвідом роботи в інформаційному полі [9, с. 420].

3. Захист інформації. У військових операціях держава повинна забезпечити захист конфіденційної інформації від ворожих розвідувальних дій. Конфіденційність і захист такої інформації сприятиме успішним наступальним і контрнаступальним операціям [10, с. 46]. Саме так, як це було з контрнаступом Збройних сил України на харківському напрямку восени 2022 року (що дало змогу звільнити значну частину окупованих територій) чи успішною атакою на Кримський міст восени того ж року (завдяки чому вдалося порушити логістичні ворожі ланцюжки на півдні України).

4. Гуманітарні аспекти. Держава повинна також враховувати гуманітарні аспекти інформаційної безпеки, забезпечуючи доступ до гуманітарної інформації та дотримання прав людини під час конфлікту. На жаль, відкритістю джерел гуманітарної інформації може скористатися ворог, щоб створювати провокації та поширювати небезпечну для всіх громадян дезінформацію [11, с. 63].

У зв'язку з повномасштабним військовим вторгненням можна виокремити такі напрями політики інформаційної безпеки Україні:

1. Захист цінностей і держави від дій агресора, спрямованих на незалежність України, її територіальну цілісність та суверенітет.

2. Інформаційний захист української культури та самовизначення.

3. Підвищення рівня суспільної свідомості, медіаграмотності населення, розвитку інформаційного суспільства.

4. Сприяння реалізації інформаційних прав фізичних осіб.

5. Інформаційне забезпечення громадян України, які проживають на тимчасово окупованих територіях.

6. Посилення надійності системи стратегічних комунікацій, інформаційної безпеки на міжнародному рівні [12, с. 23]. Забезпечення вище наведених напрямів потребує розробки та реалізації цілого комплексу заходів, пов'язаних з відкритість та загальнодоступністю, абсолютною повнотою та секретністю інформаційних даних, мережевою безпекою, а також безпекою програмно-технічного забезпечення.

Отже, маніпулятивний вплив на суспільну свідомість завжди використовується з метою досягнення певних політично-економічних результатів. Так, перед початком повномасштабного вторгнення російських військ на територію нашої держави постійно поширювалися неправдиві інформаційні дані (фейки), зокрема через соціальні мережі, спрямовані на введення суспільства в оману. Тому, надалі, держава повинна безперервно моніторити та реагувати на використання даної маніпулятивної техніки.

Висновки та перспективи подальших розвідок у цьому напрямі. Таким чином, загалом можна вважати, що політика інформаційної безпеки нашої держави в умовах сьогодення відповідає новітнім інформаційним викликам. За рахунок посилення інтеграційних та глобалізаційних процесів можна спостерігати за активізацією впровадження сучасних інформаційних технологій та інструментів, а інформація виступає важливим елементом діяльності країни. Через це подальші розвідки в сфері політики інформаційної безпеки України повинні спрямуватися на розвиток суспільної медіаграмотності та додержання громадських прав стосовно захисту та використання інформаційних даних тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Матвієнків, С., Пучко Я. Російсько-українська війна в інформаційному вимірі: виклики та їх подолання. *Вісник Прикарпатського університету. Серія: Політологія*. 2025. № 20. С. 225-232.

2. Боднар І. Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014. № 1. URL: https://core.ac.uk/download/pdf/141443493.pdf

3. Троянський О.А. Інформаційна безпека в Україні: сучасний стан та перспективи розвитку. Науковий вісник Льотної академії. 2021. Випуск 5. С. 185-194

4. Нашинець-Наумова А.Ю. Теоретико-правові основи забезпечення інформаційної безпеки українського суспільства. Вісник НТУУ «КПІ». Політологія. Соціологія. Право. 2013. Випуск 4(20). С. 124-127

5. Кривошеїн В. Політика інформаційної безпеки України в умовах військового стану. https://hups.mil.gov.ua/assets/doc/science/stud-conf/cuchasna-viina-2023.pdf#page=53

6. Виздрик В.С., Мельник О.М. Інформаційна безпека в Україні: сучасний стан. Міжнародний науковий журнал «Грааль науки». 2023. № 24. С. 196-202

7. Невельська-Гордєєва О., Нечитайло В. Феномен «fake news» в контексті забезпечення інформаційної безпеки держави. Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія. 2022. № 1 (52). С. 123-135

8. Лисенко С. Історія досліджень інформаційної безпеки як об'єкта правовідносин. Supremația Dreptului. 2016. № 2. С. 34–44

9. Колгатин А.Г. Інформаційна безпека в системах відкритої освіти. Освітні технології та суспільство. 2014. № 1. С. 417-425

10. Богданович В.Ю., Ворович Б.О., Марко Є.І. Інформаційна безпека як основа воєнної безпеки держави та суспільства. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, 2018. № 3. С.44–48

11. Савлюк М. Теоретико-методологічні засади дослідження інформаційної безпеки. *Вісник Прикарпатського університету. Серія: Політологія. 2023. №* 1.15. С. 60-68.

12. Залєвська І.І., Удренас Г.І. Інформаційна безпека України в умовах російської військової агресії. Південноукраїнський правничий часопис. 2022. № 1-2. С. 20-26.