4. МАКРОЕКОНОМІЧНІ МЕХАНІЗМИ

DOI: https://doi.org/10.32782/mer.2024.104.16
УДК 329.09.5

АНАЛІЗ СУЧАСНОГО СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Валерій Олександрович Котляров[1]

У статті досліджено питання щодо аналізу сучасного стану інформаційної безпеки в Україні. Наголошено на тому, що сучасні реалії свідчать про ефективність масових інформаційних атак, ботів та фейків як інструментів дезорієнтації, залякування та маніпуляції суспільством. Питання інформаційної безпеки та культури, особливо в умовах війни, стає питанням виживання людини, суспільства та держави. Це стосується не лише інтересів держави, а й прав та свобод кожної особи. Основою сучасної інформаційної безпеки є цілісність даних, доступність інформації, конфіденційність та надійність її збереження. Як висновок, сказано про те, що аналіз сучасного стану інформаційної безпеки держави вказує на те, що забезпечення цієї безпеки ґрунтується на діяльності інформаційних структур держави. Ці структури повинні забезпечити безпеку інформації держави та її суб'єктів в умовах глобалізації та зростаючих загроз міжнародного тероризму. На жаль, в Україні існує низка негативних чинників, що ускладнюють створення таких інформаційних структур, а одним з них є неузгодженість між органами державної влади у питаннях забезпечення інформаційної безпеки. Сучасні загрози інформаційній безпеці виходять за межі нашої держави і мають глобальні наслідки, що посягають не лише на національний простір, а й на міжнародний порядок. Щоб запобігти та протистояти сучасним інформаційним загрозам, необхідно не лише прийняти відповідні нормативно-правові акти, а й забезпечити функціонування інституційного механізму забезпечення інформаційної безпеки, включаючи освітні програми. Це передбачає системну діяльність державно-правових інститутів, що мають ефективно реалізовувати національні інтереси в інформаційній сфері. Вони повинні бути здатні не лише реагувати на поширення інформаційних маніпуляцій та неправдивої інформації, а й передбачати конфлікти та формувати інформаційну культуру суспільства. Окрім того, з урахуванням глобальних загроз та викликів, ефективна протидія інформаційній агресії можлива за участю міжнародних організацій, інституцій та міжнародної спільноти.

Ключові слова: *загрози, безпека, інформація, джерела, війна.*

Постановка проблеми. Забезпечення інформаційної безпеки є ключовим для будь-якої держави, оскільки створення безпечного і розвиненого інформаційного середовища є важливою умовою для прогресу суспільства і країни. Останнім часом у світі спостерігається значний розвиток у сфері управління, що пов'язаний із впровадженням сучасних інформаційних технологій. Це призводить до зростання загроз несанкціонованого доступу до інформаційних систем, аналіз наслідків таких втручань стає дедалі важливішим. У багатьох країнах все більше уваги звертається на захист інформації та розробку способів її забезпечення.

Країни, які не можуть забезпечити свою інформаційну безпеку, стають менш конкурентоспроможними і не можуть ефективно брати участь у боротьбі за ринки та ресурси. Неспроможність ефективного управління та недостатня адаптованість інформаційної інфраструктури до нових умов існування сприяли зникненню багатьох держав. Тому у будь-якій розвиненій країні необхідно мати систему забезпечення інформаційної безпеки, а функції та повноваження відповідних державних органів повинні бути закріплені у законодавстві.

Аналіз останніх досліджень та публікацій. Питанню щодо аналізу сучасного стану інформаційної безпеки в Україні були присвячені праці таких вчених як Морозов О.Л. [4], Кавун С.В. [3], Носов В.В., Манжай О. В., Боднар І. [6], Саприкін О.А. [7] та інших.

Україна сьогодні також стикається з великим впливом інформаційних процесів. Війна, що ведеться не лише на територіальному, а й на інформаційному просторі, ставить під загрозу національну безпеку.

Формування цілей статті (постановка завдання). Всебічно дослідити сучасний стан інформаційної безпеки в Україні, запропонувати шляхи покращення ситуації.

Виклад основного матеріалу дослідження. Поняття інформаційної безпеки охоплює два аспекти. З одного боку, це вільний доступ до різноманітних дже-

[1] *Валерій Олександрович Котляров,* докторант
Національного авіаційного університету
ORCID: https://orcid.org/0000-0002-2291-3199
E-mail: kotva0503@gmail.com

рел інформації та забезпечення якісного інформування громадян. З іншого боку, це контроль за обігом таємної інформації, збереження цілісності суспільства та захист від негативних впливів інформації. Розв'язання цих завдань сприятиме захисту інтересів суспільства і держави, а також забезпечить громадянам право на доступ до всебічної та якісної інформації.

Проблема забезпечення інформаційної безпеки у державі включає різноманітні завдання, такі як розроблення теоретичних основ забезпечення безпеки інформації, створення системи органів, що відповідають за інформаційну безпеку, керування захистом інформації, створення нормативно-правової бази, виробництво засобів захисту інформації, підготовка фахівців тощо.

Загальні питання інформаційної безпеки держави охоплюють захист та обмеження обігу інформації, захист інформаційної інфраструктури, безпеку розвитку інформаційної сфери, захист національного інформаційного ринку, попередження інформаційного тероризму та інформаційної війни.

Існують два аспекти вивчення інформаційної безпеки: вона є як самостійним елементом національної безпеки будь-якої країни, так і інтегрованою складовою інших видів безпеки, таких як військова, економічна, політична тощо.

Інформаційна безпека полягає в захищеності життєво важливих інтересів особистості, суспільства і держави, мінімізації завданого збитку через неповноту, невчасність і недостовірність інформації, а також через негативний інформаційний вплив і несанкціоноване поширення інформації [1, с. 33].

Проблема забезпечення інформаційної безпеки України знайшла відображення у законодавстві, яке визначає основні складові національної безпеки, національні цілі та принципи її захисту. Захист інформаційного суверенітету держави тісно пов'язаний з інформаційною безпекою, що охоплює захищеність внутрішньої інформації та контроль над інформаційними потоками.

Ми спостерігаємо процес інформаційного впливу, який спрямований на свідомість суспільства. Цей вплив охоплює як окремих осіб чи групи людей, так і цілі держави. Він здійснюється через засоби масової інформації з використанням легкої сприйняття та поверховості. Сучасні реалії свідчать про ефективність масових інформаційних атак, ботів та фейків як інструментів дезорієнтації, залякування та маніпуляції суспільством.

Питання інформаційної безпеки та культури, особливо в умовах війни, стає питанням виживання людини, суспільства та держави. Це стосується не лише інтересів держави, а й прав та свобод кожної особи. Основою сучасної інформаційної безпеки є цілісність даних, доступність інформації, конфіденційність та надійність її збереження [2, с. 2].

Інформаційна безпека включає нормативно-політичну та інституційну складові, що передбачають діяльність відповідних органів та використання програмно-технічних засобів. Україна приділяє велику увагу цьому питанню, що відображено в документах, таких як «Доктрина інформаційної безпеки України» та рішення РНБО щодо реалізації єдиної інформаційної політики в умовах воєнного стану.

Створення глобального інформаційного простору збільшило загрози для безпеки, особливо від стратегічних противників або глобального тероризму. Захист від таких загроз стає пріоритетним завданням, яке мають вирішувати Збройні Сили та їх фахівці з безпеки.

Збільшується значення правильного управління інформаційними масивами та їх використання, що стає найважливішим завданням для військовослужбовців. Інформаційна безпека Збройних Сил є гарантією безпеки самої держави. Захист військових інформаційних ресурсів має стати пріоритетом для фахівців з безпеки.

На шляху до забезпечення інформаційної безпеки та державної політики України стоять численні виклики:

1) монополізація інформаційного ринку – це може призвести до контролю над інформаційним простором держави або окремими його секторами зовнішніми структурами, що загрожує незалежності інформаційного простору;

2) блокування діяльності державних ЗМІ – заборони або обмеження їхньої роботи можуть призвести до обмеження доступу до інформації для української та закордонної аудиторії;

3) низька ефективність інформаційного забезпечення – це через дефіцит кваліфікованих кадрів та відсутність системи формування та реалізації державної інформаційної політики [3, с. 44].

У розвитку вітчизняної індустрії інформації можливі наступні загрози:

1) обмеження доступу до новітніх технологій (це може призвести до технологічної відсталості та залежності від закордонних ринків);

2) відтіснення вітчизняних виробників (це може стати перешкодою для розвитку внутрішнього ринку та економіки);

3) загрози для безпеки інформаційно-телекомунікаційних систем (це може включати незаконне збирання та використання інформації, порушення технологій обробки інформації, впровадження шкідливих програм, а також несанкціонований доступ до конфіденційної інформації).

Ці виклики потребують системного підходу та ефективних заходів для забезпечення інформаційної безпеки та стійкості держави.

Серйозною загрозою для військового устрою є спрямований вплив на моральний стан військових через фальсифікацію історії військових подій, збільшення соціальної напруги та спроби залучити військовослужбовців до політичних конфліктів. Засоби масової інформації часто виступають в якості виконавців таких загроз, намагаючись створити напружену атмосферу. У деяких випадках навіть контакт з представниками преси може призвести до спеціального впливу на подану ними інформацію, що загрожує втраті бойового духу військових. Це може призвести не лише

до психологічних розладів, що ведуть до вчинення військових злочинів або дезертирства, а й до формування груп, спрямованих на свідоме підрив обороноздатності країни.

Розповсюдження радикального ісламізму є серйозною загрозою для інформаційної безпеки армії. Військовослужбовець, який піддавався спеціальній психологічній терапії, може перестати відчувати себе частиною військового колективу і бачити себе як член релігійної спільноти, що створює серйозну загрозу для інформаційної безпеки військових частин.

Технічні загрози інформаційного характеру стосуються як функціонування інформаційних систем, так і збереження конфіденційної інформації, що передається військовими каналами зв'язку. Вони можуть бути викликані навмисним пошкодженням систем та крадіжкою інформації або недбалістю окремих співробітників [4]. Необхідно забезпечити підвищений рівень безпеки автоматизованих систем управління та навчання персоналу за вимогами захисту інформації.

Недостатня розвиненість законодавчої бази стосовно захисту інформації та протидії новим загрозам є серйозною проблемою. Багато явищ інформаційного простору не відображені в нормативних актах, що ускладнює застосування заходів відповідальності [6, с. 70]. Тим не менш, розвиток відповідних законодавчих норм у цьому напрямі спрямований на підвищення рівня захисту інформації військових структур.

Однією з найбільш серйозних проблем щодо безпеки є використання соціальних мереж військовослужбовцями, які ненавмисно можуть розголошувати важливу інформацію. Одним із ключових завдань захисту держави є виявлення таких загроз і їх негайне усунення.

Заходи щодо захисту інформації та забезпечення безпеки можна розділити на дві основні групи [7, с. 90]:

– захист інформаційних систем від пошкодження та запобігання витоку та перехоплення інформації.

– захист психіки військовослужбовців від цілеспрямованого інформаційно-психологічного впливу.

Ці заходи повинні бути комплексними, базуватися на нових наукових розробках і програмних продуктах [5, с. 175].

Перша група заходів включає:

– захист військових об'єктів та комп'ютерної техніки від пошкоджень та вторгнень.

– захист інформації, що становить державну або військову таємницю, від витоку та незаконного розголошення.

– розробка засобів електронної розвідки та захисту.

– використання соціальних мереж для дезінформації противника.

– захист систем зв'язку.

Друга група заходів включає:

– профілактика цілеспрямованого впливу на психіку військовослужбовців;

– корекція інформації, що надходить від потенційних супротивників;

– реалізація цих заходів передбачає створення спеціальних підрозділів, які працюватимуть у сфері інформаційної безпеки;

– необхідно контролювати військовослужбовців, які відповідають за засоби зв'язку та передачу інформації, оскільки вони можуть бути об'єктами ворожих атак;

– для протидії спрямованому інформаційно-психологічному впливу, командування Збройних Сил використовує різні методи, такі як проведення досліджень психіки та психологічна робота з військовослужбовцями.

Усі ці заходи мають на меті створити стійкий захист від інформаційного впливу та підвищити готовність військових до відсікання негативної інформації, спрямованої на дестабілізацію їхнього морально-психологічного стану.

Висновки. Отже, аналіз сучасного стану інформаційної безпеки держави вказує на те, що забезпечення цієї безпеки ґрунтується на діяльності інформаційних структур держави. Ці структури повинні забезпечити безпеку інформації держави та її суб'єктів в умовах глобалізації та зростаючих загроз міжнародного тероризму. На жаль, в Україні існує низка негативних чинників, що ускладнюють створення таких інформаційних структур, а одним з них є неузгодженість між органами державної влади у питаннях забезпечення інформаційної безпеки.

Сучасні загрози інформаційній безпеці виходять за межі нашої держави і мають глобальні наслідки, які посягають не лише на національний простір, а й на міжнародний порядок. Щоб запобігти та протистояти сучасним інформаційним загрозам, необхідно не лише прийняти відповідні нормативно-правові акти, а й забезпечити функціонування інституційного механізму забезпечення інформаційної безпеки, включаючи освітні програми.

Це передбачає системну діяльність державно-правових інститутів, що мають ефективно реалізовувати національні інтереси в інформаційній сфері. Вони повинні бути здатні не лише реагувати на поширення інформаційних маніпуляцій та неправдивої інформації, а й передбачати конфлікти та формувати інформаційну культуру суспільства.

Окрім того, з урахуванням глобальних загроз та викликів, ефективна протидія інформаційній агресії можлива за участю міжнародних організацій, інституцій та міжнародної спільноти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Лизанчук В.В. Інформаційна безпека України: теорія і практика: підручник. Львів : ЛНУ ім. Івана Франка, 2017. 725 с.
2. Інформаційна безпека: підручник / під ред. В.В. Остроухова. Київ : Видавництво Ліра-К, 2021. 412 с.
3. Кавун С.В., Носов В.В., Манжай О.В. Інформаційна безпека: навчальний посібник. Ч. 2. Харків : Вид. ХНЕУ, 2018. 196 с.
4. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. URL: http://www.viche.info

5. Шатун В.Т. Інформаційна безпека – невід'ємна складова національної безпеки України. *Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія».* 2016. Т. 267. Вип. 255. С. 174–180.

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

7. Саприкін О.А. Фейк як інструмент інформаційної війни проти України. *Бібліотекознавство. Документознавство. Інформологія*. 2016. № 1. С. 87–94.

8. Hridin O.V., Reznik N.P., Chukina I.V., Krasnorutskyy O.O. and Mykhaylichenko M.V. Mechanisms and tools of personnel management in institutional economics. AIP Conference Proceedings 2413. 2022. DOI: https://doi.org/10.1063/5.0089330

9. Резнік Н.П., Костиляну В.А. Антикризове управління підприємством, як засіб захисту підприємства від банкрутства. *Вісник ХНАУ. Серія : Економічні науки.* 2019. № 4(1). С. 213–223.

10. Zahorodnia A., Reznik N., Chornenka L. Generalization of the influence of foreign experience of the digitalization process on the economic security of enterprises. *Int. J. Innov. Technol. Econ.* № 4(36). DOI: https://doi.org/10.31435/rsglobal_ijite/30122021/7744

REFERENCES:

1. Lyzanchuk, V. V. (2017). Information security of Ukraine: theory and practice: textbook. Lviv: LNU named after Ivan Franko, 725 p.

2. Ostroukhova, V. V. (eds.) (2021). Information security. Textbook. Under the editorship. Kyiv: Lira-K Publishing House, 412 p.

3. Kavun, S. V., Nosov, V. V., Manzhai, O. V. (2018). Information security. Tutorial. Part 2. Kharkiv: Ed. Khneu, 196 p.

4. Morozov, O. L. Information security in the conditions of the modern state and prospects for the development of statehood. http://www.viche.info

5. Shatun, V. T. (2016). Information security is an integral component of the national security of Ukraine. *Scientific works of the Black Sea State University named after Peter Mohyla complex "Kyiv-Mohyla Academy"*, 267, *255*, 174–180.

6. Bodnar, I. (2014). Information security as the basis of national security. *Mechanism of economic regulation*, 1, 68–75.

7. Saprykin, O. A. (2016). Fake as a tool of information war against Ukraine. Library science. Documentary science. *Informatology*, 1, 87–94.

8. Hridin, O. V., Reznik, N. P., Chukina, I. V., Krasnorutskyy, O. O. and Mykhaylichenko, M. V. (2022). Mechanisms and tools of personnel management in institutional economics. AIP Conference Proceedings 2413, https://doi.org/10.1063/5.0089330

9. Reznik, N. P., Kostylyanu, V. A. (2019) Anti-crisis management of the enterprise as a meansprotection of the enterprise from bankruptcy. *KHNAU Bulletin. Series: Economic sciences*, 4(1), 213–223.

10. Zahorodnia, A., Reznik, N., Chornenka, L. Generalization of the influence of foreign experience of the digitalization process on the economic security of enterprises. *Int. J. Innov. Technol. Econ*., 4(36), https://doi.org/10.31435/rsglobal_ijite/30122021/7744

ANALYSIS OF THE CURRENT STATE OF INFORMATION SECURITY IN UKRAINE

Valerii O. Kotliarov[1]

The article examines the issue of analyzing the current state of information security in Ukraine. It is emphasized that modern realities testify to the effectiveness of mass information attacks, bots and fakes as tools for disorientation, intimidation and manipulation of society. The issue of information security and culture, especially in the conditions of war, becomes a matter of survival of man, society and the state. This concerns not only the interests of the state, but also the rights and freedoms of every individual. The basis of modern information security is data integrity, information availability, confidentiality and reliability of its preservation. As a conclusion, it is said that the analysis of the current state of information security of the state indicates that the provision of this security is based on the activities of the information structures of the state. These structures must ensure the security of information of the state and its subjects in the conditions of globalization and growing threats of international terrorism. Unfortunately, there are a number of negative factors in Ukraine that complicate the creation of such information structures, and one of them is the inconsistency between state authorities in matters of ensuring information security. Modern threats to information security go beyond the borders of our state and have global consequences that encroach not only on the national space, but also on the international order. In order to prevent and counter modern information threats, it is necessary not only to adopt relevant normative legal acts, but also to ensure the functioning of the institutional mechanism for ensuring information security, including educational programs. This involves the systematic activity of state-legal institutions, which must effectively realize national interests in the information sphere. They should be able not only to respond to the spread of information manipulation and false information, but also to anticipate conflicts and shape the information culture of society. In addition, taking into account global threats and challenges, effective countermeasures against information aggression is possible with the participation of international organizations, institutions and the international community.

Key words: *threats, security, information, sources, war.*

JEL Classification: *G32, L1, M21*

Стаття надійшла до редакції 12.02.2024
The article was received February 12, 2024

[1] *Valerii O. Kotliarov,* National Aviation University