УДК 681.3
DOI https://doi.org/10.32782/2312-1815/2024-19-8

Тарас Кобець
ORCID: 0009-0001-2179-321X

АНАЛІЗ ЗАГРОЗ КОГНІТИВНІЙ БЕЗПЕЦІ УКРАЇНСЬКОГО СУСПІЛЬСТВА: КЛАСИФІКАЦІЙНІ ПІДСТАВИ

У статті визначено загрози когнітивній безпеці держави та суспільства на основі наявних доктринальних та нормативно-правових документів; визначено джерела, передумови та закономірності виникнення і прояву загроз. Проаналізовано проблеми, пов'язані з класифікацією загроз когнітивній безпеці держави. Охарактеризовано внутрішні чинники, які можуть спричинити загострення ситуації в Україні. Узагальнено підходи, що існують у науковій літературі, щодо класифікації загроз. Виділено основні класифікаційні ознаки та розроблено багатокритеріальну класифікацію загроз когнітивній безпеці держави на основі ієрархічного аналізу. Також визначено головні та потенційні загрози на всіх рівнях національної безпеки України.

Проведено детальний аналіз загроз з використанням різноманітних підходів та підстав для класифікації. Аналіз вказує на відсутність єдиного підходу до визначення та розуміння загроз когнітивній безпеці. Інколи їх прирівнюють до загроз національній безпеці або ж інформаційній сфері, а також до кіберзагроз.

У наукових джерелах іноді відбувається ототожнення цих понять, або, навпаки, класифікація загроз за різними критеріями. Автор статті розглядає загрози когнітивній безпеці України як ключові чинники, що призводять до негативних явищ, які загрожують національним інтересам в політичній сфері та організації національного безпекового простору. Ці загрози можуть мати глобальний або локальний характер і бути пов'язані з ризиками в інших сферах, що впливають на національний безпековий простір та міжнародну безпеку.

Задля протидії реальним та потенційним загрозам когнітивній безпеці, стратегічним завданням держави є створення ефективного механізму забезпечення когнітивної безпеки. Він включає систематичну діяльність, низку заходів та функціонування державних інституцій, аналітичних центрів, громадських організацій.

Ключові слова: *безпека, інформаційна безпека, когнітивна безпека, загроза, небезпека, національна безпека.*

Вступ. У сучасному світі політична інформація, що впливає на свідомість людини стала своєрідним товаром, який купують, продають, зловживають і навіть використовують для злочинів. Така ситуація вимагає посиленої уваги до захисту розумових здібностей людини, ідентифікації загроз когнітивній безпеці та їх нейтралізації. Для ефективної ідентифікації цих загроз важливо не лише визначити їхні джерела, але й розуміти причини їх виникнення, що вимагає систематизації через проведення системної класифікації.

Мета статті. Всебічне дослідження та класифікація загроз когнітивній безпеці, виходячи з різноманітних критеріїв та підстав, особливо зауважено особливості психологічних аспектів безпеки захисту національного інформаційного простору з огляду на реальні й потенційні загрози та деструктивні пропагандистсько-маніпулятивні інформаційні впливи.

Матеріал і методи дослідження. Зважаючи на мету дослідження, серед ключових методів, покликаних її реалізувати виділяємо порівняльний, системний та структурно-функціональний методи.

Більшість наукових праць зосереджена на визначенні сутності та загроз інформаційній безпеці, протистояння маніпуляціях та технологіям використання пропаганди, причому

запропоновані авторами підходи до класифікації загроз іноді є предметом дискусій. До того ж, у науковій літературі відсутні системні дослідження загроз безпеці в сучасних умовах, що підкреслює актуальність і практичну значущість цього дослідження.

Питання безпеки та питання захисту національного інформаційного простору досліджували численні науковці, зокрема А. Марущак, В. Петрик, В. Ліпкан, Б. Кормич, В. Почепцов та інші. Проблеми безпеки в мережі були предметом досліджень таких фахівців, як Р. Лук'янчук, В. Бурячок, А. Бабенко, В. Гавловський, Д. Дубов, В. Номоконов, М. Погорецький, В. Шеломенцев та інші. Проте в їхніх роботах інформаційна та кібернетична безпека зазвичай розглядалася як складова національної безпеки, без детального аналізу загроз, джерел їхнього виникнення, технологій ведення когнітивних війн і психологічних операцій.

Результати та обговорення. Щоб систематизувати наукові уявлення в досліджуваній галузі, потрібно спочатку визначити сутність термінів «загроза» та «загроза інформаційній безпеці». Загроза (з англ. threat) – це будь-які обставини або події, які можуть призвести до порушення політики безпеки інформації чи завдати шкоди автоматизованій системі. Спробу реалізувати загрозу називають атакою [2]. Загроза (в загальному розумінні) – це потенційно можлива подія, дія (вплив), процес або явище, які можуть завдати шкоди чиїмось інтересам. Розглянемо погляди науковців на трактування сутності «загрози» [7].

Н. Різник зазначає, що загроза виникає тоді, коли негативні чинники безпосередньо впливають на безпеку об'єкта дослідження, порушуючи його стан рівноваги [6, с. 118].

Аналіз динаміки загроз національним інтересам України, проведений Петренко Л. А. [3], дозволив виявити такі хронологічні закономірності їх виникнення і прояву:

– Загрози мають циклічний характер і проходять різні етапи розвитку, від початкових до завершальних, із можливістю зворотного руху.

– Властива стійкість загроз полягає в їх здатності відхилятися від оптимального напряму під впливом протидій, але з часом повертатися до початкового стану після ослаблення цих сил.

– Загрози діють на об'єкти за хвилеподібною ритмікою: активізуються в моменти внутрішньої нестабільності об'єкта і слабшають, коли об'єкт досягає стабільності та здатності до опору.

– Впливи кількох загроз можуть співпадати, що призводить до виникнення глобальної мультиплікативної загрози, здатної зруйнувати всю систему безпеки держави.

– Загрози національній безпеці України в інформаційній сфері це – сукупність умов та чинників, які становлять небезпеку життєво важливим інтересам держави, суспільства і особи через можливість негативного інформаційного впливу на свідомість та поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру [4].

Незважаючи на виявлені закономірності, класифікація загроз когнітивній безпеці залишається складною через їхню взаємозалежність і вплив спільних деструктивних факторів, що стають джерелами цих загроз.

На думку представників Cognitive-Security Research-Labs (Army Cyber InstituteAt West Point) когнітивна безпека для збереження раціонального прийняття рішень в умовах протидії передбачає загальне прийняття тієї ж самої спільної реальності та правил гри для прийняття рішень, протистояння/пом'якшення емоційних маніпуляцій і захист окремих осіб та суспільств для забезпечення колективних дій у вирішенні проблем. Ризики для когнітивної безпеки включають наступне:

– Маніпуляція прийняттям рішень людиною.

– Злом «людини» у команді людина-машина.

– Маніпуляція поведінкою людини щодо групи.

– Як надати інформацію людині (симбіотичний інтерфейс людина-комп'ютер).

– Розширення за межі HMI до HME (людина-машина-середовище або людина-машина-екосистема).

– Використання збройних наративів.

– Політизовані та монетизовані інформаційні середовища [9].

В Україні відповідно до Доктрини інформаційної безпеки, Міністерство інформаційної політики відповідає за моніторинг загроз національним інтересам та безпеці в інформаційному просторі. Однак «проблема контентно-комунікаційної та комунікаційно-контентної взаємодії (на всіх рівнях) між владою та суспільством залишається невирішеною» [1, с. 165].

Серед основних глобальних викликів та загроз, виділених Стратегією інформаційної безпеки, можна назвати наступні:

– інформаційна політика рф є загрозою не лише для України, а й для інших демократичних країн;

– соціальні мережі виступають як суб'єкти впливу в інформаційному просторі;

– недостатній рівень медіаграмотності на тлі швидкого розвитку цифрових технологій [5].

Використовуючи інформаційний підхід загрози когнітивній безпеці можна класифікувати за:

– *характером реалізації*: реальні (активізація шляхів дестабілізації є неминучою і не обмежена часом і простором); потенційні (шляхи дестабілізації можливі за певних умов середовища функціонування органів публічної влади); здійснені (загрози втілені у життя); уявні (умовні чи схожі з існуючими, але такими не є).

– *ступенем гіпотетичної шкоди:* загрозливі (явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію національних інтересів у інформаційній сфері і створюють небезпеку для системи управління національною безпекою, життєзабезпечення її системостворюючих елементів); небезпечні (безпосередня дестабілізація функціонування системи управління національною безпекою).

– *ймовірністю реалізації*: вірогідні (за виконання певного комплексу умов обов'язково настануть, наприклад, оголошення атаки інформаційних ресурсів, що передує власне атаці); неможливі (за виконання певного комплексу умов ніколи не настануть, переважно мають більш декларативний характер, не підкріплений реальною і навіть потенційною можливістю здійснити проголошені наміри, вони здебільшого мають залякувальний характер); випадкові (за виконання певного комплексу умов протікають по-різному, їх аналізують за допомогою методів дослідження операцій, зокрема теорії ймовірностей і теорії ігор, які вивчають закономірності у випадкових явищах).

– *рівнем детермінізму*: випадкові (загрози, які можуть трапитися або не трапитися – загрози хакерів дестабілізувати інформаційній системи органів влади), закономірні (загрози стійкого, повторюваного характеру, зумовлені об'єктивними умовами існування та розвитку системи інформаційної безпеки) [8].

Джерела загроз можуть бути як суб'єктивними (особистість), так і об'єктивними проявами. Усі джерела загроз безпеці можна класифікувати на три основні категорії [7]:

Антропогенні джерела загроз (викликані діями людини), які виникають через незалежні дії суб'єктів, які можуть бути кваліфіковані як навмисні або ненавмисні. У такому випадку можна говорити про спричинення шкоди. Ця група є найбільшою і має ключове значення для організації захисту, оскільки дії суб'єктів можна оцінити, прогнозувати і вжити відповідних заходів. Методи протидії керовані і залежать від волі організаторів захисту інформації. Антропогенним джерелом загроз може бути суб'єкт, який має доступ (санкціонований або несанкціонований) до систем та засобів захисту. Такі суб'єкти можуть бути як зовнішніми, так і внутрішніми.

Техногенні джерела загроз (викликані технічними засобами), які визначаються техногенною діяльністю людини і розвитком цивілізації

Стихійні джерела загроз об'єднують обставини, які становлять непереборну силу, тобто такі обставини, які носять об'єктивний і абсолютний характер, поширюється на всіх. До непереборної сили в законодавстві й договірній практиці відносять стихійні лиха або інші обставини,

які неможливо передбачити або запобігти, або можливо передбачити, але неможливо запобігти за сучасного рівня людського знання і можливостей.

Згідно американської традиції, яка є більш кіберорієнтованою, важливо розглянути загрози, які пов'язані з використанням штучного інтелекту (ШІ). Хоча штучний інтелект надає безліч переваг, він також створює серйозні виклики в сфері когнітивної безпеки. Основні загрози, пов'язані з використанням технологій ШІ у цій сфері, класифікують:

– Deepfakes. Штучно створені зображення, відео чи аудіо, які виглядають переконливо і можуть ввести в оману, що призводить до дезінформації, маніпуляцій чи шантажу.

– Дезінформація. Алгоритми ШІ можуть швидко поширювати фальшиву інформацію, що підриває довіру до інституцій, руйнує політичні процеси та може викликати соціальні заворушення.

– Упередження. Системи ШІ можуть відтворювати упередження, наявні в даних, що призводить до дискримінації та поглиблення соціальної нерівності.

– Порушення конфіденційності. Технології, такі як розпізнавання обличчя та аналіз даних, можуть використовуватися для незаконного спостереження та відстеження людей.

– Маніпуляція поведінкою. Алгоритми ШІ можуть персоналізувати контент таким чином, щоб впливати на переконання та дії людей, що може спричинити радикалізацію соціально-політичного процесу.

– Кібератаки. Штучний інтелект дозволяє створювати складніші кібератаки, які важко виявити, зокрема фішингові атаки.

– Змагальні атаки. Системи ШІ можуть бути атаковані через навмисне викривлення вхідних даних, що може підірвати їх надійність.

– Залежність від ШІ. Надмірна довіра до систем ШІ може призвести до втрати критичного мислення та нездатності приймати рішення в разі виходу систем з ладу.

– Зменшення людської автономії. Через зростання ролі ШІ у виконанні когнітивних завдань може постраждати здатність людей приймати самостійні рішення.

– Новітні чат-боти, такі як ChatGPT від OpenAI, продемонстрували виняткові здібності у створенні контенту, схожого на людський, що може мати серйозні наслідки для когнітивної безпеки в інтернеті. Вирішення цих проблем потребує технічних рішень, політичного регулювання та міжнародної співпраці для забезпечення відповідального та етичного використання штучного інтелекту [10].

Техніки та технології когнітивної безпеки мають на меті захистити людей і суспільство від шкідливого впливу, роблячи дії зловмисників малоефективними. Когнітивна безпека досягається через три ключові елементи.

По-перше, це підвищення стійкості до маніпуляцій, що включає розвиток критичного мислення та медіаграмотності через освітні програми, а також створення інструментів для виявлення та захисту в реальному часі. Такі технології мають відповідати швидкості та масштабам Інтернету, як, наприклад, автоматичне розпізнавання діпфейків та інших змінених медіафайлів.

По-друге, забезпечення широкої ситуаційної обізнаності у сфері когнітивної безпеки. Це включає оперативне виявлення і аналіз кампаній шкідливого впливу та використання віртуальних помічників, які допомагають визначати джерела й цілі дезінформації.

По-третє, створення ефективних інструментів когнітивної взаємодії для боротьби з шкідливим впливом, зокрема з діяльністю програмних агентів і ботів в Інтернеті.

На відміну від кібербезпеки, яка зосереджена на захисті технічних пристроїв і мереж, когнітивна безпека охоплює захист людини, що потребує соціально-технічного підходу. Цей підхід об'єднує соціальні науки, штучний інтелект, аналіз даних та інші сфери для створення інструментів і рішень, які можуть розроблятись спільно урядом, промисловістю та науковими установами.

Висновки. Цей перелік можна продовжувати, але очевидним є такий висновок: поняття загрози здебільшого трактуються абстрактно або спрощено, іноді звужено, без належного зв'язку з поняттям «когнітивна безпека» і майже не співвідноситься з ширшим поняттям «загроза».

В умовах російсько-українського конфлікту захист національного інформаційного простору від негативних інформаційно-психологічних впливів, операцій та інформаційних війн стає надзвичайно важливим. Забезпечення інформаційної безпеки та збереження інформаційного суверенітету є ключовими факторами для підтримки національної ідентичності України та її існування як суверенної та незалежної держави.

Перспективами подальших наукових досліджень є: аналіз зарубіжного досвіду протидії негативним пропагандистсько-маніпулятивним інформаційним впливам, а також глибше дослідження технологій здійснення інформаційних операцій та війн.

Література:

1. Король В., Любовець Г. Контент негативу. Як захистити себе та країну в умовах тотального інформаційного протистояння : монографія. Київ : Видавничий дім «Києво-Могилянська академія», 2021. 266 с.

2. Основні поняття. НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Київ : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. URL: https://tzi.ua/assets/files/1.1_003_99.pdf

3. Петренко Л. А. Логіка еволюції узагальнюючих макроекономічних показників. *Формування ринкової економіки* : зб. наук. праць. 2009. № 22. URL: http://www.nbuv.gov.ua/portal/Soc_Gum/fre/2009_22.pdf

4. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. URL: http://www.justinian.com.ua/article.php?id=3222

5. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28 грудня 2021 року № 685/2021 URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

6. Різник Н.С. Теоретичні засади формування системи діагностики економічної безпеки банку. *Вісник Харківського національного технічного. університету сільського господарства : Економічні науки.* Харків : ХНТУСГ, 2007. Вип. 66. С. 118–123.

7. Харченко С.О. Наукові підходи до класифікації загроз інформаційній безпеці. *Держава та регіони. Серія : Державне управління*. 2019. № 2 (66). URL: http://pa.stateandregions.zp.ua/archive/2_2019/35.pdf

8. Шемчук В. В. Загрози інформаційній безпеці: проблеми визначення та подолання. *Експерт: парадигми юридичних наук і державного управління*, 2020, 1 (7). С.285–296.

9. Army cyber institute at West Point. URL: https://cyber.army.mil/Research/Research-Labs/Cognitive-Security/

10. Huang R.Y., Zheng Z.Q., Shang Y. On challenges of AI to cognitive security and safety. *Security and Safety.* 2023. № 2. URL: https://sands.edpsciences.org/articles/sands/full_html/2023/01/sands20230010/sands20230010.html

References:

1. Korol, V., & Liubovets, H. (2021). Kontent nehatyvu. Yak zakhystyty sebe ta krainu v umovakh totalnoho informatsiinoho protystoiannia [Content of Negativity: How to Protect Yourself and the Country in the Conditions of Total Information Confrontation]: monohrafiia. Kyiv : Vydavnychyi dim «Kyievo-Mohylianska akademiia». 266 s. [in Ukrainian]

2. Osnovni poniattia. ND TZI 1.1-003-99 (1999): Terminolohiia v haluzi zakhystu informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu [Basic Concepts. NDTZI 1.1-003-99: Terminology in the Field of Information Protection in Computer Systems from Unauthorized Access]. Kyiv : Departament spetsialnykh telekomunikatsiinykh system ta zakhystu informatsii Sluzhby bezpeky Ukrainy. URL: https://tzi.ua/assets/files/1.1_003_99.pdf [in Ukrainian]

3. Petrenko, L. A. (2009). Lohika evoliutsii uzahalniuiuchykh makroekonomichnykh pokaznykiv [The Logic of the Evolution of Aggregate Macroeconomic Indicators]. *Formuvannia rynkovoi ekonomiky* : zb. nauk. prats. №22. Retrieved from http://www.nbuv.gov.ua/portal/Soc_Gum/fre/2009_22.pdf [in Ukrainian]

4. Petryk, V. Sutnist informatsiinoi bezpeky derzhavy, suspilstva ta osoby [The Essence of Information Security of the State, Society, and the Individual]. Retrieved from http://www.justinian.com.ua/article.php?id=3222 [in Ukrainian]

5. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiiu informatsiinoi bezpeky» [On the Decision of the National Security and Defense Council of Ukraine dated October 15, 2021, "On the Information Security Strategy"] : Ukaz Prezydenta Ukrainy vid 28 hrudnia 2021 roku № 685/2021 Retrieved from https://zakon.rada.gov.ua/laws/show/685/2021#Text [in Ukrainian]

6. Riznyk, N.S. (2007). Teoretychni zasady formuvannia systemy diahnostyky ekonomichnoi bezpeky banku [Theoretical Foundations of Forming a System for Diagnosing the Economic Security of a Bank]. *Visnyk Kharkivskoho natsionalnoho tekhnichnoho. universytetu silskoho hospodarstva : Ekonomichni nauky*. Kharkiv : KhNTUSH. Vyp. 66. S. 118–123. [in Ukrainian]

7. Kharchenko, S. O. (2019). Naukovi pidkhody do klasyfikatsii zahroz informatsiinii bezpetsi [Scientific Approaches to the Classification of Information Security Threats]. *Derzhava ta rehiony. Seriia : Derzhavne upravlinnia.* № 2 (66). Retrieved from http://pa.stateandregions.zp.ua/archive/2_2019/35.pdf [in Ukrainian]

8. Shemchuk, V. V. (2020). Zahrozy informatsiinii bezpetsi: problemy vyznachennia ta podolannia [Information security threats: problems of determination and troubleshooting]. *Ekspert: paradyhmy yurydychnykh nauk i derzhavnoho upravlinnia.* 1 (7). S.285–296. [in Ukrainian]

9. Army cyber institute at West Point. Retrieved from https://cyber.army.mil/Research/Research-Labs/Cognitive-Security/ [in English]

10. Huang, R. Y., Zheng, Z. Q., & Shang, Y. (2023). On challenges of AI to cognitive security and safety. *Security and Safety.* № 2. Retrieved from https://sands.edpsciences.org/articles/sands/full_html/2023/01/sands20230010/sands20230010.html [in English]

Taras Kobets. Analysis of threats to the cognitive security of ukrainian society: classification bases

The article identifies threats to the cognitive security of the state and society based on existing doctrinal and legal documents. It defines the sources, prerequisites, and patterns of occurrence and manifestation of these threats. The issues related to the classification of threats to the cognitive security of the state are analyzed. Internal factors that may exacerbate the situation in Ukraine are characterized. Existing approaches in the scientific literature to the classification of threats are summarized. The main classification features are highlighted, and a multi-criteria classification of threats to the cognitive security of the state based on hierarchical analysis is developed. The key and potential threats at all levels of Ukraine's national security are also identified.

A detailed analysis of threats is carried out using various approaches and classification criteria. The analysis indicates the lack of a unified approach to defining and understanding cognitive security threats. Sometimes they are equated with national security threats or threats in the information sphere, as well as with cyber threats. In scientific sources, these concepts are sometimes equated or, conversely, classified according to different criteria.

The author of the article considers threats to Ukraine's cognitive security as key factors leading to negative phenomena that threaten national interests in the political sphere and the organization of the national security space. These threats can be global or local and may be related to risks in other areas affecting the national security space and international security.

To counter real and potential threats to cognitive security, the state's strategic task is to create an effective mechanism for ensuring cognitive security. This includes systematic activities, a range of measures, and the functioning of state institutions, analytical centers, and public organizations.

Key words: *security, information security, cognitive security, threat, danger, national security.*

Відомості про автора:

Тарас Кобець – аспірант кафедри політології,
Прикарпатський національний університет імені Василя Стефаника.