

8. Шендригоренко М. Товари як об'єкт обліку та внутрішнього аудиту на підприємстві. *Економіка і суспільство*. 2017. № 12. С. 722–726.

References.

1. Bondarenko, O.M., Rudenko, L.O. (2022). «Organization and methodology of inventory control and ways to improve it». *Ekonomika ta suspil' stvo*. № 39. DOI: <https://doi.org/10.32782/2524-0072/2022-39-39>.
2. Honcharuk, S., Bojko, O. (2023). «Current state and directions of improving inventory accounting». *Ekonomichni nauky*. № 7 (119). DOI: <https://doi.org/10.32839/2304-5809/2023-7-119-14>.
3. Kravchenko, O., Selez'nova, O. (2022). «The state of development of inventory accounting and control at domestic enterprises and directions of their improvement». *Ekonomika i suspil' stvo*. № 2. pp. 9–16.
4. Makarenko, A., Puhach, K. (2021). «Improving the accounting of goods and finding other ways of their implementation». *Ekonomika i upravlinnia*. № 1. pp. 1–8.
5. Marchenko, V.M., Bashylova, V.P. (2017). «ABC-XYZ analysis as a means of managing the assortment of a machine-building enterprise». *Ekonomika i suspil' stvo*. № 13. pp. 597–601.
6. Odnosheva, O., Pyl'hum, O., Bilovol, Ye. (2024). «Analytical diagnostics of the efficiency of inventory use by an enterprise, as an element of optimizing the accounting and control system». *Problemy suchasnykh transformatsiy. Seriya: ekonomika ta upravlinnia*. № 15. pp. 1–6.
7. Odnosheva, O.O., Pyl'hum, O.V., Bilovol, Ye.V. (2024). « Analytical diagnostics of the efficiency of inventory use by an enterprise as an element of optimizing the accounting and control system». *Problems of Modern Transformations. Series: Economics and Management*. № 15. DOI: <https://doi.org/10.54929/2786-5738-2024-15-09-03>.
8. Shendryhorenko, M. (2017). «Goods as an object of accounting and internal audit at the enterprise». *Ekonomika i suspil' stvo*. № 12. pp. 722–726.

Nord G., Rudenko N., Kolevatova A. *The effectiveness of goods control in the enterprise management system based on ABC analysis.*

In modern enterprise management, goods are traditionally considered objects of accounting, storage, and sale. At the same time, it is at the stage of control of commodity resources that a significant part of the management risks associated with losses, inefficient use of working capital and distortion of accounting information are formed. Under such conditions, control of goods ceases to be an auxiliary procedure and becomes an independent tool for influencing the enterprise's effectiveness. Modern management systems are characterized by an increase in the volume of accounting data, the complexity of commodity flows, and increased requirements for internal control. This necessitates not only the implementation of control measures but also their systematic evaluation from the standpoint of the expediency, direction, and effectiveness of their use of control resources. ABC analysis is a traditional analytical tool for processing accounting data and can be adapted to assess the effectiveness of goods control. Its application allows you to differentiate control efforts according to the economic significance of commodity items, thereby increasing the validity of management decisions. The purpose of the article is to substantiate methodological approaches to assessing the effectiveness of goods control within the enterprise management system using ABC analysis. In the process of the study, methods of comparison, analysis, theoretical and logical generalization were applied. The methodological basis was the dialectical research method. As a result of the study, the tools for assessing the effectiveness of goods control in the enterprise management system were systematized, and the feasibility of using ABC analysis as a basic analytical method was substantiated. It was established that traditional approaches to goods control are largely formal in nature and do not account for the economic significance of individual product positions, thereby reducing the managerial value of control results. It is proposed to adapt ABC analysis to assess the effectiveness of goods control by grouping control measures into A, B, and C, depending on their impact on the enterprise's financial results. It has been proven that the concentration of control resources on group A goods increases internal control efficiency, reduces losses, and rationalizes control costs. Practical aspects of ABC analysis confirm its integration with other management tools, in particular KPIs and internal audit, which help increase the transparency and validity of management decisions.

Keywords: enterprise management system, accounting, goods, control, ABC analysis, integration.

Стаття надійшла до редакції / Received 18.12.2025 Прийнята до друку / Accepted 03.01.2026 Оpubліковано/ Published 19.01.2026

Бібліографічний опис статті:

Норд Г.Л., Руденко Н.О., Колеватова А.В. Ефективність контролю товарів у системі управління підприємства на основі ABC-аналізу. *Актуальні проблеми інноваційної економіки та права*. 2026. № 1. С. 140–143.

Nord G., Rudenko N., Kolevatova A. *The effectiveness of goods control in the enterprise management system based on ABC analysis. Actual problems of innovative economy and law*. 2026. No. 1, pp. 140–143.

УДК: 351.86:004.056.5:316.77]:327.5; JEL classification: H11, H56, D83, Z13
DOI: <https://doi.org/10.36887/2524-0455-2026-1-31>

ЗУБЧИК Олег Анатолійович, доктор наук з державного управління, доцент, професор кафедри державного управління, Київський національний університет імені Тараса Шевченка, <https://orcid.org/0000-0001-6480-409X>
ГРИЦАЙ Роман Олексійович, аспірант кафедри державного управління, Київський національний університет імені Тараса Шевченка, <https://orcid.org/0009-0007-4914-3749>

ДЕРЖАВНА СТРАТЕГІЯ ЗАХИСТУ КОГНІТИВНОГО ПРОСТОРУ: АРХІТЕКТОНІКА ТА УПРАВЛІНСЬКІ ІНСТРУМЕНТИ ФОРМУВАННЯ СУСПІЛЬНОЇ РЕЗИЛЬЄНТНОСТІ

Зубчик О.А., Грицай Р.О. *Державна стратегія захисту когнітивного простору: архітектоніка та управлінські інструменти формування суспільної резильєнтності.*

У статті здійснено комплексний аналіз теоретико-методологічних засад захисту когнітивного простору в умовах гібридних загроз та інтенсивних семантичних впливів. Розкрито архітектоніку багаторівневої системи когнітивної безпеки, що включає гуманітарний, комунікаційний та аналітико-технологічний рівні, а також визначено їхню роль у формуванні суспільної резильєнтності. Проведено критичний аналіз інституційної взаємодії суб'єктів публічної влади у сфері стратегічних комунікацій та протидії дезінформації, виокремлено ключові функціональні лакуни, що знижують ефективність управлінського реагування на семантичні загрози. Обґрунтовано, що сучасна модель державної політики має трансформуватися від контролю інформаційних потоків до модератії середовища стійкості, забезпечуючи узгодженість смислових наративів та розвиток довіри. Запропоновано концептуальну модель державної стратегії захисту когнітивного простору, засновану на інтеграції гуманітарних, комунікаційних і технологічних інструментів у єдиний когнітивний контур. Доведено, що перехід від фрагментарних реакцій до протокольної детермінації управлінських дій дозволяє мінімізувати стратегічну невизначеність та підвищити адаптивність державних інституцій. Підкреслено значення розвитку стратегічних комунікацій як інструменту забезпечення інформаційного суверенітету та формування суспільної резильєнтності. Окреслено напрями вдосконалення державної політики, зокрема епістемічну інтеграцію аналітичних підрозділів, розбудову національної інфраструктури моніторингу когнітивних ризиків та забезпечення дромологічної стійкості інституцій у динамічному семантичному середовищі.

Ключові слова: когнітивний простір, семантичні загрози, стратегічні комунікації, інформаційний суверенітет, резильєнтність, архітектоніка державного управління, когнітивна безпека, аналітико-технологічний контур.



This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

© Зубчик Олег Анатолійович, Грицай Роман Олексійович, 2026

Постановка проблеми у загальному вигляді. Сучасні гібридні агресії демонструють, що ключовим об'єктом впливу стає не лише інформаційна інфраструктура, а й когнітивний простір – система уявлень, цінностей, емоційних реакцій та здатності громадян до критичного мислення [2; 8–10; 13].

Саме тут формуються наративи, що визначають рівень довіри до держави, стійкість інституцій і готовність суспільства протидіяти дезінформаційним атакам, що робить захист когнітивного простору стратегічним пріоритетом публічного управління [1; 2; 9; 10].

Перед державою постає подвійний виклик, адже необхідно забезпечити ментальну безпеку громадян і водночас зберегти стандарти свободи слова та демократичного плюралізму [5; 6; 12]. Традиційні інструменти інформаційної політики є недостатніми, оскільки семантичні загрози діють на рівні смислів, емоцій та поведінкових моделей, що потребує переходу до комплексної гуманітарно-технологічної архітектоники захисту когнітивного простору [1; 2; 8-10; 12].

Аналіз останніх досліджень і публікацій.

У міжнародному дискурсі захист когнітивного простору трактується через концепції Cognitive Security та Societal Resilience, що формуються у стратегічних документах НАТО та ЄС [1; 2; 4; 7-10; 12]. Обидва підходи зміщують акцент від реагування на окремі атаки до формування стійких суспільних систем, здатних витримувати тривалі семантичні впливи [2; 4; 9; 12]. НАТО розглядає когнітивну безпеку як ключовий елемент оборони [1; 2; 7-10], тоді як ЄС акцентує на резильєнтності як здатності суспільства адаптуватися й зберігати демократичну стійкість [4; 12]. У цьому контексті роль держави трансформується від контролю інформаційних потоків до модерзації середовища стійкості, що передбачає розвиток критичного мислення, медіаграмотності та довіри [5; 6; 12]. Такий підхід спрямований на створення екосистеми, у якій громадяни здатні самостійно розпізнавати маніпуляції [1; 2; 9; 10].

В Україні проблема захисту когнітивного простору досліджена фрагментарно: увага зосереджена переважно на інформаційній безпеці та дезінформації [13; 15; 16; 23; 24], тоді як архітекtonіка когнітивного захисту та інструменти резильєнтності залишаються недостатньо систематизованими [14; 23]. Це ускладнює формування політики, здатної інтегрувати гуманітарні, комунікаційні та технологічні механізми впливу [17-22].

Формулювання цілей статті (постановка завдання). Метою статті є теоретичне обґрунтування архітектоники державної стратегії захисту когнітивного простору та систематизація управлінських інструментів формування суспільної резильєнтності в умовах гібридних загроз. Для її досягнення визначено концептуальні засади когнітивної безпеки та резильєнтності у підходах НАТО й ЄС [1; 2; 4; 7-12], розкрито структуру архітектоники когнітивного захисту, класифіковано гуманітарні, комунікаційні та технологічні інструменти стійкості, обґрунтовано роль держави як модератора середовища стійкості та сформовано концептуальну модель державної стратегії, орієнтованої на довгострокову адаптивність і психологічну витривалість громадян.

Методологічну основу становить поєднання системного, когнітивного, комунікаційного та мережецентричного підходів [1; 2; 8-10; 12]. Застосовано структурно-функціональний аналіз для визначення архітектоники когнітивного захисту [1; 3; 7-10], порівняльний аналіз – для узагальнення підходів НАТО та ЄС [1; 2; 4; 7-12], контент-аналіз стратегічних документів і наукових джерел [4-6; 11-16; 17-24]. Інституційний аналіз використано для оцінки ролі держави як модератора стійкості [5; 6; 12; 17-22], а концептуальне моделювання – для класифікації управлінських інструментів резильєнтності [1; 2; 8-10; 12; 14].

Виклад основного матеріалу дослідження. У сучасних умовах гібридної агресії когнітивний простір стає ключовим об'єктом державного захисту, оскільки саме в ньому формуються інтерпретації подій, поведінкові моделі та рівень довіри до інституцій [2; 8-10; 11; 12]. Концепція Cognitive Security, що активно розвивається у стратегічних документах НАТО, визначає когнітивну сферу як критичний елемент національної безпеки, вразливий до маніпулятивних впливів, інформаційних симулякрів та технологій поведінкового таргетингу [1; 2; 7-10]. У цьому контексті захист когнітивного простору розглядається не як обмеження інформації, а як забезпечення

здатності громадян зберігати критичність мислення та стійкість до семантичних атак [1; 2; 8-10; 12].

Паралельно Європейський Союз формує підхід Societal Resilience, який акцентує увагу на здатності суспільства адаптуватися, відновлюватися та функціонувати в умовах тривалого інформаційного тиску [4; 12]. Резильєнтність трактується як інтегральна характеристика соціальної системи, що поєднує психологічну стійкість громадян, довіру до держави, ефективність комунікацій та наявність інституційних механізмів реагування [4; 5; 6; 12].

Узагальнення міжнародних підходів дозволяє визначити кілька ключових положень, важливих для українського контексту. По-перше, когнітивна безпека є міждисциплінарною категорією, що поєднує гуманітарні, комунікаційні та технологічні аспекти [1; 2; 8-10; 12; 14]. По-друге, суспільна резильєнтність формується не лише державою, а й громадянським суспільством, медіа та освітніми інституціями [4; 12; 13; 15; 16]. По-третє, ефективна стратегія захисту когнітивного простору потребує системної архітектоники, а не окремих реактивних заходів [1; 2; 7-10; 14]. По-четверте, роль держави трансформується від контролю інформаційних потоків до модерзації середовища стійкості, що забезпечує баланс між безпекою та демократичними свободами [5; 6; 17-22].

Цей міжнародний досвід підтверджує необхідність переходу від фрагментарних інформаційних заходів до комплексної моделі когнітивного захисту, у якій ключовим результатом є не блокування загроз, а підвищення здатності суспільства самостійно їм протидіяти.

Архітектоніка захисту когнітивного простору розглядається як цілісна система, яка поєднує гуманітарні, комунікаційні та технологічні компоненти, спрямовані на забезпечення стійкості суспільства до семантичних загроз [1; 2; 8-10; 12; 13; 14]. На відміну від традиційних моделей інформаційної безпеки, які фокусуються на інфраструктурі та каналах поширення інформації, когнітивний вимір охоплює глибинні процеси сприйняття, інтерпретації та формування поведінкових реакцій громадян [2; 8-10; 16]. Тому його захист потребує багаторівневої архітектури, що враховує як психологічні, так і технологічні чинники [1; 2; 8-10; 12; 13].

У структурному вимірі архітектоніка когнітивного захисту охоплює три взаємопов'язані рівні. Гуманітарно-ціннісний рівень формує основу когнітивної стійкості, визначаючи систему цінностей, ідентичностей та соціальних норм, що забезпечують здатність суспільства протистояти маніпуляціям (критичне мислення, медіаграмотність, національна ідентичність, психологічна стійкість) [4; 12; 13; 15; 16]. Він виконує роль «внутрішнього імунітету» до семантичних атак [13; 16]. Комунікаційно-наративний рівень визначає механізми формування й поширення смислів державою, медіа та громадянським суспільством (стратегічні комунікації, узгоджені наративи, протидія дезінформації, прозорий зворотний зв'язок) [1; 2; 5; 6; 9; 10; 12; 15]. Він забезпечує узгодженість смислового поля та зменшує ризики когнітивної фрагментації [1; 2; 9; 10]. Технологічно-аналітичний рівень охоплює системи моніторингу, аналізу та прогнозування загроз, інструменти верифікації контенту, алгоритмічні моделі виявлення маніпуляцій і цифрові платформи координації [7-10; 12; 15; 17-22]. Цей рівень забезпечує швидкість реагування та точність аналітичних рішень [7-10; 12].

Формування стійкості суспільства до семантичних загроз потребує використання взаємодоповнювальних інструментів, які охоплюють гуманітарний, комунікаційний та технологічний виміри [1; 2; 8-10; 12-16]. У гуманітарному блоці ключову роль відіграють розвиток критичного мислення, медіаграмотності, психологічної стійкості та ціннісної ідентичності громадян [4; 12; 13; 15; 16]. Комунікаційні інструменти включають стратегічні комунікації держави, узгоджені наративи, прозорі механізми зворотного зв'язку та системи протидії

дезінформації [1; 2; 5; 6; 9; 10; 12; 15]. Технологічний блок охоплює інструменти моніторингу інформаційного середовища, аналізу великих даних (Big Data), алгоритмічної верифікації контенту та цифрові платформи координації між інституціями [7-10; 12; 15; 17-22].

Узгоджене застосування цих трьох груп інструментів забезпечує комплексний вплив на когнітивний простір, поєднуючи зміцнення внутрішньої стійкості громадян, формування єдиного смислового поля та оперативне виявлення загроз у цифровому середовищі [1; 2; 8-10; 12-16]. У сучасних умовах держава вже не може обмежуватися функцією контролера інформаційних потоків, оскільки пряме втручання у комунікаційне середовище суперечить демократичним принципам і часто виявляється неефективним проти децентралізованих семантичних загроз [5; 6; 12; 17-22]. Натомість її роль трансформується у роль модератора середовища стійкості, який створює умови для розвитку критичного мислення, довіри та психологічної витривалості громадян [4; 12; 13; 15; 16]. Модеративна функція держави передбачає три ключові напрями діяльності, а саме:

- інституційне забезпечення стійкості, що включає формування нормативної бази, підтримку освітніх і просвітницьких програм, розвиток медіаграмотності та психологічної підтримки населення [17-22];

- смислову координацію, яка полягає у виробленні узгоджених наративів, прозорих стратегічних комунікацій та забезпеченні відкритого діалогу між владою, медіа та громадянським суспільством [1; 2; 5; 6; 9; 10; 12; 15];

- технологічну модерацию, яка охоплює створення інструментів моніторингу, верифікації та прогнозування загроз без прямого обмеження свободи слова [7-10; 12; 15; 17-22].

У такій моделі держава не нав'язує інформаційні рамки, а забезпечує екосистему, у якій суспільство може самостійно розпізнавати маніпуляції, зберігати когнітивну рівновагу та підтримувати довіру до інституцій [1; 2; 4; 12; 13; 15]. Це відповідає сучасним підходам НАТО та ЄС, де стійкість розглядається як спільна відповідальність держави, громадянського суспільства та приватного сектору [1; 2; 4; 5; 6; 9; 10; 12].

Україні сьогодні потрібна концептуальна модель державної стратегії захисту когнітивного простору, яка ґрунтується на інтеграції гуманітарних, комунікаційних і технологічних механізмів і забезпечує стійкість суспільства до семантичних загроз [1; 2; 8-10; 12-16]. Її архітектоніка передбачає поєднання трьох взаємодоповнювальних блоків - ціннісного, смислового та аналітико-технологічного, які формують єдину екосистему когнітивної безпеки [1; 2; 8-10; 12-16; 17-22] (рис. 1).

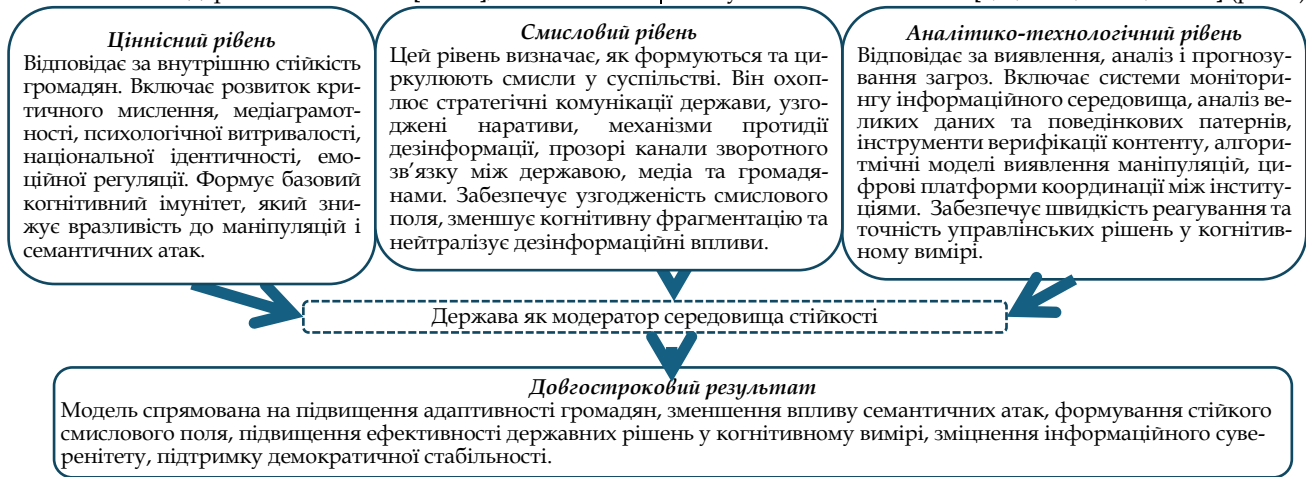


Рис. 1. Модель державної стратегії захисту когнітивного простору. Джерело: розробка авторів

Логіка функціонування моделі така, що модель працює як єдиний когнітивний контур, у якому гуманітарний блок формує стійкість громадян, комунікаційний блок забезпечує смислову узгодженість, технологічний блок виявляє та нейтралізує загрози. Центральною ланкою моделі виступає держава як модератор середовища стійкості, яка не контролює інформаційні потоки, а створює умови для саморегуляції суспільства, розвитку критичного мислення та зміцнення довіри. Ціннісний (гуманітарний) блок - зміцнює внутрішню стійкість громадян через розвиток критичного мислення, медіаграмотності, психологічної витривалості та національної ідентичності, формуючи базовий когнітивний імунітет до маніпуляцій. Смисловий (комунікаційний) блок - забезпечує узгодженість інформаційного середовища завдяки стратегічним комунікаціям, прозорим наративам і ефективному діалогу між державою, медіа та громадянським суспільством, зменшуючи когнітивну фрагментацію та нейтралізуючи дезінформацію. Аналітико-технологічний блок - включає системи моніторингу, аналізу й прогнозування загроз, інструменти верифікації контенту, алгоритмічні моделі виявлення маніпуляцій і цифрові платформи координації, забезпечуючи швидке реагування та точність управлінських рішень.

Запропонована концептуальна модель забезпечує довгострокове підвищення адаптивності громадян, зменшення впливу семантичних атак на суспільні настрої, формування стійкого смислового поля, підвищення ефективності державних рішень у когнітивному вимірі,

зміцнення інформаційного суверенітету та демократичної стабільності.

Висновки та перспективи подальших досліджень. Захист когнітивного простору є ключовим стратегічним пріоритетом публічного управління в умовах гібридних загроз. Узагальнення підходів НАТО та ЄС засвідчило, що ефективна протидія семантичним впливам ґрунтується на поєднанні когнітивної безпеки та суспільної резильєнтності як взаємодоповнювальних компонентів сучасної державної політики.

Зміст і структура архітектоніки захисту когнітивного простору включає гуманітарний, комунікаційний та аналітико-технологічний рівні. Така багаторівнева система дозволяє розглядати когнітивний простір не лише як інформаційне середовище, а як комплексну соціальну систему, чутливу до смислових, емоційних і поведінкових впливів.

Класифікація управлінських інструментів показала, що стійкість суспільства формується через синергію гуманітарних механізмів (критичне мислення, медіаграмотність, психологічна стійкість), комунікаційних практик (стратегічні наративи, прозорі комунікації, механізми протидії дезінформації) та технологічних рішень (моніторинг, аналіз даних, верифікація контенту, цифрова координація).

Роль держави трансформується від контролера інформаційних потоків до модератора середовища стійкості, який забезпечує умови для саморегуляції суспільства, розвитку довіри та формування узгодженого

смыслового поля. Такий підхід відповідає демократичним стандартам і водночас підвищує ефективність регулювання на семантичні загрози.

Запропонована концептуальна модель державної стратегії захисту когнітивного простору демонструє, що довгострокова стійкість можлива лише за умови інтеграції гуманітарних, комунікаційних і технологічних інструментів у єдиний когнітивний контур. Її реалізація сприятиме зміцненню інформаційного суверенітету, підвищенню адаптивності громадян та

формуванню стійкого демократичного суспільства в умовах високої стратегічної невизначеності.

Подальші дослідження доцільно спрямувати на розроблення індикаторів оцінювання когнітивної стійкості та методів вимірювання ефективності державних інструментів захисту когнітивного простору. Перспективним також є вивчення можливостей інтеграції штучного інтелекту й поведінкової аналітики у системи раннього виявлення семантичних загроз.

Література.

1. *Christou G.* Cyber Diplomacy: From Concept to Practice. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2024. 28 p.
2. *Claverie B., du Cluzel F.* Cognitive Warfare. Norfolk: NATO Innovation Hub, 2021. 45 p.
3. *Davydiuk A., Potii O.* National Cybersecurity Governance: Ukraine. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2024. 64 p.
4. European Commission. 2020 Strategic Foresight Report: Charting the course towards a more resilient Europe. Brussels, 2020. 34 p. URL: https://commission.europa.eu/strategy-and-policy/strategic-foresight/2020-strategic-foresight-report_en.
5. G7 Foreign and Development Ministers' Meeting. Defending Democracy from Foreign Threats and Championing Shared Values: Communiqué. London: Foreign, Commonwealth & Development Office, 2021. URL: <https://www.gov.uk/government/publications/g7-foreign-and-development-ministers-meeting-may-2021-communicue/defending-democracy-from-foreign-threats-and-championing-shared-values>.
6. G7 Rapid Response Mechanism. RRM Data Report. Berlin: G7 Germany, 2022. 18 p. URL: <https://www.g7germany.de/resource/blob/998352/2037538/e0ade1417b8078cbc189e149b578126c/2022-05-06-rrm-data.pdf?download=1>.
7. NATO CCDCOE. Cyber Commanders' Handbook 2. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2025. 120 p.
8. NATO CCDCOE. Cyber Threats and NATO Resilience. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2021. 54 p.
9. NATO CCDCOE. Cyberspace Strategic Outlook 2030: Horizon Scanning and Analysis. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2022. 110 p.
10. NATO CCDCOE. Influence Operations in Cyberspace. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2020. 76 p.
11. *Person R., Kulalic I., Mayle J.* Back to the future: the persistent problems of hybrid war. *International Affairs*. 2024. Vol. 100. No. 4. P. 1749-1761.
12. *Wigell M., Harri M., Tapio J.* Best Practices in the whole-of-society approach in countering hybrid threats. Brussels: European Parliament Policy Department for External Relations, 2021.
13. *Дубов Д.В.* Когнітивна безпека в умовах гібридної війни: монографія. Київ: НІСД, 2019. 256 с.
14. *Зубчик О.В., Грцишай Р.О.* Функціональна конвергентність як інституційна відповідь на семантичні загрози публічному управлінню. *Актуальні проблеми інноваційної економіки та права*. 2025. № 5. С. 112-120.
15. Методичні підходи до виявлення та нейтралізації дезінформаційних кампаній. Київ: Центр протидії дезінформації при РНБО України, 2023. 48 с.
16. *Почепцов Г.* Когнітивні війни в соціальних медіа, масовій культурі та масових комунікаціях. Харків: Фоліо, 2019.
17. Про національну безпеку України: Закон України № 2469-VIII від 21.06.2018 р. URL: <https://zakon.rada.gov.ua/laws/show/2469-19>
18. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05.10.2017 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>.
19. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України № 685/2021 від 28.12.2021 р. URL: <https://zakon.rada.gov.ua/laws/show/685/2021>.
20. Про схвалення Концепції розвитку системи стратегічних комунікацій у секторі безпеки і оборони України: Розпорядження Кабінету Міністрів України № 1069-р від 29.09.2021 р. URL: <https://zakon.rada.gov.ua/laws/show/1069-2021-%D1%80>.
21. Про утворення Центру протидії дезінформації: Указ Президента України № 106/2021 від 19.03.2021 р. URL: <https://zakon.rada.gov.ua/laws/show/106/2021>.
22. Про утворення Центру стратегічних комунікацій та інформаційної безпеки: Постанова Кабінету Міністрів України № 1217 від 02.12.2020 р. URL: <https://www.kmu.gov.ua/npras/pro-utvorennya-centru-strategichnih-komunikacij-ta-informatsijnoi-bezpeki-i021220-1217>.
23. *Ситник Г.П., Клименко Н.Г., Гореліков І.О.* Державна політика забезпечення інформаційної безпеки та кібербезпеки як її складової: проблеми та шляхи їх вирішення. *Державне управління: удосконалення та розвиток*. 2024. № 5. DOI: <https://doi.org/10.32702/2307-2156.2024.5.3>.
24. *Таран С.* Інформаційна політика як складова стратегії національної безпеки України. *Наукові перспективи*. 2025. № 3(57). С. 546-554. DOI: [https://doi.org/10.52058/2708-7530-2025-3\(57\)-546-554](https://doi.org/10.52058/2708-7530-2025-3(57)-546-554).

References.

1. *Christou, G.* (2024). *Cyber Diplomacy: From Concept to Practice*. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn, Estonia.
2. *Claverie, B., du Cluzel, F.* (2021). *Cognitive Warfare*. NATO Innovation Hub, Norfolk.
3. *Davydiuk, A., Potii, O.* (2024). *National Cybersecurity Governance: Ukraine*. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn, Estonia.
4. (2020). European Commission. 2020 Strategic Foresight Report: Charting the course towards a more resilient Europe. Brussels, Belgium. Available at: https://commission.europa.eu/strategy-and-policy/strategic-foresight/2020-strategic-foresight-report_en.
5. (2021). G7 Foreign and Development Ministers' Meeting. Defending Democracy from Foreign Threats and Championing Shared Values: Communiqué. Foreign, Commonwealth & Development Office. London, England. Available at: <https://www.gov.uk/government/publications/g7-foreign-and-development-ministers-meeting-may-2021-communicue/defending-democracy-from-foreign-threats-and-championing-shared-values>.
6. (2022). G7 Rapid Response Mechanism. RRM Data Report. Berlin, Germany. Available at: <https://www.g7germany.de/resource/blob/998352/2037538/e0ade1417b8078cbc189e149b578126c/2022-05-06-rrm-data.pdf?download=1>.
7. (2025). NATO CCDCOE. Cyber Commanders' Handbook 2. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn, Estonia.
8. (2021). NATO CCDCOE. Cyber Threats and NATO Resilience. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn, Estonia.
9. (2022). NATO CCDCOE. Cyberspace Strategic Outlook 2030: Horizon Scanning and Analysis. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn, Estonia.
10. (2020). NATO CCDCOE. Influence Operations in Cyberspace. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn, Estonia.
11. *Person, R., Kulalic, I., Mayle, J.* (2024). «Back to the future: the persistent problems of hybrid war». *International Affairs*. Vol. 100. No. 4. pp. 1749-1761.
12. *Wigell, M., Harri, M., Tapio, J.* (2021). *Best Practices in the whole-of-society approach in countering hybrid threats*. European Parliament Policy Department for External Relations, Brussels.
13. *Dubov, D.V.* (2019). *Kohmityona bezpeka v umovakh hibrydnoi viiny*. [Cognitive security in the context of hybrid warfare]. NISD, Kyiv, Ukraine.
14. *Zubchuk, O.V., Hrytsaj, R.O.* (2025). «Functional convergence as an institutional response to semantic threats to public administration». *Aktual'ni problemy innovatsijnoi ekonomiky ta prava*. № 5. pp. 112-120.
15. (2023). *Metodychni pidkhody do vyjavlennia ta nejtralizatsii dezinformatsijnykh kampanij*. [Methodological approaches to identifying and

neutralizing disinformation campaigns]. Tsentr protydyi dezinformatsii pry RNBO Ukrainy. Kyiv. Ukraine.

16. *Pochepstov, H.* (2019). *Kohnytoni vijny v sotsial'nykh media, masoviy kul'turi ta masovykh komunikatsiakh*. [Cognitive wars in social media, mass culture and mass communications]. Folio. Kharkiv. Ukraine.

17. Pro natsional'nu bezpeku Ukrainy: Zakon Ukrainy. (2018). [On the National Security of Ukraine: Law of Ukraine]. № 2469-VIII dated June 21, 2018. Available at: <https://zakon.rada.gov.ua/laws/show/2469-19>

18. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy. (2017). [On the Basic Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine]. № 2163-VIII dated October 5, 2017. Available at: <https://zakon.rada.gov.ua/laws/show/2163-19>.

19. Pro rishennia Rady natsional'noi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiu informatsijnoi bezpeky»: Ukaz Prezydenta Ukrainy. (2021). [On the Decision of the National Security and Defense Council of Ukraine of October 15, 2021 "On the Information Security Strategy": Decree of the President of Ukraine]. № 685/2021 dated December 28, 2021. Available at: <https://zakon.rada.gov.ua/laws/show/685/2021>.

20. Pro skhvalennia Kontseptsii rozvytku systemy stratehichnykh komunikatsij u sektori bezpeky i oborony Ukrainy: Rozporiadzhennia Kabinetu Ministriv Ukrainy. (2021). [On approval of the Concept for the development of the strategic communications system in the security and defense sector of Ukraine: Resolution of the Cabinet of Ministers of Ukraine]. № 1069-r dated September 29, 2021. Available at: <https://zakon.rada.gov.ua/laws/show/1069-2021-%D1%80>.

21. Pro utvorennia Tsentru protydyi dezinformatsii: Ukaz Prezydenta Ukrainy. (2021). [On the establishment of the Center for Counteracting Disinformation: Decree of the President of Ukraine]. № 106/2021 dated March 19, 2021. Available at: <https://zakon.rada.gov.ua/laws/show/106/2021>.

22. Pro utvorennia Tsentru stratehichnykh komunikatsij ta informatsijnoi bezpeky: Postanova Kabinetu Ministriv Ukrainy. (2020). [On the establishment of the Center for Strategic Communications and Information Security: Resolution of the Cabinet of Ministers of Ukraine]. № 1217 dated December 2, 2020. Available at: <https://www.kmu.gov.ua/npas/pro-utvorennia-centru-strategichnih-komunikacij-ta-informacijnoi-bezpeki-i021220-1217>.

23. *Sytnyk, H.P., Klymenko, N.H., Horielikov, I.O.* (2024). «State policy of ensuring information security and cybersecurity as its component: problems and ways to solve them». *Derzhavne upravlinnia: udoskonalennia ta rozvytok*. № 5. DOI: <https://doi.org/10.32702/2307-2156.2024.5.3>.

24. *Taran, Ye.* (2025). «Information policy as a component of the national security strategy of Ukraine». *Naukovi perspektyvy*. № 3(57). pp. 546–554. DOI: [https://doi.org/10.52058/2708-7530-2025-3\(57\)-546-554](https://doi.org/10.52058/2708-7530-2025-3(57)-546-554).

Abstract.

Zubchuk O., Hrytsai R. State strategy for protecting the cognitive space: architecture and governance instruments for building societal resilience.

The article presents an in-depth examination of the theoretical, methodological, and institutional foundations of protecting the cognitive space under conditions of hybrid threats, intensified semantic influence, and rapidly evolving information environments. Attention is devoted to conceptualizing the architecture of a multi-level cognitive security system that integrates humanitarian, communicative, and analytical-technological dimensions. These components are analyzed as interdependent elements that collectively shape societal resilience, influence public trust, and determine the capacity of democratic institutions to withstand manipulative and destabilizing cognitive impacts. The study provides a comprehensive assessment of the interaction among public authorities responsible for strategic communications, counter-disinformation, and information security. It identifies structural and functional gaps that reduce the coherence of governmental responses to semantic threats and hinder the development of an integrated cognitive security framework. The analysis demonstrates that contemporary public policy must evolve from a paradigm of controlling information flows toward a model of moderating a resilience-oriented communicative environment. Such a shift requires narrative coherence, transparent communication practices, and the cultivation of public trust as a strategic resource of national security. A conceptual model of the state strategy for protecting the cognitive space is proposed, grounded in the integration of humanitarian, communicative, and technological instruments into a unified cognitive contour. The model emphasizes the transition from fragmented, reactive measures to protocol-based, anticipatory governance, thereby reducing strategic uncertainty and enhancing institutional adaptability. The article highlights the critical role of strategic communications in safeguarding information sovereignty, strengthening democratic stability, and fostering long-term societal resilience. Furthermore, the study outlines priority directions for improving state policy, including the epistemic integration of analytical units, the development of a national infrastructure for monitoring cognitive risks, and the enhancement of diromological (speed-related) stability of public institutions operating in a dynamic semantic environment. These measures are presented as essential prerequisites for constructing a coherent and future-oriented system of cognitive security.

Keywords: cognitive space; semantic threats; strategic communications; information sovereignty; resilience; public administration architecture; cognitive security; analytical-technological contour.

Стаття надійшла до редакції / Received 23.12.2025 Прийнята до друку / Accepted 08.01.2026 Оpubліковано / Published 19.01.2026

Бібліографічний опис статті:

Zubchuk O.A., Griytsai P.O. Державна стратегія захисту когнітивного простору: архітектура та управлінські інструменти формування суспільної резильєнтності. Актуальні проблеми інноваційної економіки та права. 2026. № 1. С. 143-147.

Zubchuk O., Hrytsai R. State strategy for protecting the cognitive space: architecture and governance instruments for building societal resilience. Actual problems of innovative economy and law. 2026. No. 1, pp. 143-147.

УДК: 658.7:005.334; JEL classification: L23, M11, D23

DOI: <https://doi.org/10.36887/2524-0455-2026-1-32>

КЛЮЧНИК Альона Володимирівна, д.е.н., проф., зав. кафедри публічного управління та адміністрування і міжнародної економіки, Миколаївський національний аграрний університет, <https://orcid.org/0000-0001-6012-6666>

УПРАВЛІНСЬКИЙ ПІДХІД ДО ОПТИМІЗАЦІЇ БІЗНЕС-ПРОЦЕСІВ АУТСОРСИНГУ

Ключник А.В. Управлінський підхід до оптимізації бізнес-процесів аутсорсингу.

У статті обґрунтовано управлінський підхід до оптимізації бізнес-процесів аутсорсингу в умовах трансформації сучасного бізнес-середовища, що характеризується підвищенням вимог до ефективності управління та раціонального використання ресурсів підприємства. Визначено, що основою прийняття рішень щодо передачі функцій на аутсорсинг виступає стратегічний аналіз, який забезпечує формування довгострокових цілей, їх адаптацію до динаміки зовнішнього середовища та узгодження з ресурсними можливостями підприємства. Доведено, що оптимізація бізнес-процесів передбачає структуровану ідентифікацію функцій для делегування без втрати стратегічного контролю, а також вибір відповідної моделі аутсорсингу відповідно до стратегічних пріоритетів розвитку. Обґрунтовано доцільність поєднання аутсорсингових та інсорсингових механізмів у межах єдиної системи управління бізнес-процесами, що забезпечує ефективну інтеграцію внутрішніх і зовнішніх ресурсів. Акцентовано увагу на необхідності впровадження стандартизованих показників ефективності та базатокритеріальних систем оцінювання, які охоплюють фінансові та нефінансові параметри результативності, що дозволяє здійснювати безперервний моніторинг і своєчасне коригування процесів. Встановлено, що інтеграція цифрових технологій, зокрема роботизованої автоматизації процесів, систем штучного інтелекту та аналітичних платформ, суттєво підвищує ефективність управління, сприяє реінжинірингу бізнес-процесів і забезпечує формування синергетичного ефекту. Визначено базові напрями оптимізації, серед яких виокремлено горизонтальне та вертикальне стиснення бізнес-процесів, що передбачає усунення надлишкових операцій, скорочення ієрархічних рівнів і делегування повноважень із використанням аутсорсингових інструментів. Доведено, що ефективність аутсорсингу залежить від обґрунтованості вибору процесів для передачі, рівня їх стратегічної значущості та здатності підприємства забезпечити рівновагу між економічною доцільністю та стратегічною орієнтацією. На основі аналізу практик провідних компаній, зокрема Global Bilgi, Deloitte, Agility та КРМГ, встановлено, що сучасні аутсорсингові моделі орієнтовані на індивідуалізацію рішень, цифровізацію процесів та інтеграцію зовнішніх компетенцій у внутрішню структуру підприємства. Узагальнено, що застосування аутсорсингу



This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

© Ключник Альона Володимирівна, 2026