ISSN 2786-6300 Print

УДК 35.072: 004.056

https://doi.org/10.52058/2786-6300-2026-5(47)-1350-1361

Помаза-Пономаренко Аліна Леонідівна доктор наук з державного управління, професор, завідувач науково-дослідної лабораторії з дослідження проблем управління у сфері цивільного захисту Національного університету цивільного захисту України, м. Черкаси, https://orcid.org/0000-0001-5666-9350

Тарадуда Дмитро Віталійович к.т.н., доцент, професор кафедри управління діяльністю підрозділів цивільного захисту інституту післядипломної освіти Львівського державний університет безпеки життєдіяльності, м. Львів, https://orcid.org/0000-0001-9167-0058

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДНИК НАЦІОНАЛЬНОЇ ОБОРОНИ

Анотація. Охарактеризовано інформаційну безпеку як стратегічний складник національної оборони держави в умовах гібридних загроз, цифрової трансформації та когнітивного протиборства. Обґрунтовано, що сучасна система інформаційної безпеки виходить за межі виключно технічного розвитку чи кібернетичного захисту, охоплюючи психологічні, соціальні, правові, комунікаційні й когнітивні аспекти функціонування держави та суспільства. Доведено, що інформаційна війна трансформується у когнітивну, основною метою якої є вплив на суспільну свідомість, руйнування довіри до державних інституцій, дестабілізація суспільних процесів і формування панічних настроїв.

Особливу увагу приділено концепції полігонального моделювання інформаційних загроз як інноваційному підходу до формування системи інформаційної оборони. Визначено сутність додекаедричної моделі гарантування інформаційної безпеки, що складається з таких взаємопов'язаних полігонів: когнітивної стійкості, кібербезпеки, медіаграмотності, стратегічних комунікацій, захисту критичної інфраструктури, інформаційної аналітики та стратегування, протидії дезінформації, технологічного розвитку, інфопростору, правозахисту, інституційної стійкості та міжнародної співпраці. Наголошено, що запропонована модель дозволяє перейти від реактивної до превентивної системи забезпечення інформаційної безпеки завдяки використанню штучного інтелекту, великих масивів даних, цифрового моніторингу та прогнозування інформаційних криз у режимі реального часу.

Увагу приділено міжнародній співпраці у сфері інформаційної безпеки, зокрема взаємодії України з НАТО та ЄС у напрямах кіберзахисту, стратегічних

комунікацій, протидії дезінформації та розвитку колективної цифрової стійкості. Акцентовано, що додекаедрична модель інформаційної безпеки формує нову архітектуру державної стійкості та створює передумови для ефективного протистояння сучасним інформаційним, кібернетичним і когнітивним загрозам.

Ключові слова: публічне управління, система безпеки, національна оборона, національна безпека, інформаційна безпека, кібератаки, медіаграмотність, полігональне моделювання, сектор безпеки й оборони, ЄС, НАТО.

Pomaza-Ponomarenko Alina Leonadivna Doctor in Public Administration, Professor, Head of the research laboratory for studying management problems in the field of civil protection of the National University of Civil Protection of Ukraine, Cherkasy, https://orcid.org/0000-0001-5666-9350

Taraduda Dmytro Vitaliovych Candidate of Technical Sciences, Associate Professor, Professor of the Department of Management of Civil Defense Units, Institute of Postgraduate Education, Lviv State University of Life Safety, Lviv, https://orcid.org/0000-0001-9167-0058

INFORMATION SECURITY AS A COMPONENT OF NATIONAL DEFENSE

Information security is characterized as a strategic component of the national defense of the state in the conditions of hybrid threats, digital transformation and cognitive confrontation. It is substantiated that the modern information security system goes beyond exclusively technical development or cybernetic protection, covering psychological, social, legal, communication and cognitive aspects of the functioning of the state and society. It is proven that information warfare is transformed into cognitive, the main goal of which is to influence public consciousness, destroy trust in state institutions, destabilize social processes and form panic moods.

Special attention is paid to the concept of polygonal modeling of information threats as an innovative approach to the formation of an information defense system. The essence of the dodecahedral model of information security assurance is determined, consisting of the following interconnected polygons: cognitive resilience, cybersecurity, media literacy, strategic communications, critical infrastructure protection, information analytics and strategizing, countering disinformation, technological development, infospace, human rights, institutional resilience, and international cooperation. It is emphasized that the proposed model allows for a transition from a reactive to a preventive information security system through the use of artificial intelligence, big data, digital monitoring, and real-time information crisis forecasting.

ISSN 2786-6300 Print

Attention is paid to international cooperation in the field of information security, in particular, the interaction of Ukraine with NATO and the EU in the areas of cyber defense, strategic communications, countering disinformation, and the development of collective digital resilience. It is emphasized that the dodecahedral model of information security forms a new architecture of state resilience and creates the prerequisites for effective counteraction to modern information, cybernetic, and cognitive threats.

Keywords: public administration, security system, national defense, national security, information security, cyberattacks, media literacy, polygonal modeling, security and defense sector, EU, NATO.

Постановка проблеми. У XXI ст. інформаційний простір перетворився на окремий театр воєнних дій, у межах якого здійснюється боротьба за суспільну свідомість, стійкість державних інституцій, контроль над інформаційними потоками та вплив на прийняття політичних рішень. Сучасні війни дедалі частіше мають гібридний характер, поєднуючи класичні військові дії з кібератаками, дезінформацією, психологічними операціями, інформаційним імпактом та маніпуляцією громадською думкою [12]. Саме тому інформаційна безпека сьогодні виступає не допоміжним елементом державної політики, а є одним із ключових складників оборонної сфери.

Для України питання інформаційної безпеки набуло особливого значення після початку російської агресії у 2014 році та повномасштабного вторгнення у 2022 році. Інформаційні атаки супроводжують практично кожен етап воєнних дій, спрямовуючись на деморалізацію українського населення, дискредитацію державних інституцій, створення панічних настроїв, поширення фейкових повідомлень і руйнування довіри до влади. Слід відзначити, що інфоатаки з боку рф – це звичне явище не тільки для України, а й для Грузії, Молдови, Німеччини, Польщі та інших країн. У цих умовах виникає необхідність формування нової концепції інформаційної оборони, що поєднує правові, організаційні, цифрові й аналітичні механізми публічного захисту.

Аналіз останніх досліджень і публікацій. Питання публічного управління у сфері національної й інформаційної безпеки привертає увагу як вітчизняних, так і зарубіжних науковців М. Єжеєва, А. Каляєва, Г. Кириченко, Л. Кочубей, О. Крюкова, В. Новікова, О. Пархоменко-Куцевіл, Г. Почепцова, О. Пучкова, О. Радченка, О. Савченко, І. Сердюк, Р. Стефанука, І, Ткешіашвілі, Т. Ярового та ін. [1; 2; 3; 4; 5; 7; 8; 9; 12; 14]. У той же час, існує необхідність у наукових розвідках щодо співвіднесення інформаційної безпеки та інформаційної оборони, а також визначення їхнього місця в системі безпеки.

Постановка завдання. Метою статті є визначення особливостей гарантування інформаційної безпеки як складника національної оборони.

Виклад основного матеріалу. Інформаційна безпека є складною багаторівневою системою захисту інтересів держави, суспільства й особистості

від зовнішніх і внутрішніх інформаційних загроз [3; 4]. Її особливість полягає в тому, що вона охоплює не лише технологічний компонент, але й психологічний, соціальний, політичний, правовий та когнітивний виміри.

У сучасних умовах оборонна сфера вже не обмежується військовою інфраструктурою, збройними силами, кінетичною зброєю та ін. [1; 2; 5]. До цієї сфери належать кіберпростір, медіа середовище, цифрові комунікації, системи управління критичною інфраструктурою, цифрові технології, зокрема, штучний інтелект, інформаційно-аналітичні системи, когнітивна безпека суспільства та ін. Особливу роль при цьому відіграє захист стратегічних інформаційних ресурсів держави. Йдеться про державні реєстри, військові бази даних, цифрові системи управління, канали урядового зв'язку та системи критичної інфраструктури.

Однією з перспективних інноваційних ідей у сфері гарантування інформаційної безпеки є концепція полігонального моделювання інформаційних загроз (рис. 1). Сутність даної концепції полягає в тому, що інфобезпека розглядається з позиції низки блоків (полігонів). Полігональне моделювання – це створення багаторівневих цифрових полігонів, які визначають підсистеми, на які спрямовані інформаційні атаки, кібератаки, інформаційні кампанії. На відміну від класичних кіберполігонів, запропонована модель передбачає: інтеграцію психологічних моделей поведінки населення; аналіз швидкості поширення фейків; симуляцію панічних хвиль; прогнозування дестабілізаційних процесів; моделювання інформаційних криз у реальному часі.

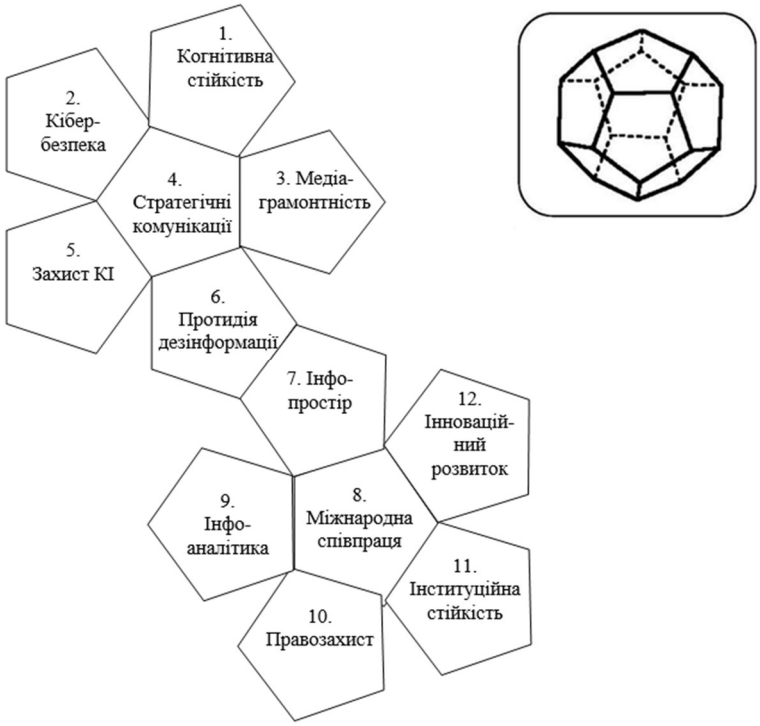

Рис. 1. Полігони додекаедричної моделі гарантування інформаційної безпеки
Джерело: авторська розробка

ISSN 2786-6300 Print

На наше переконання, застосовуючи полігональне моделювання, можна визначити такі полігони додекаедричної моделі гарантування інформаційної безпеки: 1)когнітивна стійкість; 2)кібербезпека (цифрова безпека); 3)медіаграмотність; 4)стратегічні комунікації; 5) захист критичної інфраструктури; 6) інформаційна аналітика та стратегування; 7) протидія дезінформації; 8) інноваційний і технологічних розвиток; 9) інфопростір; 10) правозахист; 11) інституційна стійкість; 12) міжнародна співпраця та підтримка. Зважаючи на ємність і багатоаспектність полігонів додекаедричної моделі гарантування інформаційної безпеки, уважаємо за доцільне зупинитись на їхньому більш детальному розгляді.

1. Когнітивна стійкість визначає здатність суспільства зберігати критичне мислення, психологічну рівновагу та здатність до раціонального аналізу інформації навіть в умовах масштабного інформаційного тиску. Саме когнітивна сфера та ментальне здоров'я сьогодні є основною мішенню інформаційної війни, оскільки вплив на свідомість населення дозволяє противнику формувати паніку, соціальну агресію й апатію, недовіру до держави та деструктивні суспільні настрої [4; 7] У сучасних умовах інформаційна війна дедалі більше трансформується у когнітивну війну, де головною ціллю стає не фізичне знищення об'єктів, а модифікація поведінки населення, нав'язування вигідних противнику моделей сприйняття реальності та руйнування національної ідентичності.

2. Кібербезпека (цифрова безпека) є одним із центральних елементів інформаційної оборони держави, оскільки сучасна інфраструктура управління, оборонної сфери, економіки й енергетики функціонує переважно у цифровому середовищі. Будь-яке порушення функціонування цифрових систем може спричинити масштабні наслідки для нацбезпеки. Особливістю сучасних кіберзагроз є їхня комплексність, латентність і швидкість поширення. Кібератаки можуть бути спрямовані не лише на викрадення інформації, але й на дестабілізацію системи державного управління та сектору безпеки й оборони, руйнування логістичних систем, порушення роботи енергетичної та іншої критичної інфраструктури, а також створення інформаційного хаосу.

3. Медіаграмотність є одним із фундаментальних інструментів суспільної стійкості до інформаційної агресії. Саме рівень медіаграмотності населення визначає здатність громадян розпізнавати маніпуляції, відокремлювати факти від пропаганди та критично оцінювати інформаційні повідомлення. Уважаємо, що медіаграмотність повинна розглядатися не як освітня дисципліна, а як елемент оборонної політики держави [10; 13]. Фактично йдеться про формування інформаційного імунітету суспільства.

4. Стратегічні комунікації забезпечують координацію інформаційної політики держави, узгодженість дій органів влади та формування єдиного інформаційного наративу [12]. У кризових умовах відсутність системних

ISSN 2786-6300 Print

стратегічних комунікацій призводить до інформаційного вакууму, який швидко заповнюється дезінформацією, панікою та ворожими інформаційними впливами.

5. Критична інформаційна інфраструктура охоплює енергетичні системи, транспортні мережі, банківський сектор, військові комунікації, системи зв'язку та цифрові державні сервіси та ін. Порушення функціонування хоча б одного з цих елементів може спричинити системний ефект дестабілізації всієї держави. Кожна країна визначає власний реєстр об'єктів критичної інфраструктури, проте схожість закордонних практик у цій сфері полягає у застосуванні секторального підходу [6].

6. Інформаційна аналітика та стратегування забезпечують вчасне прогнозування інформаційних загроз, аналіз інформаційних потоків та виявлення ознак інформаційних операцій. У сучасних умовах інформаційна аналітика повинна базуватися на технологіях штучного інтелекту, великих даних та автоматизованого моніторингу цифрового середовища, тобто передбачати дієве використання новітніх технологій [5].

7. Дезінформація є одним із головних інструментів інформаційної агресії, оскільки дозволяє маніпулювати суспільною свідомістю без прямого військового втручання. Ефективна протидія дезінформації потребує поєднання правових, технологічних, освітніх та комунікаційних механізмів. Дезінформація безпосередньо пов'язана з психологічної безпекою, що передбачає захист населення від інформаційно-психологічних впливів, спрямованих на деморалізацію, формування страху та руйнування соціальної згуртованості. Саме психологічна стійкість суспільства визначає здатність держави тривалий час протистояти гібридним загрозам [3].

8. Технологічний і технічний суверенітет означає здатність держави створювати власні цифрові технології, програмні рішення та системи інформаційного захисту без критичної залежності від зовнішніх суб'єктів. Для України це питання набуває стратегічного значення, оскільки технологічна та технічна залежність створює ризики зовнішнього контролю критично важливими інформаційними процесами.

9. Правовий вимір додекаедричної моделі передбачає формування нормативно-правової основи функціонування системи інформаційної безпеки. Саме правові інструменти забезпечують визначення компетенції органів влади, відповідальність за інформаційні правопорушення, регулювання кібербезпеки, захист персональних даних, функціонування системи стратегічних комунікацій і протидію інформаційній агресії.

10. Інфопростір передбачає створення інтегрованої системи захисту інформаційного середовища держави, включаючи військові інформаційні системи, державні реєстри, електронне урядування та комунікаційні мережі. У майбутньому інфосфера трансформуватиметься у повноцінну цифрову екосистему

ISSN 2786-6300 Print

національної безпеки, де елементи штучного інтелекту, автоматизовані системи аналізу загроз та квантові технології забезпечуватимуть випереджувальний характер реагування на інформаційні загрози.

11. Інституційна стійкість означає дієве функціонування та взаємодію державних і недержавних інституцій у сфері гарантування інформаційної безпеки. Це відбувається за рахунок використання низки публічно-управлінських інструментів (правових, ресурсних, соціально-політичних тощо) [2; 4].

12. Міжнародна співпраця та підтримка у сфері гарантування інформаційної безпеки набуває значення одного з ключових механізмів зміцнення національної стійкості держав до інформаційної агресії. Сутність цього напрямку полягає не лише у наданні технічної чи фінансової допомоги, але й у створенні єдиного інформаційно-безпекового простору, де відбувається координація дій щодо виявлення, попередження та нейтралізації інформаційних загроз. Особливо важливим це є для України, яка в умовах повномасштабної агресії рф фактично стала полігоном апробації новітніх методів гібридної війни, що поєднують військові дії з масштабними інформаційними атаками, кібервпливом, цифровими диверсіями та психологічними операціями.

Одним із провідних напрямів міжнародної взаємодії у сфері інформаційної безпеки є співробітництво з НАТО. Саме в межах партнерства з цим альянсом Україна отримує доступ до сучасних технологій кіберзахисту, систем моніторингу цифрових загроз, аналітичних платформ протидії дезінформації та механізмів координації кризового реагування [3]. Водночас співпраця з ЄС відкриває можливості інтеграції України до європейської системи інфобезпеки, що передбачає гармонізацію законодавства, розвиток системи кіберстійкості, обмін інформацією про загрози та спільну участь у програмах цифрової трансформації.

Особливого значення набуває співпраця у сфері боротьби з дезінформацією та інформаційно-психологічними операціями. Сучасна інформаційна агресія характеризується тим, що її основною ціллю стає не лише дестабілізація державних інституцій, але й руйнування суспільної довіри, формування панічних настроїв, поляризація суспільства та підрив національної єдності [1]. Саме тому міжнародна підтримка у сфері інформаційної безпеки передбачає створення спільних платформ фактчекінгу, систем аналізу інформаційних потоків, центрів стратегічних комунікацій та мереж реагування на інформаційні інциденти, а також надання/отримання грантів на підвищення рівня безпеки в тій чи іншій країні.

Не менш важливим компонентом міжнародної співпраці є розвиток системи колективної кібероборони [8]. У сучасному цифровому середовищі кібератаки можуть бути спрямовані на критичну інфраструктуру, енергетичні системи, транспортні мережі, банківський сектор, військові об’єкти та державні

ISSN 2786-6300 Print

реєстри. З огляду на це міжнародні партнери України забезпечують її підтримку у сфері передачі технологій кіберзахисту, підготовки фахівців із цифрової безпеки, проведення спільних кібернавчань, створення резервних систем збереження даних, формування механізмів оперативного реагування на кіберінциденти тощо [14].

Власне, міжнародна співпраця у сфері інформаційної безпеки повинна розглядатися не лише через безпекову, але й гуманітарну й освітню призму. Одним із найбільш небезпечних наслідків інформаційної агресії є маніпулювання свідомістю населення, поширення пропаганди та викривлення історичної пам'яті. Саме тому міжнародні програми підтримки дедалі більше орієнтуються на розвиток медіаграмотності, критичного мислення, цифрової культури та інформаційної стійкості суспільства. Такі програми дозволяють формувати у громадян здатність розпізнавати маніпулятивний контент, перевіряти джерела інформації та протидіяти психологічному впливу.

Наприклад, останнім часом у Польщі зреалізовано низку заходів щодо протистояння дезінформації з боку рф: заборонено трансляцію «Спутника», офіційно запустилася українська редакція Telewizja Polska, телеканал Slava TV. До речі, Slava TV є одним із найважливіших проєктів Медіацентру для закордонних мов (Ośrodek Mediów dla Zagranicy TVP) – нового підрозділу TVP, створеного у грудні 2024 року. Slava TV транслює програми протягом 6 год. щодня на каналі «Biełsat». Крім того, запущено вебсайт Slava TV, на якому розміщено ключову інформацію про Україну. Медіацентр TVP для закордонних справ (Ośrodek Mediów dla Zagranicy TVP) фінансується Міністерством закордонних справ Республіки Польща. Головою OMdZ є Міхал Бронятовський [15]. У квітні 2026 року розпочав роботу польський суспільний мовник – грузинськомовна новинна служба [9]. У своєму першому випуску ця новин служба заявила, що висвітлюватиме «важливе», говоритиме про європейські цінності та викриватиме російську дезінформацію [там само].

Принагідно відзначимо, що з 2022 року діє новий Кодекс поведінки (практики) протидії дезінформації, спрямований на досягнення цілей рекомендацій Комісії від травня 2021 року, зокрема, щодо встановлення значного спектру зобов'язань і заходів для боротьби з дезінформацією в Інтернеті [11]. Власне, цей документ був прийнятий у 2018 році, але саме у 2022 році він був значно посилений і визнаний кодексом етики відповідно до Закону про цифрові послуги. Кодекс є результатом роботи, проведеної підписантами. Вони самі вирішують, які зобов'язання беруть на себе, і саме за них несуть відповідальність щодо забезпечення їх ефективного виконання. Кодекс не був схвалений Комісією, хоча Комісія виклала свої очікування в керівних принципах і вважає, що Кодекс в цілому відповідає цим очікуванням. Підписанти взяли на себе зобов'язання за такими напрямками: зменшувати

ISSN 2786-6300 Print

фінансове стимулювання поширення дезінформації; сприяти прозорості у сфері політичної реклами; надавати користувачам більше можливостей для орієнтації в інформаційному просторі; зміцнювати співпрацю з організаціями, які займаються перевіркою фактів; а також забезпечувати науковцям кращий і ширший доступ до необхідних даних. Підписанти матимуть 6 місяців для виконання зобов'язань та заходів. Разом з Європейською групою регуляторів аудіовізуальних медіапослуг (ERGA) та Європейською обсерваторією цифрових медіа (EDMO) Комісія регулярно оцінюватиме прогрес у впровадженні Кодексу на основі детальних якісних та кількісних звітів, які очікуються від підписантів [там само].

Уважаємо, що в контексті полігонального моделювання інформаційної безпеки міжнародна співпраця може бути представлена як окремий полігон у структурі додекаедричної моделі національної оборони, який поєднує між собою всі інші елементи системи безпеки. Цей полігон взаємодіє з кібербезпекою, цифровим урядуванням, оборонною інфраструктурою, стратегічними комунікаціями, полігоном «медіа грамотність», інформаційною стійкістю населення. Саме така модель демонструє, що міжнародна підтримка виступає не допоміжним, а інтегруючим елементом сучасної архітектури інформаційної безпеки держави.

Крім того, перспективним напрямом розвитку міжнародної взаємодії є створення транснаціональних центрів прогнозування інформаційних загроз, які використовуватимуть штучний інтелект, великі масиви даних та алгоритми полігонального аналізу для прогнозування сценаріїв інформаційних атак. Уважаємо, що такий підхід дозволить перейти від реактивної моделі безпеки до проактивної, у межах якої держава та її партнери не лише реагують на інформаційні загрози, але й прогнозують їх виникнення та формують превентивні механізми захисту.

Отже, міжнародна співпраця та підтримка у сфері гарантування інформаційної безпеки є стратегічною основою формування сучасної системи національної оборони, яка передбачає дотримання принципів колективної стійкості, цифрової взаємодії, інформаційної солідарності та спільного реагування на глобальні виклики. В умовах сучасної гібридної війни саме міжнародна координація дозволяє забезпечити ефективний захист інформаційного простору держави, підвищити рівень стійкості суспільства та створити передумови для довгострокової безпеки й стабільності.

Висновки. Отже, інформаційна безпека у сучасних умовах виступає повноцінним складником національної оборони та покликана забезпечити стійкість держави до інформаційної агресії, кіберзагроз і когнітивних впливів. Їх гібридний характер зумовлює необхідність формування нових підходів до захисту інформаційного простору, де поєднуються кібернетичні, психологічні,

ISSN 2786-6300 Print

когнітивні та цифрові механізми. З огляду на багатоаспектність інформаційної безпеки запропонована додекаедрична модель її гарантування, що дозволяє сформувати новий підхід до розуміння такої безпеки як багаторівневої полігональної системи захисту держави. На нашу думку, її практична реалізація здатна забезпечити формування стратегічно стійкої держави, здатної ефективно протистояти сучасним формам гібридної війни, інформаційної агресії та цифрових загроз. Запропонована модель полігонального моделювання інформаційних загроз створює можливість переходу від реактивної до превентивної моделі інформаційної оборони. У післявоєнний період саме інноваційні механізми інформаційної безпеки можуть стати фундаментом нової архітектури державної стійкості.

Література:

1. Єжеєв М. Система забезпечення національної безпеки як складова публічного управління країни // Публічно-управлінські та цифрові практики. 2024. Вип. 1. С. 45–54.

2. Каляєв А.О. Теоретичні підходи щодо трансформації сучасних моделей державногоуправління у сфері безпеки та оборони // Ефективність державного управління. 2018. Вип.1 (54). С. 13–19.

3. Кириченко Г. Публічне управління у сфері інформаційної безпеки: теоретико-правовий аналіз сучасних викликів // Herald of Khmelnytskyi National University. Economic sciences 2026, No 2. https://doi.org/10.31891/2307-5740-2026-352-5.

4. Кочубей Л.О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі) // Наукові записки Інституту політичних і етнонаціональних досліджень імені І.Ф. Кураса. 2015. № 3. С. 220–237.

5. Пархоменко-Куцевіл О. І. Проблеми забезпечення національної безпеки в умовах воєнного часу // Науковий вісник Вінницької академії безперервної освіти. Серія «Екологія. Публічне управління та адміністрування». 2023. Вип. 3. С. 143–150. DOI: https://doi.org/ 10.32782/2786-5 681-2023-3.

6. Помаза-Пономаренко А.Л., Тарадуда Д.В. Механізми забезпечення цивільної безпеки України: аспекти попередження НС на об'єктах військово-промислового комплексу // Публічне адміністрування та національна безпека. 2024. № 3 (44). https://www.inter-nauka.com/issues/administration2024/3/9732.

7. Сердюк І.А. Підходи публічного управління до інформаційної безпеки особистості // Публічне урядування, 2022. № 3 (31). С. 53–59.

8. Стефанчук Р. Гарантії зовнішньої підтримки україни в умовах воєнного стану: безпековий напрям // Право України. 2024. № 10. С. 121–136. DOI: 10.33498/louu-2024-10-121.

9. Gvadzabia M. Poland's public broadcaster launches Georgian-language news service. 28.04.2026. URL: https://oc-media.org/polands-public-broadcaster-launches-georgian-language-news-service/.

10. Kharchenko S., Savchuk A., Dehtiarova H., Pomaza-Ponomarenko A., Siemilietov O. Media Literacy of Citizens as a Factor in Counteracting Manipulative Influence on the State // European Journal of Sustainable Development, 2026. vol. 15(1), 563. https://doi.org/10.14207/ejsd. 2026.v15n1p563.

11. Kodeks postępowania w zakresie zwalczania dezinformacji z 2022 r. // Komisja Europejska. URL: https://digital-strategy.ec.europa.eu/pl/policies/code-practice-disinformation.

12. Novikov V. Approaches to improvement of the institutional system and mechanisms of public administration in the conditions of information-hybrid wars // Eurasian Academic Research Journal. 2020. Vol. 37. Pp. 75–80.

13. Pomaza-Ponomarenko A., Akhmedova O., Naumenko M., Kurtsev O., Kyrkovskyi V. Digital technologies as a driver of infrastructure modernization and innovative progress in the context of sustainable development Goal 9 // European Journal of Sustainable Development Research, Volume 10, Issue 2, 2026, Article No: em0392. https://doi.org/10.29333/ejosdr/18308.

14. Radchenko O., Kriukov O., Kovach V. ext of "Civilizations Clash" as the Main Object of Infovation War in Ukraine. In: Radchenko O., Kovach V., Semenets-Orlova I., Zaporozhets A. (eds) National Security Drivers of Ukraine. 2023. Contributions to Political Science. Springer, Cham. https://doi.org/10.1007/978-3-031-33724-6_18. pp. 301–316.

15. Slawa.tv. URL: https://slawa.tv/.

References:

1. Ezheiev, M. (2024). Systema zabezpechennia natsionalnoi bezpeky yak skladova publichnoho upravlinnia krainy [The system of ensuring national security as a component of the country's public administration]. *Publichno-upravlinski ta tsyfrovi praktyky – Public administration and digital practices*, 1, 45–54 [in Ukrainian].

2. Kaliiaev, A.O. (2018). Teoretychni pidkhody shchodo transformatsii suchasnykh modelei derzhavnoho upravlinnia u sferibezpeky ta oborony [Theoretical approaches to the transformation of modern models of public administration in the field of security and defense]. *Efektyvnist derzhavnoho upravlinnia – Effectiveness of public administration*, 1 (54), 13–19 [in Ukrainian].

3. Kyrychenko, G. (2026). Publichne upravlinnya u sferi informatsiynoyi bezpeky: teoretyko-pravovyy analiz suchasnykh vyklykiv [Public administration in the sphere of information security: theoretical and legal analysis of modern challenges]. *Herald of Khmelnytskyi National University. Economic sciences*, 2. https://doi.org/10.31891/2307-5740-2026-352-5 [in Ukrainian].

4. Kochubei, L.O. (2015). Informatsiina bezpeka derzhavy: instrumenty zakhystu ukrainskoho informatsiinoho polia (naprykladi osoblyvostei informatsiino-komunikatsiinykh tekhnolohii u suchasnomu Donbasi) [Information security of the state: tools for protecting the Ukrainian information field (using the example of the features of information and communication technologies in modern Donbas)]. *Naukovi zapysky Instytutu politychnykh ietnonatsionalnykh doslidzhen imeni I.F. Kurasa – Scientific notes of the I.F. Kuras Institute of Political and Ethno-National Studies*, 3, 220–237 [in Ukrainian].

5. Parkhomenko-Kutsevil, O.I. (2023). Problemy zabezpechennia natsionalnoi bezpeky v umovakh voiennoho chasu [Problems of ensuring national security in wartime]. *Naukovyi visnyk Vinnytskoi akademii bezperervnoi osvity. Seriia "Ekologiia. Publichne upravlinnia ta administruvannia" – Scientific Bulletin of the Vinnytsia Academy of Continuing Education. Series "Ecology. Public Management and Administration",* 3, 143–150. DOI: https://doi.org/10.32782/2786-5681-2023-3. [in Ukrainian].

6. Pomaza-Ponomarenko, A.L. & Taraduda, D.V. (2024). Mekhanizmy zabezpechennya tsyvil′noyi bezpeky Ukrayiny: aspekty poperedzhennya NS na ob″yektakh viys′kovo-promyslovoho kompleksu [Mechanisms for ensuring civil security of Ukraine: aspects of emergency prevention at military-industrial complex facilities]. *Publichne administruvannya ta natsional'na bezpeka – Public Administration and National Security,* 3 (44). Retrieved from https://www.inter-nauka.com /issues/administration2024/3/9732 [in Ukrainian].

7. Serdiuk, I.A. (2022). Pidkhody publichnoho upravlinnia do informatsiinoi bezpeky osobi [Public administration approaches to information security of the individual]. *Publichne uriaduvannia – Public governance*, 3(31), 53–59 [in Ukrainian].

8. Stefanchuk, R. (2024). Harantiyi zovnishn′oyi pidtrymky ukrayiny v umovakh voyennoho stanu: bezpekovyy napryam [Guarantees of foreign support for Ukraine in martial law: security direction]. *Pravo Ukrayiny – Law of Ukraine*, 10, 121–136. DOI: 10.33498/louu-2024-10-121.

9. Gvadzabia, M. (2026). Poland's public broadcaster launches Georgian-language news service. URL: https://oc-media.org/polands-public-broadcaster-launches-georgian-language-news-service/ [In English].

10. Kharchenko, S., Savchuk, A., Dehtiarova, H., Pomaza-Ponomarenko, A. & Siemilietov, O. (2026). Media Literacy of Citizens as a Factor in Counteracting Manipulative Influence on the State. *European Journal of Sustainable Development*, 15(1), 563. https://doi.org/10.14207/ejsd.2026.v15n1p563. [In English]

11. Kodeks postępowania w zakresie zwalczania dezinformacji z 2022 r. Komisja Europejska. Retrieved from https://digital-strategy.ec.europa.eu/pl/policies/code-practice-disinformation [In Polish].

12. Novikov, V. (2020). Approaches to improvement of the institutional system and mechanisms of public administration in the conditions of information-hybrid wars. *Eurasian Academic Research Journal*, 37, 75–80 [In English].

13. Pomaza-Ponomarenko, A., Akhmedova, O., Naumenko, M., Kurtsev, O. & Kyrkovskyi, V. (2026). Digital technologies as a driver of infrastructure modernization and innovative progress in the context of sustainable development Goal 9. *European Journal of Sustainable Development Research*, 10, 2, https://doi.org/10.29333/ejosdr/18308 [In English].

14. Radchenko, O., Kriukov, O. & Kovach, V. (2023). "Civilizations Clash" as the Main Object of Infovation War in Ukraine. In: Radchenko O., Kovach V., Semenets-Orlova I., Zaporozhets A. (eds) National Security Drivers of Ukraine. 2023. Contributions to Political Science. Springer, Cham. https://doi.org/10.1007/978-3-031-33724-6_18. pp. 301-316 [In English].

15. Slawa.tv. (2026). Retrieved from https://slawa.tv/ [In English].

Дата першого надходження статті до видання: 27.04.2026
Дата прийняття статті до друку після рецензування: 11.05.2026