

*Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019).*

*Спеціальність – 281.*

*Державне управління: удосконалення та розвиток. 2024. № 11.*

**DOI: <http://doi.org/10.32702/2307-2156.2024.11.27>**

**УДК 351:355:342.7**

*С. П. Галушко,*

*аспірант, Національний університет цивільного захисту України*

*ORCID ID: <https://orcid.org/0009-0005-3169-1478>*

## **ПІДХОДИ ДО ВДОСКОНАЛЕННЯ СИСТЕМИ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ЦИФРОВІЗАЦІЇ**

*S. Galushko,*

*Postgraduate student, National University of Civil Protection of Ukraine, Kharkiv*

## **APPROACHES TO THE IMPROVEMENT OF THE PUBLIC ADMINISTRATION SYSTEM IN THE SPHERE OF NATIONAL SECURITY OF UKRAINE UNDER THE CONDITIONS OF DIGITALIZATION**

*Виявлено, що за сучасних умов функціонування України ускладненим є забезпечення її системи безпеки, на підтримку якої виділяється основна частина державного бюджету. Акцентовано, що бюджетних видатків на гарантування національної безпеки не вистачає, тому слід говорити про розвиток такого інструментарію, як публічно-приватне партнерство. Він забезпечує отримання додаткових джерел фінансування та розвиток інноваційної діяльності в національній економіці загалом і в оборонному секторі зокрема. Це зумовлює необхідність прийняття відповідних стимулюючих і регулюючих заходів і методів на загальнодержавному та регіональному рівнях по відношенню до інституцій, які розвивають інноваційну діяльність, у т.ч. у безпековій сфері. Аналіз статистичних даних*

Європейського інвестиційного банку та дослідницької організації *International Crisis Group* дозволив проранжувати країни у двох площинах: 1) стан розвитку цифрових технологій; 2) наявність збройних конфліктів на території країни. Аргументовано гіпотезу, що значні досягнення країни у сфері цифровізації та розвитку цифрових технологій підвищують рівень національної безпеки. Установлено, що неоголошена війна РФ проти України позначилась на рівні безпеки та соціально-економічного розвитку в інших країнах світу (Азербайджан, Вірменія, Ізраїль та ін.). Наполягається, що цей вплив є нічим іншим, як «російський слідом». У низці країн, зокрема Великій Британії, Польщі, Туреччині та США, було виявлено кібернапади на сектор безпеки, скоєні за підтримки РФ. У деяких випадках ці атаки здійснювались паралельно з іншими гібридними загрозами щодо енергетичних об'єктів (наприклад, надання шкідливого впливу та скорочення постачання природного газу). Якщо скласти все це разом, то стає очевидним, що в останні десять років РФ веде регулярну гібридну кампанію, спрямовану на підрив системи безпеки різних країн світу, у т.ч. України, причому зі зростаючою силою. Дана обставина вимагає постійного моніторингу з позиції експертів, особливо за умов ескалації російсько-української війни. Обґрунтовано, що зменшити градус негативного впливу цих причин можливо за рахунок результативної реалізації механізмів публічного управління у сфері національної безпеки та інноваційного розвитку секторів і галузей економіки в Україні, що передбачають упровадження прогресивних моделей соціально-економічного розвитку та сучасних моделей інформаційних технологій.

*Emphasis is placed on the prospects and relevance of the introduction of ecological innovations in the national economy in general and in the agricultural sector in particular, as well as on the formation of their primary and secondary market in Ukraine. It was determined that this necessitates the adoption of stimulating and regulatory measures and methods at the national and regional levels. Among these management methods, institutional, financial and economic, informational and other methods are distinguished, the use of which is intended to increase the level of the security system (economic, social and environmental). The system of the specified methods of public management of the formation of the ecological innovation market by enterprises of the national economy and agricultural industry includes means that have proven their effectiveness – public-private*

*partnership and investment. In order to determine the prospects of its implementation, the peculiarities of the functioning of the operating enterprises in the agricultural sector of Ukraine and the state of the ecological and innovative measures implemented by them were analyzed. It was established that in the period 2014–2022, the number of agricultural enterprises in Ukraine significantly decreased, in particular, by 1.4 times. It was found that this also led to a decrease in the amount of funding allocated within the scope of capital investments for environmental protection by types of economic activity (agriculture) with distribution by types of environmental protection measures in 2022–2023. Regions-leaders in reducing the amount were identified agricultural enterprises (Donetsk, Luhansk, Zaporizhzhya, Kharkiv, Kherson and other regions). It has been proven that it is possible to reduce the degree of influence of external and internal factors on the activities of agricultural enterprises due to the effective implementation of ecological and innovative mechanisms of public management in the field of agribusiness development in Ukraine. It is substantiated that these mechanisms involve the introduction of progressive models of socio-economic development and modern models of information technologies.*

**Ключові слова:** *публічне управління, сфера національної безпеки, цифровізація, технології цифровізації, цифрова трансформація, органи влади, публічно-приватне партнерство.*

**Keywords:** *public administration, sphere of national security, digitalization, digitalization technologies, digital transformation, authorities, public-private partnership.*

**Постановка проблеми.** У 2010 році було прийнято Закон України «Про державно-приватне партнерство» [1]. У період 2016–2017 рр. постановами Кабінету Міністрів України було затверджено Порядок заміни приватного партнера за договором, укладеним у рамках державно-приватного партнерства, та нову редакцію оцінювання ефективності здійснення державно-приватного партнерства [там само]. Останні зміни до законодавства у сфері державно-приватного партнерства (публічно-приватного партнерства) дають підстави стверджувати, що вони зумовлюють підвищення інтересу до реалізації проєктів

на умовах державно-приватного партнерства у сферах, що є важливими для суспільства. Однією з таких сфер є національна безпека, що вимагає розвитку публічно-приватного партнерства та розвитку інноваційної діяльності. Це є необхідним для гарантування системи безпеки України, бюджетні видатки якої спрямовані на оборонну сферу та сектор безпеки. Відтак, потрібно говорити про важливість залучення позабюджетних коштів на підвищення рівня національної безпеки України і допомогти в цьому може застосування публічно-приватного партнерства. Усе це засвідчує актуальність обраної теми дослідження.

**Аналіз останніх досліджень і публікацій.** Розгляду особливостей формування та реалізації державної політики у сфері забезпечення національної безпеки присвячені публікації таких науковців, як Базиліук Я., Гриценко А., Денисенко М., Домбровської С., Карсруд А., Клют Р., Колісніченко П., Крюкова О., Лекарь С., Машкова О., Нижник Н., Орлик В., Помази-Пономаренко А., Почепцов Г, Ситник Г., Скотт Дж., Тайер А., Чуб С. та інші [2; 5–6; 7].

**Мета статті** – обґрунтування підходів до вдосконалення системи публічного управління у сфері національної безпеки України в умовах цифровізації в Україні.

**Виклад основного матеріалу.** За інформацією Європейського інвестиційного банку (далі – ЄІБ) у Європі є дуже розвиненим застосування інструментарію публічно-приватного партнерства. ЄІБ навів такі дані щодо реалізованих інноваційних проєктів у межах публічно-приватного партнерства (далі – ППП) у 2023 році [4]:

– 38 транзакцій у межах ринку ППП досягли фінансового завершення загальною вартістю 13,6 млрд євро.

– у вартісному вираженні ринок ППП Європи зріс на 35% порівняно з 2022 роком.

– у 2023 році в кількісному вираженні ринок ППП скоротився на 17% порівняно з 2022 роком.

– у звітному періоді найактивнішим учасником ринку ППП була Німеччина за вартістю та кількістю проєктів ППП (до речі, у 2022 р. найактивною була Франція на ринку ППП);

– 13 країн Європи закрили принаймні один проєкт ППП, порівняно з 15 проєктами ППП у 2022 році;

– у звітному періоді транспортна сфера була визнана найбільшим результативним сектором як у вартісному, так і в кількісному вираженні реалізованих проєктів ППП (рис. 1);

– понад 53% закритих транзакцій у Європі були проведені в межах ППП;

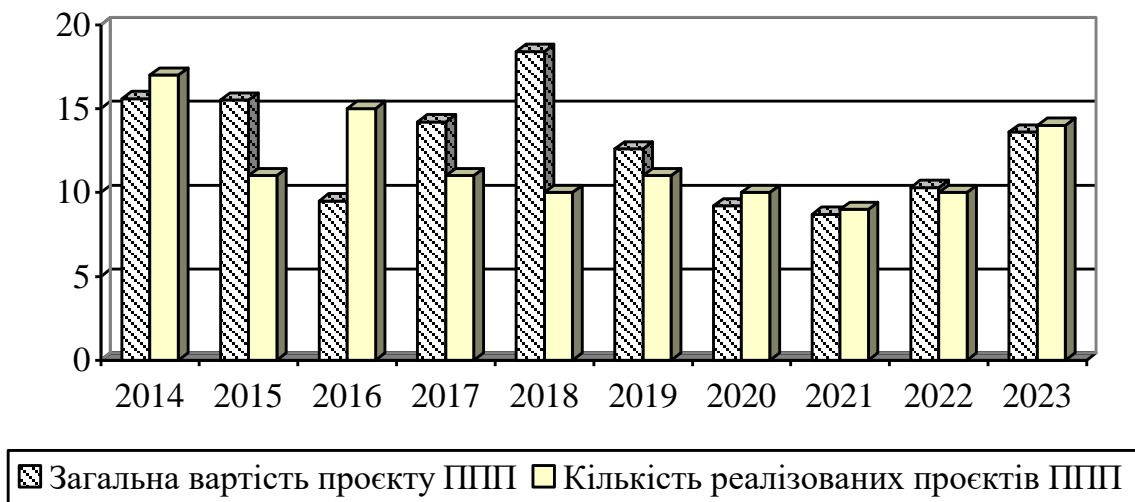
– виявлено, що Європа прагне досягти плато в розвитку ринку ППП (рис. 2).



**Рис. 1. Кількість проєктів ППП у Європі, що реалізуються в основних інфраструктурних секторах у 2023 р., у %**

*Джерело: складено на підставі [2; 4; 5–6].*

Слід відзначити, що серед не Європейських країн лідируючі позиції на ринку ППП займають такі держави: у 2018 році лідером із реалізації найбільших проєктів ППП є Туреччина, а у 2023 році – Ізраїль.

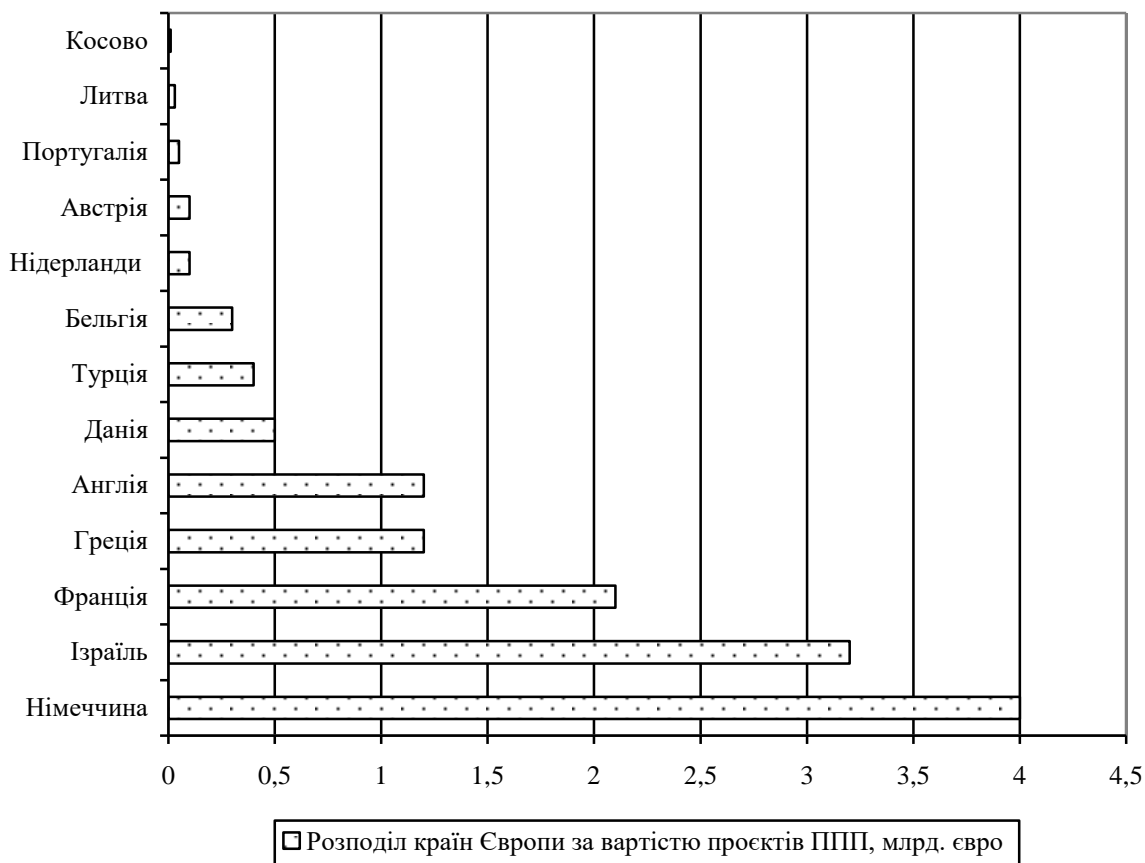


**Рис. 2. Стан зміни європейського ринку ППП за вартістю та кількістю реалізованих проєктів (2014-2023 рр.)**

*Джерело: складено на підставі [2; 4; 5–6]*

Слід зазначити, що у 2023 році спостерігалось збільшення вартості трансакцій за проєктами ППП у Європі, але відбувалось зменшення кількості договорів і проєктів ППП, закритих у 2023 році. Це може певною мірою відображати інфляційне середовище щодо цін на будівництво інфраструктурних об'єктів, що продовжує проявлятися на багатьох європейських ринках. Середовище високих процентних ставок у більшості європейські країни у 2022 та 2023 роках (незважаючи на відмінності між країнами) також збільшили загальну кількість і вартість проєктів протягом їх життєвого циклу. Це могло призвести до затримки чи зупинки проєктів ППП тендерних процесів через зниження прибутковості приватного сектору та підвищення вартості проєктів для державного та безпекового сектору.

У 2023 році було закрито 8 великих проєктів ППП у Європі (у порівнянні з трьома закритими європейськими проєктами ППП у 2022 році). Їх сукупна вартість склала 9,4 млрд євро, що становить 69% від загальної ринкової вартості (порівняно з 42% у 2022 році).



**Рис. 3. Розподіл країн Європи за вартістю проєктів ППП у 2023 році (у мільярдах євро)**

*Джерело: складено на підставі [2; 4; 5–6]*

Розгляд особливостей трансформації системи національної безпеки за кордоном дав підстави стверджувати, що ці процеси опосередковані політикою цифровізації та пов'язаними з нею ризиками та загрозами. Їх мережевий аналіз дозволив умовно виокремити:

– країни 1 рівня, які мають найкращі досягнення у сфері цифровізації та продажу її технологій, а також активно розвивають публічно-приватне партнерство в напрямку реалізації інноваційних проєктів (Бельгія, Великобританія, Ірландія, Італія, Канада, Нідерланди, Німеччина, Сінгапур, США, Фінляндія, Франція, Швейцарія, Швеція, Японія та ін.);

– країни 2 рівня, які відзначаються середніми показниками в розвитку цифрових технологій, і не мають конфліктів з іншими державами (Австралія,

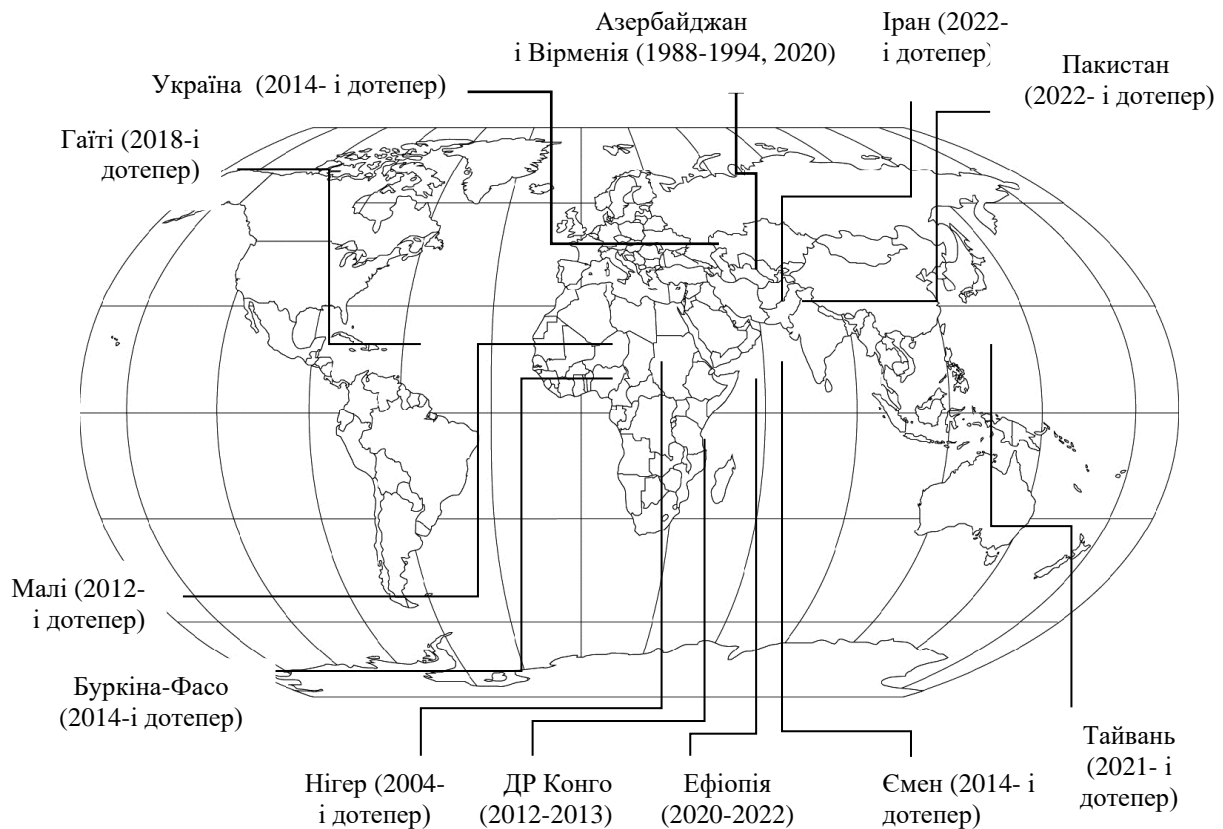
Індія, Іспанія);

– країни 3 рівня, які відзначаються значними показниками в розвитку цифрових технологій і публічно-приватного партнерства в напрямку реалізації інноваційних проєктів, але при цьому мають конфлікти з іншими державами (Ізраїль, Китай, Тайвань, Північна Корея та ін.);

– країни 4 рівня, які мають низькі показники в розвитку цифрових технологій (Буркіна-Фасо, Ефіопія, Ємен, ДР Конго, Малі, Нігер та ін.).

Мережевий аналіз проводився щодо показників центральностей у двох площинах: 1) стан використання Інтернету та Інтернету речей, кількість патентів на цифрові технології зв'язку, комп'ютерні та інші технології, стан розвитку штучного інтелекту, автоматизації та робототехніки, стан продажів відповідних технологій тощо; 2) рівень безпеки в країні, наявність на її території конфліктів (рис. 2). Під час мережевого аналізу показників у межах першої площини до уваги брались дані «Analyzing Affiliation Networks» (J. Scott) і Європейського інвестиційного банку, а в межах другої площини – дані дослідницької організації International Crisis Group [Топ; Analyzing Affiliation].

Визначено, що розуміння місця цифрових технологій у системі безпеки та публічного управління вимагає конкретизації ролі в цих процесах штучного інтелекту. Його характеристику слід проводити крізь призму визначення технологій цифровізації загалом як алгоритмічних і комп'ютерних систем (у тому числі програмне забезпечення та/або обладнання), що дозволяє акцентувати на такій особливості штучного інтелекту, як можливість самостійно навчатись і вдосконалюватись, а не тільки вирішувати складні проблеми чи робити прогнози або виконувати завдання, що потребують планування, організації тощо. Доведено, що ця особливість у розвитку штучного інтелекту набуває актуальності в коротко-, середньо- і довгостроковій перспективі у сфері забезпечення нацбезпеки по всьому світу.



**Рис. 4. Найбільша кількість збройних і військово-політичних конфліктів у світі у 2023 році**

*Джерело: складено на підставі [2]*

Погоджуємось із ученими, що російсько-українська війна актуалізувала значну кількість збройних конфліктів по всьому світові (Азербайджан, Ізраїль, Тайвань та ін.) [2]. У 2023 р. безпековий сектор у Європі отримав фінансування для реалізації європейських проєктів ППП в обсязі щонайменше 995 мільйонів євро складається (6 проєктів ППП було реалізовано в Німеччині, по 2 проєкти ППП у Литві та Бельгії) [там само]. 4 з 6 проєктів ППП у секторі громадського порядку та безпеки в Європі спрямовані на покращення надання поліцейських послуг.

Отже, поки що відсутнє єдине наукове розуміння того, як саме технологічні зміни національної безпеки мають відбуватися для того, щоб підвищувати її рівень. Наполягається, що дані зміни можуть зреалізовуватись у

напрямку забезпечення сталого розвитку, який передбачає підвищення конкурентоспроможності держави, стимулювання високотехнологічного розвитку галузей і секторів її економіки, тобто підтримку інноваційної діяльності в країні, що дозволяє підвищувати її рівень безпеки.

**Висновки.** Отже, за сучасних умов функціонування України ускладненим є забезпечення системи її безпеки, на підтримку якої виділяється основна частина державного бюджету. У той же час, бюджетних видатків на гарантування національної безпеки не вистачає, тому слід говорити про розвиток такого інструментарію, як публічно-приватне партнерство. Воно забезпечує отримання додаткових джерел фінансування та розвиток інноваційної діяльності в національній економіці загалом і в оборонному секторі зокрема. Це зумовлює необхідність прийняття відповідних стимулюючих і регулюючих заходів і методів на загальнодержавному та регіональному рівнях по відношенню до інституцій, які розвивають інноваційну діяльність, у т.ч. у безпековій сфері. Аналіз статистичних даних Європейського інвестиційного банку та дослідницької організації International Crisis Group дозволив проранжувати країни:

– країни 1 рівня, які мають найкращі досягнення у сфері цифровізації та продажу її технологій, а також активно розвивають публічно-приватне партнерство в напрямку реалізації інноваційних проєктів (Бельгія, Великобританія, Ірландія, Італія, Канада, Нідерланди, Німеччина, Сінгапур, США, Фінляндія, Франція, Швейцарія, Швеція, Японія та ін.);

– країни 2 рівня, які відзначаються середніми показниками в розвитку цифрових технологій, і не мають конфліктів з іншими державами (Австралія, Індія, Іспанія);

– країни 3 рівня, які відзначаються значними показниками в розвитку цифрових технологій і публічно-приватного партнерства в напрямку реалізації інноваційних проєктів, але при цьому мають конфлікти з іншими державами (Ізраїль, Китай, Тайвань, Північна Корея та ін.);

– країни 4 рівня, які мають низькі показники в розвитку цифрових

технологій (Буркіна-Фасо, Ефіопія, Ємен, ДР Конго, Малі, Нігер та ін.).

Крім того, встановлено, що неоголошена війна РФ проти України позначилась на рівні безпеки та соціально-економічного розвитку в інших країнах світу (Азербайджан, Вірменія, Ізраїль та ін.). Наполягається, що цей вплив є нічим іншим, як «російський слідом». У низці інших країн, зокрема Великій Британії, Польщі, Туреччині та США, було виявлено кібернапади на сектор безпеки, скоєні за підтримки РФ. У деяких випадках ці атаки здійснювались паралельно з іншими гібридними загрозами щодо енергетичних об'єктів (наприклад, надання шкідливого впливу та скорочення постачання природного газу) [2; 5–6]. Якщо скласти все це разом, то стає очевидним, що в останні десять років РФ веде регулярну гібридну кампанію, спрямовану на піддрив системи безпеки різних країн світу, причому зі зростаючою силою. Дана обставина вимагає постійного моніторингу з позиції експертів, особливо за умов ескалації російсько-української війни. Обґрунтовано, що зменшити градус негативного впливу цих причин можливо за рахунок результативної реалізації механізмів публічного управління у сфері національної безпеки та інноваційного розвитку секторів і галузей економіки в Україні, що передбачають упровадження прогресивних моделей соціально-економічного розвитку та сучасних моделей інформаційних технологій.

### **Література:**

1. Законодавство України // Офіційний веб-сайт Верховної Ради України.  
URL: <https://www.rada.gov.ua/news/zak>.
2. Помаза-Пономаренко А.Л., Тарадуда Д.В. Розвиток енергетичної сфери як імперативу енергетичної безпеки та національної економіки // Державне управління: удосконалення та розвиток. 2024. № 9. URL: <https://www.nauka.com.ua/index.php/dy/article/view/4601>. (дата звернення: 13.11.2024 р.).
3. Топ збройних та політичних конфліктів у 2023 році: що про них відомо // Слово і діло. URL:

<https://www.slovoidilo.ua/2023/04/03/infografika/svit/top-zbrojnyx-ta-politychnyx-konfliktiv-2023-roczy-pro-nyx-vidomo> (дата звернення: 13.11.2024 р.).

4. Review of the European public-private partnership market in 2023 // European Investment Bank. URL: <https://www.seifrance.fr/services/post/post.php?action=download&id=19558> (дата звернення: 13.11.2024 р.).

5. Pomaza-Ponomarenko A., Kryvova S., Hordieiev A., Hanzjuk A., Halunko O. Innovative Risk Management: Identification, Assessment and Management of Risks in the Context of Innovative Project Management // Economic Affairs (New Delhi). 2023, 68(4), pp. 2263–2275.

6. Pomaza-Ponomarenko A., Taraduda D., Leonenko N., Poroka S., Sukhachov M. Ensuring the safety of citizens in times of war: aspects of the organization of civil defense // AD ALTA: Journal of Interdisciplinary Research. 2024. Volume 14. Issue 1. Pp. 216–220.

7. Scott J. Analyzing Affiliation Networks. Handbook of Social Network Analysis, 2015. URL: <https://methods.sagepub.com/book/the-sage-handbook-of-social-network-analysis> (дата звернення: 13.11.2024 р.).

### **References:**

1. The official site of Verkhovna Rada of Ukraine (2024), “Legislation of Ukraine”, available at: <https://www.ukrstat.gov.ua/> (Accessed 13 Nov 2024).

2. Pomaza-Ponomarenko, A.L. and Tarduda, D.V. (2024), “Development of the energy sector as an imperative for energy security and the national economy”, *Derzhavne upravlinnya: udoskonalennya ta rozvytok*, vol. 9, available at: <https://www.nayka.com.ua/index.php/dy/article/view/4601> (Accessed 13 Nov 2024).

3. The Word and deed (2023), “Top armed and political conflicts in 2023: what is known about them”, available at: <https://www.slovoidilo.ua/2023/04/03/infografika/svit/top-zbrojnyx-ta-politychnyx-konfliktiv-2023-roczy-pro-nyx-vidomo> (Accessed 13 Nov 2024).

4. The European Investment Bank (2024), “Review of the European public-

private partnership market in 2023”, available at: <https://www.sefifrance.fr/services/post/post.php?action=download&id=19558> (Accessed 13 Nov 2024).

5. Pomaza-Ponomarenko, A., Kryvova, S., Hordieiev, A., Hanzhuk, A. and Halunko O. (2023), “Innovative Risk Management: Identification, Assessment and Management of Risks in the Context of Innovative Project Management”, *Economic Affairs*, vol. 68(4), pp. 2263–2275.

6. Pomaza-Ponomarenko, A., Taraduda, D., Leonenko, N., Poroka, S. and Sukhachov, M. (2024), “Ensuring the safety of citizens in times of war: aspects of the organization of civil defense”, *AD ALTA: Journal of Interdisciplinary Research*, vol. 14, issue 1, pp. 216–220.

7. Scott, J. (2015), “Analyzing Affiliation Networks. Handbook of Social Network Analysis”, available at: <https://methods.sagepub.com/book/the-sage-handbook-of-social-network-analysis> (Accessed 13 Nov 2024).

*Стаття надійшла до редакції 14.11.2024 р.*