

*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. 2025. № 11.*

**DOI: <http://doi.org/10.32702/2307-2156.2025.11.9>**

**УДК 351:342.57**

*V. V. Kushnikov,*

*аспірант, Національний аерокосмічний університет  
«Харківський авіаційний інститут»*

*ORCID ID: <https://orcid.org/0009-0003-0843-4516>*

*A. O. Diegtiar,*

*д. держ. упр., професор, Заслужений діяч науки і техніки України,  
професор кафедри економіки та публічного управління, Національний  
аерокосмічний університет «Харківський авіаційний інститут»*

*ORCID ID: <https://orcid.org/0000-0003-3258-447X>*

## **ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ ЯК ГЛОБАЛЬНА ПРОБЛЕМА**

*V. Kushnikov,*

*PhD student, National Aerospace University “Kharkiv Aviation Institute”*

*A. Diegtiar,*

*Doctor of Sciences in Public Administration, Honored Worker of Science and  
Technology of Ukraine, Full Professor,*

*Professor of the Department of Economics and Public Administration,  
National Aerospace University “Kharkiv Aviation Institute”*

## **ENSURING OF THE INFORMATION SECURITY OF THE STATE IN THE FACE OF HYBRID THREATS AS A GLOBAL PROBLEM**

*У статті досліджено специфіку забезпечення інформаційної безпеки держави в умовах гібридних загроз як глобальна проблема. Зокрема, визначено риси інформаційної безпеки як глобальної проблеми; виокремлено напрямки формування глобальної інформаційної безпеки; окреслено ліквідацію «цифрової нерівності» як одне із ключових завдань забезпечення глобальної інформаційної безпеки.*

*Показано, що, як глобальній проблемі, інформаційній безпеці притаманні наступні характеристики: вона виступає об'єктивним фактором та одним з найважливіших механізмів подальшого світового розвитку у його новій цивілізаційній формі; вона висувається на перший план у зв'язку з становленням планетарного інформаційного суспільства як початкової фази ноосфери інформаційна безпека; недостатнє забезпечення інформаційної безпеки призводить до загроз інформаційної війни, інформаційного тероризму тощо; для ефективного забезпечення інформаційної безпеки необхідні спільні зусилля усієї світової спільноти.*

*Виділено ключові напрямки формування глобальної інформаційної безпеки: захист єдиного світового інформаційного простору від різних небезпек та загроз; рівноправне використання планетарного інформаційного простору всіма народами та країнами світової спільноти; безпечний для людини, суспільства, держав, світової спільноти та біосфери розвиток цього інформаційного простору; позитивний вплив глобальної інформаційної безпеки, що формується, на перехід до сталого соціоекосистемного розвитку.*

*Підкреслено, що одним із завдань глобальної інформаційної безпеки є ліквідація «цифрової нерівності». Важливо забезпечити доступ усіх країн світової спільноти, а не лише країн-лідерів економічного розвитку, до глобального інформаційного простору, що дозволить їм отримувати повну, достовірну та своєчасну інформацію та інформаційні ресурси, необхідні для їхнього переходу до сталого розвитку. Це дозволить забезпечити максимально можливу орієнтацію суб'єкта у всьому інформаційному просторі.*

*The paper examines the specifics of ensuring of the information security of the state in the conditions of hybrid threats as a global problem. In particular, the features of information security as a global problem are identified; the directions of formation of global information security are defined; the elimination of "digital inequality" is outlined as one of the key tasks of ensuring of the global information security.*

*It is shown that, as a global problem, information security has the following characteristics: it acts as an objective factor and one of the most important mechanisms of further world development in its new civilizational form; it comes to the fore in connection with the formation of a planetary information society as the initial phase of the noosphere information security; insufficient provision of information security leads to threats of information war, information terrorism, etc.; joint efforts of the entire world community are necessary for effective provision of information security.*

*The following key areas of global information security formation are highlighted: protection of a single global information space from various dangers and threats; equal use of the planetary information space by all peoples and countries of the world community; development of this information space that is safe for humans, society, states, the world community and the biosphere; positive impact of the emerging global information security on the transition to sustainable socio-ecological development.*

*It is emphasized that one of the tasks of global information security is the elimination of "digital inequality". It is important to ensure access of all countries of the world community, and not only the leading countries in economic development, to the global information space, which will allow them to receive complete, reliable and timely information resources necessary for their transition to sustainable development. This will ensure the maximum possible orientation of the subject in the entire information space.*

**Ключові слова:** держава, інформаційна безпека, гібридні загрози, інформаційний простір, глобальна проблема.

**Keywords:** state, information security, hybrid threats, information space, global problem.

**Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями.** З розвитком інформатизації людина включилася до глобальних інформаційних систем, стаючи суб'єктом цих систем. Глобальні інформаційні системи пов'язують світ у єдине ціле та роблять усі держави інформаційно взаємозалежними. Розвиток інформаційних технологій призвів до глобалізації комунікаційних зв'язків на планеті, значного розширення транскордонних контактів. Творча міць сучасних інформаційно-комунікаційних технологій, їх ефективність та корисність багато в чому залежать від рівня відкритості цих технологій по відношенню до національного та світового інформаційного простору та потенціалу.

В даний час відбувається бурхливий розвиток глобальних інформаційних мереж зв'язку та інформаційних комунікацій: супутникового телебачення, радіомовлення, телефонного зв'язку та засобів факсимільної передачі інформації, глобальних комп'ютерних телекомунікаційних мереж, які використовують високошвидкісні міжконтинентальні супермагістралі. Внаслідок цього на планеті формується принципово новий інформаційний простір, який і буде основою життєдіяльності майбутнього інформаційного суспільства. У межах цього простору виробляється накопичення, обробка, зберігання та обмін інформацією між різними суб'єктами – людьми, організаціями, державами.. Вищезазначене обумовлює актуальність обраної теми дослідження.

#### **Аналіз останніх досліджень і публікацій.**

Багато дослідників, зокрема, І. Сердюк, Г. Ситник, І. Семенець-Орлова та ін., вважають, що недооцінка питань інформаційної безпеки може призвести до непередбачуваних соціальних, політичних, економічних, екологічних та інших наслідків. У цих умовах набуває першорядного значення у всіх сферах суспільного життя та державної діяльності інформаційна безпека. А на рівні світової спільноти інформаційна безпека стає глобальною проблемою. Проте недостатньо уваги приділяється глобальному характеру

проблеми забезпечення інформаційної безпеки держави в умовах гібридних загроз.

**Формулювання цілей статті (постановка завдання).** Метою роботи є дослідження специфіки забезпечення інформаційної безпеки держави в умовах гібридних загроз як глобальна проблема.

Для досягнення поставленої мети в роботі пропонується поставити та вирішити такі завдання:

- визначити риси інформаційної безпеки як глобальної проблеми;
- виокремити напрямки формування глобальної інформаційної безпеки;
- окреслити ліквідацію «цифрової нерівності» як одне із ключових завдань забезпечення глобальної інформаційної безпеки.

### **Виклад основного матеріалу дослідження.**

Планетарний інформаційний простір забезпечує ефективну інформаційну взаємодію між людьми, їх доступ до національних та світових інформаційних ресурсів, задоволення їхніх інформаційних потреб. Вперше з'явилася реальна можливість планетарного інформаційного об'єднання людства. Але ця можливість таїть у собі і численні небезпеки, оскільки багато найважливіших інтересів людини, суспільства, держави та світової спільноти вже нині зосереджені у планетарному інформаційному просторі. Тому такі поняття як інформаційна війна, інформаційний тероризм та інформаційна зброя опинилися у центрі уваги розвинених країн.

Як глобальна проблема інформаційна безпека має такі риси:

- характерна для більшості (а в перспективі – для всіх) країн світу;
- виступає об'єктивним фактором та одним з найважливіших механізмів подальшого світового розвитку у його новій цивілізаційній формі;
- у зв'язку з становленням планетарного інформаційного суспільства як початкової фази ноосфери інформаційна безпека висувається на перший план;
- недостатнє забезпечення інформаційної безпеки призводить до загроз інформаційної війни, інформаційного тероризму тощо;

- для ефективного забезпечення інформаційної безпеки необхідні спільні зусилля усієї світової спільноти [1; 5].

Оскільки за наявності єдиного планетарного інформаційного простору інформаційна безпека не може бути забезпечена повною мірою зусиллями однієї країни або групи країн, то виникає необхідність формування системи забезпечення глобальної інформаційної безпеки як складової всієї системи загальносвітової безпеки – одного з основних компонентів переходу до сталого розвитку людської цивілізації.

У цьому зв'язку важливо виділити такі напрямки формування глобальної інформаційної безпеки:

- захист єдиного світового інформаційного простору від різних небезпек та загроз;

- рівноправне використання планетарного інформаційного простору всіма народами та країнами світової спільноти;

- безпечний для людини, суспільства, держав, світової спільноти та біосфери розвиток цього інформаційного простору;

- позитивний вплив глобальної інформаційної безпеки, що формується, на перехід до сталого соціоекорозвитку [2; 4].

Єдиний планетарний інформаційний простір не знає державних кордонів і тому удар по ньому може завдати шкоди одночасно у різних країнах світу. Тому необхідно забезпечувати інформаційну безпеку у глобальному масштабі зусиллями всіх країн через узгодження національних законів, покликаних захистити інформаційний простір від електронних вторгнень, багатосторонню співпрацю у справах про комп'ютерні злочини, що перетинають національні кордони, укладання міжнародних договорів про видачу осіб, які вчиняють комп'ютерні злочини, а також готовність до введення санкцій проти тих, хто захищатиметься.

Хоча формування єдиного планетарного інформаційного простору тільки почалося (причому воно вже почалося в моделі нестійкого розвитку), у ньому вже зараз відбувається протистояння між провідними країнами світу.

Інформаційне протиборство виступає як використання державами глобального інформаційного простору та інформаційної інфраструктури для проведення різних стратегічних операцій, що ведуть до отримання переваг у всіх сферах суспільного життя та зменшення впливу на власну інформаційну сферу. Фактично це означає збереження необхідного рівня своєї інформаційної безпеки та зниження рівня цієї безпеки з іншого боку. Розвиток та вдосконалення форм інформаційного протиборства може призвести до повної відмови від використання збройних сил (у їхньому матеріально-енергетичному вираженні), оскільки добре скоординовані інформаційні операції просто не дозволяють застосувати традиційні збройні сили [3; 6].

Розвиток інформатизації має відбуватися таким чином, щоб протягом ХХІ століття досягнення в галузі інформаційних технологій працювали дедалі більше на благо людства. В іншому випадку людство ризикує стати на поріг чергового витка гонки тепер уже інформаційних озброєнь. В цьому випадку небезпека розв'язання глобальної інформаційної війни, об'єктом впливу в якій стане найтонше досягнення еволюції природи – свідомість людини, може стати реальністю.

Формування планетарного інформаційного простору потребує уніфікації інформаційних та телекомунікаційних технологій усіх країн – суб'єктів інформаційної спільноти. Це дає можливість потужним індустріальним державам посилити свою політичну, економічну та військову перевагу за рахунок лідерства в інформатизації та здійснювати глобальний інформаційний контроль над світовою спільнотою. Небезпека для країн, які мають низький рівень розвитку інфосфери, полягає в тому, що ліквідувати розрив стає практично неможливо. Це дає можливість впливу на економіку та політичний устрій такої країни через відключення цієї країни від планетарного інформаційного простору, що набагато дешевше та простіше, ніж ведення воєнних дій. Зрозуміло, що перспектива такої залежності та можливість втрати самостійності викликають занепокоєння інших держав, громадських інститутів та громадян. Цілком імовірно, що на цьому ґрунті можуть виникати

політичні та економічні конфронтації держав, а також принципово нові кризи в міжнародних відносинах [1; 2].

Тому одним із завдань глобальної інформаційної безпеки є ліквідація «цифрової нерівності». Важливо забезпечити доступ усіх країн світової спільноти, а не лише країн-лідерів економічного розвитку, до глобального інформаційного простору, що дозволить їм отримувати повну, достовірну та своєчасну інформацію та інформаційні ресурси, необхідні для їхнього переходу до сталого розвитку. Це дозволить забезпечити максимально можливу орієнтацію суб'єкта у всьому інформаційному просторі. Коли суб'єкт з яких-небудь причин не може скористатися інформацією, що циркулює в інформаційному просторі, яка необхідна для прийняття відповідних управлінських та інших рішень, тоді виникає небезпека інформаційної загрози. Недостатність поінформованості може призвести до ухвалення неадекватних політичних, економічних, військових та інших рішень. Розвиток світових інформаційних ресурсів дозволив підвищити обґрунтованість та оперативність прийнятих рішень у промисловості, торгівлі, державних установах та ін. за рахунок своєчасного використання необхідної інформації, що циркулює у планетарному інформаційному просторі [4; 7].

#### **Висновки та перспективи подальших розвідок у даному напрямі.**

Таким чином, необхідною складовою глобальної інформаційної безпеки є невід'ємне право всіх країн світу та всього населення на вільний доступ до інформації та телекомунікацій. Ситуація повного контролю над планетарним інформаційним простором однієї країни чи групи країн може призвести до інформаційного тоталітаризму вже у глобальному масштабі, а не лише в рамках однієї країни, що ускладнить або взагалі виключить можливість реалізації нової цивілізаційної парадигми.

У цьому контексті важливо відзначити, що при виробленні стратегії глобальної інформаційної безпеки не можуть враховуватися лише національні інтереси, пріоритетними стають загальнолюдські цінності та інтереси людства. Національні інтереси, як і раніше, відіграватимуть важливу роль, але

вони мають бути визначені більше в загальнолюдському, а не в державному масштабі та мають бути поєднаними з ширшими інтересами всього людства в єдину систему. Тому однією з проблем забезпечення глобальної інформаційної безпеки є досягнення балансу інтересів усіх суб'єктів цього виду безпеки (особистості, суспільства, держави та світової спільноти).

## Література

1. Савосько Т. Особливості формування державної інформаційної політики. *Аспекти публічного управління*. 2024. № 12(1). С. 22–28.
2. Семенець-Орлова І., Клочко А., Амро Т. Публічне управління у сфері інформаційної безпеки для забезпечення розвитку демократії в Україні (контекст воєнного стану). *Публічне урядування*. 2024. № 5(33). С. 73–82.
3. Сердюк І. А. Підходи публічного управління до інформаційної безпеки особистості. *Публічне урядування*. 2022. № 3(31). С. 53–59.
4. 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. URL: [http://nbuv.gov.ua/UJRN/Duur\\_2024\\_5\\_6](http://nbuv.gov.ua/UJRN/Duur_2024_5_6).
5. Сілаєв В., Горінов П. Політика інформаційної безпеки в умовах цифрової трансформації України: виклики та шляхи попередження. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2024. № 3(75). С. 81–87.
6. Торічний В. О. Формування та впровадження державної інформаційної політики як запорука забезпечення державної безпеки. *Вісник Національного університету цивільного захисту України. Серія «Державне управління»*. 2019. Вип. 1 (10). С. 64–69.
7. Хромов А. Оптимізація системи центральних державних архівів України в умовах війни. *Архіви України*. 2022. Вип. 1 (330). С. 103–114.

## References

1. Khromov, A. (2022), “Optimization of the system of central state archives of Ukraine in the conditions of war”, *Arkhivi Ukraini*, vol. 1(330), pp. 103–114.
2. Savosko, T. (2024), “Features of the formation of state information policy”, *Aspekty publichnoho upravlinnia*, vol. 12(1), pp. 22–28.
3. Semenets-Orlova, I., Klochko, A. and Amro, T. (2024), “Public administration in the field of information security to ensure the development of democracy in Ukraine (the context of martial law)”, *Publichne uriaduvannia*, vol. 5(33), pp. 73–82.
4. Serdiuk, I. A. (2022), “Public administration approaches to information security of the individual”, *Publichne uriaduvannia*, vol. 3(31), pp. 53–59.
5. Silaiev, V. and Horinov, P. (2024), “Information security policy in the context of digital transformation of Ukraine: challenges and ways of prevention”, *Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Politychni nauky ta publichne upravlinnia*, vol. 3(75), pp. 81–87.
6. Sytnyk, H. P., Klymenko, N. H. and Horielikov, I. O. (2024), “State policy of ensuring of information security and cybersecurity as its component: problems and ways to solve”, *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, vol. 5, available at: [http://nbuv.gov.ua/UJRN/Duur\\_2024\\_5\\_6](http://nbuv.gov.ua/UJRN/Duur_2024_5_6) (Accessed 10 Oct 2025).
7. Torichny, V.A. (2019), “Formation and implementation of state information policy as a guarantee of state security”, *Visnik Natsionalnogo universitetu tsyvilnogo zakhistu Ukraini. Seriya «Derzhavne upravlinnya»*, vol. 1(10), pp. 64–69.

*Стаття надійшла до редакції 22.10.2025 р.*