УДК 004.056:351.86
JEL Classification: D83; H56; O33
DOI: https://doi.org/10.32983/2222-4459-2025-2-163-170

ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ІНСТРУМЕНТУ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

© 2025 **ГАПЄЄВА О. М., РОМАШКО С. М.**

УДК 004.056:351.86
JEL Classification: D83; H56; O33

Гапєєва О. М., Ромашко С. М. Теоретичні засади формування інформаційної безпеки як інструменту забезпечення національної безпеки

У статті висвітлено основні теоретичні аспекти формування інформаційної безпеки, яка є невід'ємною складовою забезпечення національної безпеки держави. Встановлено, що сучасні технологічні та інформаційні зміни в суспільстві створюють гостру потребу у створенні ефективних механізмів захисту інформаційних ресурсів, які здатні забезпечити стабільність функціонування державних установ. Досліджено ключові загрози, пов'язані з інформаційною безпекою, такі як концентрація інформаційного впливу в руках окремих суб'єктів, розповсюдження недостовірної інформації, незаконний доступ до конфіденційних даних, а також порушення роботи важливих інформаційних систем. Проаналізовано існуючі підходи до забезпечення інформаційної безпеки, які спираються на комплексний підхід, що системно охоплює ідентифікацію основних загроз, оцінку рівня ризиків, розробку стратегій протидії та створення багаторівневих моніторингових систем для виявлення й усунення потенційних загроз. Обґрунтовано необхідність удосконалення правової бази з урахуванням сучасних викликів інформаційного простору, наголошуючи на її адаптації до міжнародних стандартів. Важливо забезпечити баланс між свободою інформаційного обміну та захистом національних інтересів. Особливу увагу приділено регулюванню питань, пов'язаних із захистом конфіденційної інформації, та забезпеченням прозорості у сфері інформаційної діяльності. Розроблено організаційні та методичні основи для створення єдиної державної системи інформаційної безпеки, яка враховує багатовимірний характер сучасного інформаційного простору та складність можливих загроз. Запропоновано використання міжнародного досвіду як основи для створення ефективної системи управління інформаційною безпекою на національному рівні. На основі проведеного дослідження сформульовано рекомендації щодо розробки національної стратегії інформаційної безпеки, яка інтегрує технологічні, правові та організаційні аспекти. Запропоновані підходи спрямовані на підвищення стійкості держави до сучасних інформаційних викликів та зміцнення її позицій у глобальному інформаційному середовищі.

Ключові слова: *інформаційна безпека, національна безпека, захист інформації, інформаційні загрози, нормативно-правове регулювання, інноваційні технології.*

Рис.: *3.* ***Табл.:*** *1.* ***Бібл.:*** *17.*

Гапєєва Ольга Миколаївна *– доктор економічних наук, професор, професор кафедри економіки та економічної безпеки, Університет митної справи та фінансів (вул. Володимира Вернадського, 2/4, Дніпро, 49000, Україна)*
E-mail: *golga@ukr.net*
ORCID: *https://orcid.org/0000-0001-6320-2775*
Researcher ID: *AAI-6884-2020*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57211506062*

Ромашко Сергій Миколайович *– аспірант кафедри економіки та економічної безпеки, Університет митної справи та фінансів (вул. Володимира Вернадського, 2/4, Дніпро, 49000, Україна)*
E-mail: *romahasergey@gmail.com*
ORCID: *https://orcid.org/0009-0000-6849-3786*

UDC 004.056:351.86
JEL Classification: D83; H56; O33

Hapieieva O. M., Romashko S. M. The Theoretical Foundations for the Formation of Information Security as a Tool for Ensuring National Security

The article highlights the main theoretical aspects of formation of information security, which is an integral component of the national security of the State. It is determined that modern technological and informational changes in society create an urgent need for the development of effective mechanisms to protect informational resources that can ensure the stability of the functioning of governmental institutions. Key threats associated with information security are examined, such as the concentration of informational influence in the hands of certain entities, the dissemination of unreliable information, unauthorized access to confidential data, and disruptions to the operation of critical information systems. An analysis has been conducted on existing approaches to ensuring information security, which rely on a comprehensive approach that systematically covers the identification of key threats, risk assessment, development of counter-strategies, and the establishment of multi-level monitoring systems for the detection and elimination of potential threats. The necessity of enhancing the legal framework in light of contemporary challenges in the information space has been substantiated, emphasizing its adaptation to international standards. It is important to ensure a balance between the freedom of information exchange and the protection of national interests. Special attention has been paid to the regulation of issues related to the protection of confidential information and ensuring transparency in the field of information activities. Organizational and methodological foundations have been developed for the creation of a unified State system of information security, taking into account the multidimensional nature of the modern information space and the complexity of potential threats. The use of international experience is proposed as a basis for establishing an effective national information security management system. Based on the conducted research, recommendations have been formulated for the development of a national information security strategy that integrates technological, legal, and organizational aspects. The proposed approaches aim to enhance the State's resilience to contemporary information challenges and strengthen its position in the global information environment.

Keywords: *information security, national security, information protection, information threats, regulatory framework, innovative technologies.*

Fig.: *3.* ***Tabl.:*** *1.* ***Bibl.:*** *17.*

Hapieieva Olha M. *– Doctor of Sciences (Economics), Professor, Professor of the Department of Economics and Economic Security, University of Customs and Finance (2/4 Volodymyr Vernadsky Str., Dnipro, 49000, Ukraine)*
E-mail: *golga@ukr.net*
ORCID: *https://orcid.org/0000-0001-6320-2775*
Researcher ID: *AAI-6884-2020*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57211506062*

Romashko Serhii M. *– Postgraduate Student of the Department of Economics and Economic Security, University of Customs and Finance (2/4 Volodymyr Vernadsky Str., Dnipro, 49000, Ukraine)*
E-mail: *romahasergey@gmail.com*
ORCID: *https://orcid.org/0009-0000-6849-3786*

Поточні умови функціонування національної економіки, коли глобалізація, цифровізація економіки та розвиток інформаційного суспільства стрімко змінюють усі сфери життя, формують питання забезпечення інформаційної безпеки, набуває надзвичайно важливого значення, оскільки вона є фундаментальним компонентом національної безпеки, що покликаний забезпечити надійний захист критично важливих інформаційних ресурсів, попереджати кібератаки, а також сприяти підтримці стабільності у сфері державного управління, економіки та соціального життя. Для України, яка стикається з тривалими гібридними загрозами, серед яких кібератаки, інформаційні війни та маніпулятивний вплив з боку як зовнішніх, так і внутрішніх суб'єктів, формування ефективної системи інформаційної безпеки набуває особливої актуальності, адже такі загрози створюють не лише технологічні виклики, але й значною мірою впливають на соціально-політичну стабільність, формуючи додаткові ризики для збереження державної цілісності.

Отже, проведення дослідження, спрямованого на поглиблене вивчення теоретичних засад формування інформаційної безпеки, є вкрай необхідним, адже це дозволить визначити новітні підходи до протидії сучасним загрозам, розробити ефективну державну політику в цій сфері та забезпечити стійкий і стабільний розвиток суспільства в умовах інформаційних викликів.

У роботі Шевчук М. [13] досліджуються способи вдосконалення правової бази для протидії гібридним загрозам, зокрема адаптація законодавства до міжнародних стандартів. Своєю чергою, Захаров М. [5] акцентує увагу на адміністративно-правових механізмах, які балансують між свободою інформації та її обмеженням для захисту державних інтересів. Дослідники Македон В., Маковецька А. [9] розглядають технології, такі як криптографія, штучний інтелект і моніторинг, для збереження цілісності інформаційних ресурсів. Інші вітчизняні вчені, Войціховський А. [3] і Чмир Я. [12], аналізують вплив деструктивної інформації, яка може викликати маніпуляції, дезінформацію та погіршення суспільного настрою. Міжнародний досвід, зокрема стандарти підтримки і класифікації рівнів інформаційної безпеки країни, розглядали Ментух Н. Ф., Шевчук О. Р., Вербіцька М. В., Кузь Т. В. [15], що сприяє розробці ефективних стратегій інформаційної безпеки. Загалом, питання інформаційної безпеки потребує комплексного підходу для подолання правових, технологічних і соціальних викликів.

Метою статті є обґрунтування теоретичних основ інформаційної безпеки для забезпечення національної безпеки держави через аналіз загроз, оцінку ризиків та розробку ефективних підходів до захисту інформаційних ресурсів у координатах національної безпеки.

Розвиток суспільства характеризується стрімкими змінами в технологічному та інформаційному середовищі, що призводить до радикальних трансформацій у сфері забезпечення національної безпеки. Інформація, яка стає ключовим ресурсом, здатним формувати соціальні, політичні та економічні процеси, вимагає створення дієвих механізмів її захисту від загроз, які мають багатофакторну природу та охоплюють фізичні, технічні, організаційні та психологічні аспекти. Саме тому інформаційна безпека розглядається як невід'ємна складова національної безпеки, яка покликана забезпечити стійкість державних інститутів, захист інтересів громадян і стабільність суспільства в умовах постійного впливу як національних, так і глобальних викликів (*табл. 1*).

З теоретичної точки зору, формування інформаційної безпеки має базуватися на комплексному підході, що включає визначення ключових понять, ідентифікацію загроз, оцінку ризиків, а також розробку стратегій і механізмів, спрямованих на їх нейтралізацію. Основою цього

Таблиця 1

Теоретичне моделювання станів порушення інформаційної безпеки держави

Градації станів порушення і впливів на інформаційну безпеку держави				
Зовнішньої політики	**Соціуму**	**Екології**	**Економіки**	**Технологій**
Взаємовигідне співробітництво	Процвітання за рівнем життя	Гармонізація відносин людини та природи	Монополія	Абсолютна перевага в розвитку
Мирне співіснування	Стабільність суспільства	Антропогенний вплив на природу	Лідерство	Лідерство в розвитку науки та технологій
Нейтралітет	Невизначеність	Невизначеність	Невизначеність	Невизначеність
Холодні війни	Соціальна напруженість	Перевищення норм екологічної безпеки	Передкризовий стан	Відставання в розвитку технологій
Озброєні конфлікти	Соціальний вибух	Природні катаклізми	Банкрутство, криза, крах	Нерозвиненість

Примітка: Таблиця складена на основі систематизації імен можливих станів в аналізованих предметних областях (PEST- і SEET-аналіз), які склалися в теорії та практиці досліджень. PEST – політика, економіка, соціум, технології; SEET – соціум, екологія, економіка, технології.

Джерело: складено авторами на основі [1; 13].

процесу є системний підхід, який дозволяє враховувати взаємозв'язок між технологічними, соціальними та економічними факторами. Інформаційна безпека, як категорія, охоплює захист конфіденційності, цілісності та доступності інформації, а також протидію зовнішнім та внутрішнім загрозам, які можуть бути спричинені як технічними збоями, так і навмисними діями злочинців чи інших суб'єктів впливу [2, с. 223].

Формування ефективної системи інформаційної безпеки, як одного з ключових інструментів забезпечення національної безпеки держави, потребує врахування багатовимірності сучасного інформаційного середовища та складності загроз, які виникають у цьому просторі. Центральним аспектом у цій системі є побудова моделей, які дозволяють структурувати й оцінювати ризики, зокрема за допомогою концепції ймовірнісного аналізу, що поділяє потенційні результати на втрати або вигоди залежно від коректності прийнятих рішень. У таких моделях особливі точки, як-от межі ймовірності чи перегини, служать орієнтирами для створення деталізованих градацій загроз і визначення рівнів захисту, що є основою для нормування інформаційної стійкості [7, с. 94].

Інформаційна безпека займає особливе місце в архітектурі національної безпеки, адже забезпечує не лише захист державних інституцій, але й стабільність суспільства та безпеку кожного громадянина. В умовах інформаційної агресії з боку недружніх держав, яка включає пропаганду, дезінформацію та кібератаки, необхідно створити систему, що дозволяє швидко й ефективно реагувати на подібні виклики. Особливо важливим у цьому контексті є посилення захисту критичної інфраструктури та розробка механізмів протидії деструктивним впливам на інформаційне середовище [10, с. 183].

Цифрова трансформація, яка охоплює всі сфери життя, значно впливає на те, як ми розуміємо роль держави, права та людини в умовах нової цифрової реальності. Інтеграція сучасних технологій, таких як штучний інтелект, блокчейн або багаторівневі системи захисту, стає невід'ємною частиною формування інформаційної безпеки. Вказані технології формують можливість не лише вдосконалювати технічну складову захисту, але й підвищувати організаційний рівень управління ризиками, що виникають у цифровому середовищі.

Загрози інформаційній безпеці, які вийшли на перший план у XXI столітті, вимагають від держав розробки чітких стратегій і нормативно-правових механізмів. Серед них ключову роль відіграє міжнародне співробітництво, яке спрямоване на запобігання використанню інформаційно-комунікаційних технологій для деструктивних цілей, таких як підрив економічної стабільності чи поширення екстремістських ідей. У цьому контексті важливо також впроваджувати національні ініціативи, що спрямовані на посилення кібербезпеки [14].

Включення інформаційної безпеки до стратегічних національних пріоритетів України стало закономірним кроком у відповідь на зростання кількості

загроз і викликів, які постають перед державою. Зосередження уваги на посиленні правового регулювання, розвитку наукових досліджень і впровадженні інноваційних рішень дозволяє Україні не лише протидіяти сучасним викликам, але й зайняти гідне місце у глобальному інформаційному просторі, забезпечуючи довгострокову стійкість і безпеку своїх громадян (*рис. 1*).

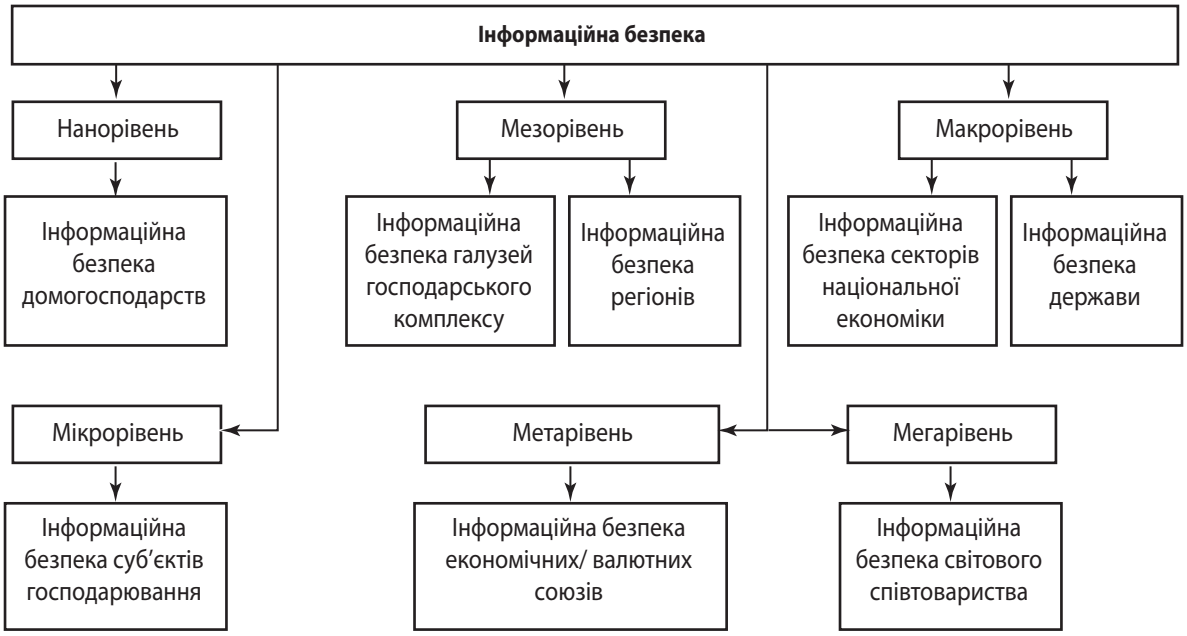

Рис. 1. Інформаційна безпека та діалектичні зв'язки на різних управлінських рівнях економіки

Джерело: розроблено авторами.

Сучасне уявлення про інформаційну безпеку як складову національної безпеки держави формується на основі розуміння важливості захисту життєво важливих інтересів особистості, суспільства та держави в інформаційному просторі. Це поняття, яке тісно пов'язане із соціально-психологічними ідеалами безпеки, відображає прагнення створити умови для надійного функціонування інформаційних систем і захисту громадян від негативних інформаційних впливів [6, с. 160]. Для глибшого розуміння сутності інформаційної безпеки важливо зосередити увагу на ключових національних інтересах в інформаційній сфері, які включають забезпечення права громадян на доступ до інформації, гарантії свободи слова, захист приватності, а також розвиток інформаційної інфраструктури, яка сприяє соціально-економічному прогресу.

Крім того, значну увагу слід приділити формуванню механізмів правового регулювання, що стосуються конфіденційної інформації, державних таємниць і захисту інтелектуальної власності. Серед основних загроз для інформаційної безпеки можна виділити монополізацію інформаційного простору, дезінформацію, маніпуляцію масовою свідомістю, порушення роботи технічних систем, а також перехоплення конфіденційної інформації [8, с. 201–202] (*рис. 2*).

Основними джерелами загроз в інформаційному просторі можуть бути як іноземні держави, міжнародні терористичні організації, так і внутрішні суб'єкти, зокрема засоби масової інформації, що створюють деструктивний вплив на суспільство. До таких джерел також належать технічні системи, які можуть стати об'єктами зловмисних атак, і національні або наднаціональні інформаційно-комунікаційні платформи, які можуть використовуватися для маніпулювання громадською думкою.

Деструктивні інформаційні фактори здатні суттєво впливати на рівень обізнаності суб'єктів державного управління, викривлюючи їхнє сприйняття реальності, що, своєю чергою, призводить до формування спотворених уявлень у населення про явища та процеси сучасності. Такий вплив негативно позначається на поведінці людей, їхньому розвитку, вихованні, психологічному стані та навіть здоров'ї, що ставить під загрозу основи існування особистості у суспільстві [4]. Поширення антигуманних ідей, зниження культурного рівня населення та інші деструктивні явища є прямим наслідком руйнівного впливу на інформаційне поле суспільної свідомості.

У матеріальній сфері інформаційні загрози проявляються через сприяння таким негативним явищам, як корупція, монополізація, шантаж чи

Рис. 2. Напрями додержання та моніторингу інформаційної безпеки держави

Джерело: розроблено авторами.

інші форми незаконної діяльності. Подібні фактори можуть бути використані для інспірації внутрішніх конфліктів, зокрема страйків, національної ворожнечі чи навіть громадянської війни. Такий вплив інформаційних загроз вимагає ретельного аналізу, оскільки неадекватне сприйняття реальності суб'єктами прийняття рішень може мати значні негативні наслідки для держави [17, p. 45].

Ефективна протидія цим викликам можлива лише через створення єдиної державної системи забезпечення інформаційної безпеки. Такого плану система має об'єднувати державні органи, відповідальні за інформаційну безпеку, сили та засоби, які функціонують на основі чинного законодавства та перебувають під контролем судової влади. Основними напрямами діяльності цієї системи є виявлення та прогнозування інформаційних загроз, розробка та реалізація довгострокових стратегій для їх попередження, а також створення та підтримка необхідних ресурсів для забезпечення інформаційної безпеки.

Заходи захисту, які застосовуються державою для нейтралізації інформаційних загроз, включають широкий спектр методів, спрямованих на зменшення рівня небезпеки. Вони можуть бути економічними, військовими, політичними, інформаційними або інтелектуальними, і спрямовані на захист як інтересів держави, так і громадян. Водночас громадяни мають обмежений доступ до засобів захисту, що підкреслює необхідність ефективної діяльності державних органів у цій сфері (*рис. 3*) [16].

Основними завданнями держави у сфері забезпечення інформаційної безпеки є формування та реалізація державної політики, яка спрямована на захист національних інтересів у інформаційному середовищі. Це включає вдосконалення законодавчої бази, координацію діяльності державних структур, створення балансу між вільним обміном інформацією та її обмеженням, а також розвиток інформаційної інфраструктури. Особливу увагу слід приділити впровадженню новітніх інформаційних технологій, уніфікації засобів роботи з інформацією та інтеграції України до глобальної інформаційної інфраструктури [11, с. 125].

Підсумовуючи, важливо підкреслити, що теоретичні основи формування інформаційної безпеки повинні базуватися на багатоаспектному міждисциплінарному підході, який інтегрує технологічні, правові, соціальні та організаційні аспекти в єдину систему. Лише цілісна стратегія, що враховує як національні, так і глобальні тенденції інформаційного простору, здатна забезпечити ефективний захист інформаційних

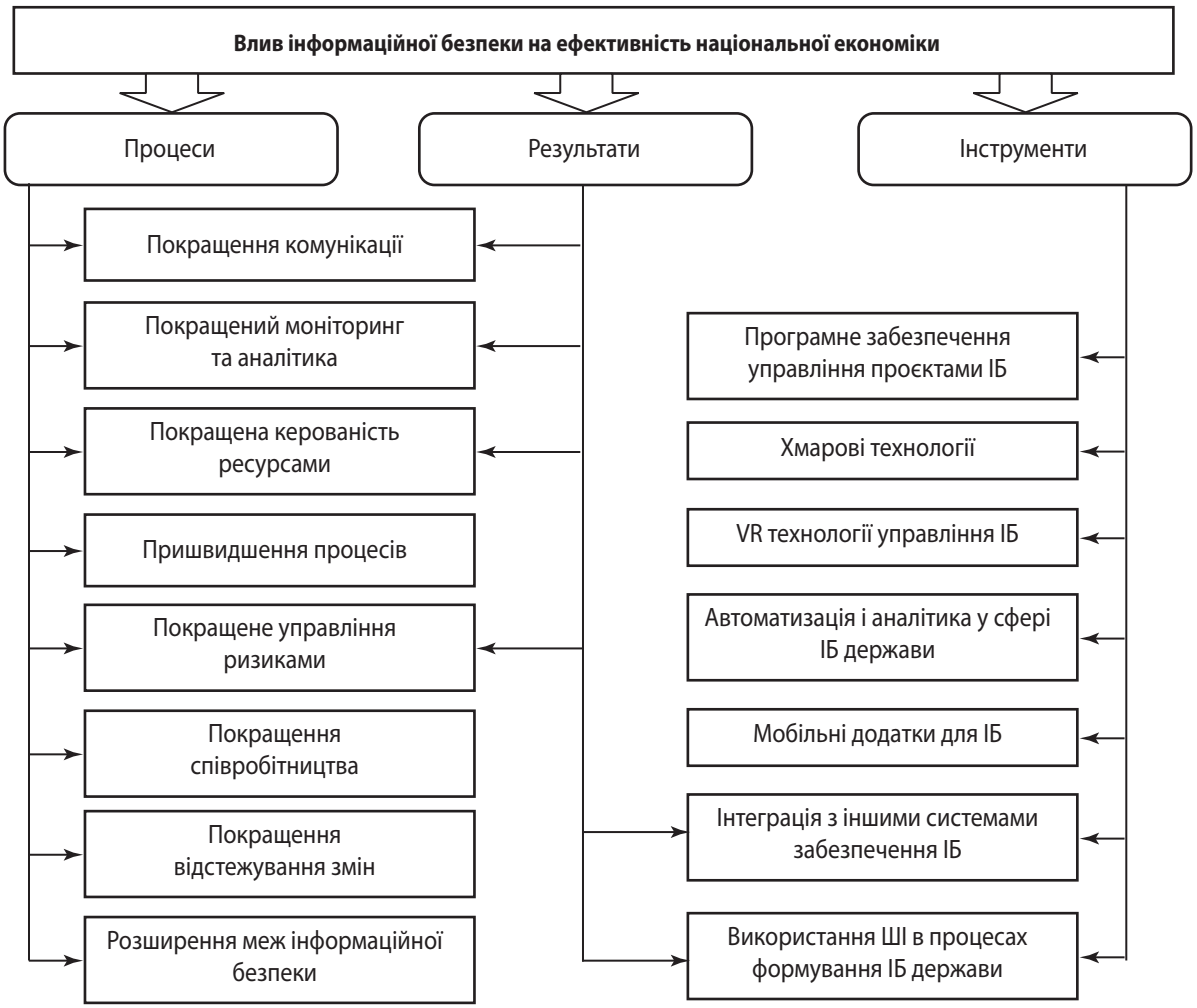

Рис. 3. Організаційна модель забезпечення національної інформаційної безпеки

Джерело: розроблено авторами.

ресурсів і зміцнити стійкість держави перед сучасними викликами. У цьому контексті ключову роль відіграє подальший розвиток наукових досліджень, модернізація нормативно-правового регулювання та впровадження передових технологій, що дозволить Україні закріпити свої позиції у світовому інформаційному просторі та забезпечити національну безпеку.

ВИСНОВКИ

Встановлено, що деструктивні інформаційні чинники мають значний вплив на стабільність суспільства та функціонування держави, спричиняючи викривлення у сприйнятті реальності, маніпулювання масовою свідомістю та поширення антигуманних ідей, що в результаті негативно позначається на культурному рівні населення, соціальній стабільності та загальній безпеці.

З'ясовано основні сучасні загрози інформаційній безпеці, серед яких найважливішими є: монополізація інформаційного простору, злочинне використання інформаційно-комунікаційних технологій, дезінформація, незаконний доступ до конфіденційних даних, а також порушення функціонування компонентів національної критичної інфраструктури.

Розглянуто наявні моделі побудови систем інформаційної безпеки, які базуються на комплексному підході. Вони включають ідентифікацію основних загроз, оцінювання ризиків, розробку стратегій захисту та впровадження багаторівневих систем для моніторингу та оперативного реагування на загрози.

Розроблено організаційно-методичні підходи до створення інтегрованої державної системи інформаційної безпеки, яка передбачає тісну взаємодію між державними органами, використання правових інструментів та застосування сучасних технологічних рішень для забезпечення комплексного захисту. ■

БІБЛІОГРАФІЯ

1. Босак І. М., Данилович-Кропивницька М. Л. Аналіз світового досвіду формування системи інформаційної безпеки в контексті публічного управління. *Науковий вісник Міжнародного гуманітарного університету*. 2024. № 58. С. 72–78. DOI: https://doi.org/10.32782/2413-2675/2024-58-9
2. Вітер Д. В., Руденко О. О. Сучасна парадигма протидії загрозам національній безпеці: питання стратегічного управління. *Право та державне управління*. 2022. № 3. С. 220–226. DOI: https://doi.org/10.32840/pdu.2022.3.33
3. Войціховський А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право»*. 2020. Вип. 29. С. 281–288. DOI: https://doi.org/10.26565/2075-1834-2020-29-38
4. Дикий А. П., Дика О. С., Наумчук К. М., Тростенюк Т. М. Понятійно-категоріальний апарат інформаційної безпеки України в забезпеченні національної безпеки. *Таврійський науковий вісник. Серія «Публічне управління та адміністрування»*. 2022. № 4. С. 23–31. DOI: https://doi.org/10.32851/tnv-pub.2022.4.3
5. Захаров М. В. Концептуалізація підходів до забезпечення інформаційної безпеки держави в умовах війни. *Вчені записки ТНУ імені В. І. Вернадського. Серія «Публічне управління та адміністрування»*. 2024. Т. 34. № 1. С. 252–253. DOI: https://doi.org/10.32782/TNU-2663-6468/2024.1/44
6. Кучменко В. О., Єнічев М. І. Місце інформаційної безпеки як важливої складової національної безпеки. *Вчені записки ТНУ імені В. І. Вернадського. Серія «Публічне управління та адміністрування»*. 2024. № 4. С. 159–160. DOI: https://doi.org/10.32782/TNU-2663-6468/2024.4/24
7. Мазепа С. Забезпечення інформаційної безпеки в Україні: перспективи адміністративно-правового регулювання. *Актуальні проблеми правознавства*. 2024. № 1. С. 92–97. DOI: https://doi.org/10.35774/app2024.01.092
8. Македон В. В. Дослідження процесів забезпечення соціальної відповідальності у провідних моделях корпоративного управління. *Вісник Харківського національного технічного університету сільського господарства. Серія «Економічні науки»*. 2012. Вип. 126. С. 198–206.
9. Македон В. В., Маковецька А. О. Інформаційне забезпечення економічної безпеки підприємств в умовах ринкової нестабільності. *Інтернаука. Серія «Економічні науки»*. 2023. № 12. DOI: https://doi.org/10.25313/2520-2294-2023-12-9477
10. Милосердна І. М. Інформаційна безпека як елемент національної безпеки: теоретичний вимір та особливості впровадження. *Політикус*. 2024. Вип. 4. С. 179–185. DOI: https://doi.org/10.24195/2414-9616.2024-4.26
11. Смотрич Д., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2023. Вип. 77. Ч. 2. С. 121–127. DOI: https://doi.org/10.24144/2307-3322.2023.77.2.20
12. Чмир Я. Сучасні проблеми інформаційної безпеки України та перспективні напрями їх вирішення. *Наукові праці Міжрегіональної Академії управління персоналом. Серія «Політичні науки та публічне управління»*. 2022. Вип. 2. С. 149–154. DOI: https://doi.org/10.32689/2523-4625-2022-2(62)-23
13. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2023. Вип. 78. Ч. 2. С. 134–139. DOI: https://doi.org/10.24144/2307-3322.2023.78.2.21
14. Makedon V., Korneyev M. Improving methodology of estimating value of financial sector entities dealing in mergers and acquisitions. *Investment Management and Financial Innovations*. 2014. Vol. 11. No 1. P. 44–55. URL: https://www.researchgate.net/publication/289853616_Improving_methodology_of_estimating_value_of_financial_sector_entities_dealing_in_mergers_and_acquisitions
15. Mentukh N. F., Shevchuk O. R., Verbitska M. V., Kuz T. V. Ensuring Information Security: Comparative Legal Aspect. *Central European Management Journal*. 2023. Vol. 31. No. 3. P. 74–87. URL: https://journals.kozminski.cem-j.org/index.php/pl_cemj/article/view/917
16. Shelukhin M., Kupriichuk V., Kyrylko N., Makedon V., Chupryna N. Entrepreneurship Education with the Use of a Cloud-Oriented Educational Environment. *International Journal of Entrepreneurship*. 2021. Vol. 25. Iss. 6. URL: https://www.abacademies.org/articles/entrepreneurship-education-with-the-use-of-a-cloudoriented-educational-environment-11980.html
17. Taherdoost H. Cybersecurity vs. Information Security. *Procedia Computer Science*. 2022. Vol. 215. P. 483–487. DOI: https://doi.org/10.1016/j.procs.2022.12.050

REFERENCES

Bosak, I. M., and Danylovych-Kropyvnytska, M. L. "Analiz svitovoho dosvidu formuvannia systemy informatsiinoi bezpeky v konteksti publichnoho upravlinnia" [Analysis of the World Experience of Forming an Information Security System in the Context of Public Administration]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu*, no. 58 (2024): 72-78. DOI: https://doi.org/10.32782/2413-2675/2024-58-9

Chmyr, Ya. "Suchasni problemy informatsiinoi bezpeky Ukrainy ta perspektyvni napriamy yikh vyrishennia" [Current Problems of Information Security in Ukraine and Prospective Directions for Their Solution]. *Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Seriia «Politychni nauky ta publichne upravlinnia»*, no. 2 (2022): 149-154.
DOI: https://doi.org/10.32689/2523-4625-2022-2(62)-23

Dykyi, A. P. et al. "Poniatiino-katehorialnyi aparat informatsiinoi bezpeky Ukrainy v zabezpechenni natsionalnoi bezpeky" [Conceptual and Categorical Apparatus of Information Security of Ukraine in Ensuring National Security]. *Tavriiskyi naukovyi visnyk. Seriia «Publichne upravlinnia ta administruvannia»*, no. 4 (2022): 23-31.
DOI: https://doi.org/10.32851/tnv-pub.2022.4.3

Kuchmenko, V. O., and Yenichev, M. I. "Mistse informatsiinoi bezpeky yak vazhlyvoi skladovoi natsionalnoi bezpeky" [The Place of Information Security as an Important Component of National Security]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia «Publichne upravlinnia ta administruvannia»*, no. 4 (2024): 159-160.
DOI: https://doi.org/10.32782/TNU-2663-6468/2024.4/24

Makedon, V. V. "Doslidzhennia protsesiv zabezpechennia sotsialnoi vidpovidalnosti u providnykh modeliakh korporatyvnoho upravlinnia" [Research Into the Processes of Ensuring Social Responsibility in Leading Corporate Governance Models]. *Visnyk Kharkivskoho natsionalnoho tekhnichnoho universytetu silskoho hospodarstva. Seriia «Ekonomichni nauky»*, no. 126 (2012): 198-206.

Makedon, V. V., and Makovetska, A. O. "Informatsiine zabezpechennia ekonomichnoi bezpeky pidpryiemstv v umovakh rynkovoi nestabilnosti" [Information Support for the Economic Security of Enterprises in Conditions of Market Instability]. *Internauka. Seriia «Ekonomichni nauky»*, no. 12 (2023).
DOI: https://doi.org/10.25313/2520-2294-2023-12-9477

Makedon, V., and Korneyev, M. "Improving methodology of estimating value of financial sector entities dealing in mergers and acquisitions". Investment Management and Financial Innovations. 2014. https://www.researchgate.net/publication/289853616_Improving_methodology_of_estimating_value_of_financial_sector_entities_dealing_in_mergers_and_acquisitions

Mazepa, S. "Zabezpechennia informatsiinoi bezpeky v Ukraini: perspektyvy administratyvno-pravovoho rehuliuvannia" [Ensuring Information Security in Ukraine: Prospects for Administrative and Legal Regulation]. *Aktualni problemy pravoznavstva*, no. 1 (2024): 92-97.
DOI: https://doi.org/10.35774/app2024.01.092

Mentukh, N. F. et al. "Ensuring Information Security: Comparative Legal Aspect". Central European Management Journal. 2023. https://journals.kozminski.cem-j.org/index.php/pl_cemj/article/view/917

Myloserdna, I. M. "Informatsiina bezpeka yak element natsionalnoi bezpeky: teoretychnyi vymir ta osoblyvosti vprovadzhennia" [Information Security as an Element of National Security: Theoretical Dimension and Implementation Features]. *Politykus*, no. 4 (2024): 179-185.
DOI: https://doi.org/10.24195/2414-9616.2024-4.26

Shelukhin, M. et al. "Entrepreneurship Education with the Use of a Cloud-Oriented Educational Environment". International Journal of Entrepreneurship. 2021. https://www.abacademies.org/articles/entrepreneurship-education-with-the-use-of-a-cloud-oriented-educational-environment-11980.html

Shevchuk, M. O. "Do pytannia henezy poniattia informatsiinoi bezpeky yak skladovoi natsionalnoi bezpeky" [On the Question of the Genesis of the Concept of Information Security as a Component of National Security]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia «Pravo»*, vol. 2, no. 78 (2023): 134-139.
DOI: https://doi.org/10.24144/2307-3322.2023.78.2.21

Smotrych, D., and Brailko, L. "Informatsiina bezpeka v umovakh voiennoho stanu" [Information Security under Martial Law]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia «Pravo»*, vol. 2, no. 77 (2023): 121-127.
DOI: https://doi.org/10.24144/2307-3322.2023.77.2.20

Taherdoost, H. "Cybersecurity vs. Information Security". *Procedia Computer Science*, vol. 215 (2022): 483-487.
DOI: https://doi.org/10.1016/j.procs.2022.12.050

Viter, D. V., and Rudenko, O. O. "Suchasna paradyhma protydii zahrozam natsionalnii bezpetsi: pytannia stratehichnoho upravlinnia" [The Modern of Countering National Security Theats: Issues of Strategic Management]. *Pravo ta derzhavne upravlinnia*, no. 3 (2022): 220-226.
DOI: https://doi.org/10.32840/pdu.2022.3.33

Voitsikhovskyi, A. V. "Informatsiina bezpeka yak skladova systemy natsionalnoi bezpeky (mizhnarodnyi i zarubizhnyi dosvid)" [Information Security as Component National Security Systems (International and Foreign Experience)]. *Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina. Seriia «Pravo»*, no. 29 (2020): 281-288.
DOI: https://doi.org/10.26565/2075-1834-2020-29-38

Zakharov, M. V. "Kontseptualizatsiia pidkhodiv do zabezpechennia informatsiinoi bezpeky derzhavy v umovakh viiny" [Conceptualization of Approaches to Ensuring Information Security of the State in Conditions of War]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia «Publichne upravlinnia ta administruvannia»*, vol. 34, no. 1 (2024): 252-253.
DOI: https://doi.org/10.32782/TNU-2663-6468/2024.1/44