Київський національний університет імені Тараса Шевченка
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

ДУБОВСЬКИЙ ОЛЕКСАНДР ГЕННАДІЙОВИЧ

УДК 004.056:32(477)(100)

ДИСЕРТАЦІЯ

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ГЛОБАЛІЗАЦІЇ СВІТОВОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ

291 – Міжнародні відносини, суспільні комунікації та регіональні студії
Галузь знань – 29 «Міжнародні відносини»

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Дубовський Олександр Геннадійович

Науковий керівник: Бєлоусова Наталія Борисівна, кандидат політичних наук, доцент

Київ – 2025

АНОТАЦІЯ

Дубовський О. Г. Інформаційна безпека України в умовах глобалізації світового інформаційного простору. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 291 «Міжнародні відносини, суспільні комунікації та регіональні студії» (29 «Міжнародні відносини»). – Київський національний університет імені Тараса Шевченка, МОН України. Київ, 2025.

Дисертаційна робота присвячена визначенню тенденцій та можливостей посилення спроможностей України щодо забезпечення інформаційної безпеки в умовах глобалізації інформаційного простору. З огляду на це, актуальність дослідження інформаційної безпеки України підсилюється у контексті використання світового інформаційного простору як арени для міжнародного протиборства, політичного впливу, стратегічного планування та впровадження інновацій, а також в умовах трансформації безпекової ситуації внаслідок збройної агресії Російської Федерації проти України. Україна як держава з відкритим інформаційним простором і геополітично вразливим становищем постає не лише об’єктом зовнішнього інформаційного впливу, але й активним актором інформаційного протиборства, а стратегічна значущість її інформаційної безпеки потребує посилення спроможностей забезпечення національної безпеки.

Зазначено, що інформаційна безпека розглядається автором роботи як об’єктно-суб’єктний феномен, що визначає умови функціонування суб’єктів в інформаційному просторі, конституйованому глобалізацією. При цьому світовий інформаційний простір розглядається як індикатор глобалізації, на який впливають інтеграційні чинники і який характеризується просторово-часовими, трансформаційними, ефекторними та динамічними особливостями.

Глобальні загрози та виклики інформаційній безпеці України визначено як результат впливу зовнішніх чинників, зокрема відзначено, що демографічні та технологічні чинники мають каталізуючий вплив на глобалізаційні процеси,

політичні чинники – ретардаційний та модераційний вплив, екологічні – медіаційний. Глобальними викликами для інформаційної безпеки України вважаються складний характер інформаційних впливів і стрімкий розвиток інформаційних технологій, а загрозою глобального та національного масштабу – інформаційні операції Російської Федерації. Встановлено, що внутрішньою загрозою інформаційній безпеці України є відсутність системи виявлення та ефективного реагування на інформаційні впливи, що формує підґрунтя для перетворення зовнішніх загроз у внутрішні небезпеки і негативно впливає на реалізацію національних інтересів та функціонування інформаційного простору.

У роботі проаналізовано нормативно-правове та інституційне забезпечення інформаційної безпеки України та виявлено короткостроковість і проблемно-орієнтованість стратегічних цілей, фрагментарність функціональної цілісності системи та її нерівномірність захищеності, необхідність посилення ефективності координації діяльності національних структурних підрозділів і створення системи оперативного реагування на інформаційні впливи на основі використання цифрового науково-аналітичного розробку. Крім цього, автор розглянув управління інформаційним простором як механізм захисного рівня забезпечення інформаційної безпеки України в контексті феноменологічної парадигми.

Виявлено, що визначальними для інформаційної безпеки стали політичні чинники, оскільки вони впливають на тенденції її розвитку. При цьому розуміння внутрішніх чинників детермінації достатності інформаційної безпеки України є важливими для розробки заходів її посилення в умовах державно-політичної стагнації, коли вона може виступати перепоною ефективному функціонуванню системи інформаційної безпеки країни як з точки зору її реформування, так і реалізації заходів її стратегічного розвитку.

За результатами дослідження визначено інтегральну проєктивну систему інформаційної безпеки держави, що ґрунтується на принципі дуальності та основах проєктивної геометрії та передбачає побудову проєктивного інформаційного простору. Інтегральність системи забезпечується використанням систем штучного інтелекту, що дозволить автоматизувати частину процесів і розширити техніко-

технологічний підхід забезпечення інформаційної безпеки. Впровадження системи сприятиме безперервному моніторингу інформаційного простору, забезпечить швидке виявлення загроз і оперативне реагування на них, дозволить прогнозувати та запобігати негативним наслідкам інформаційного впливу та підвищить координацію роботи різних структурних підрозділів. Відзначено, що інтегральна проєктивна система інформаційної безпеки може сприяти активізації міжнародного співробітництва у сфері обміну інформацією, уніфікації систем стандартизації моніторингу та оперативного реагування на загрози.

Практичне використання результатів дисертації може бути враховано при оновлені Стратегії інформаційної безпеки України та плану заходів, оскільки діюча редакція документу розрахована на період до кінця 2025 року.

Ключові слова: глобалізація, інформаційний простір, інформаційна безпека, виклики, загрози, культурні особливості, штучний інтелект, воєнний стан, Україна.

ANNOTATION

Dubovskyi O. Information Security of Ukraine in the Context of Globalization of the World Information Space. – Qualifying scientific work as a manuscript.

The dissertation for obtaining academic degree of the Philosophy Doctor (Ph.D.), specialization 291 «International Relations, Social Communications and Regional Studies» (29 – International Relations). – Taras Shevchenko National University of Kyiv, MES of Ukraine. Kyiv, 2025

The dissertation is devoted to identifying trends and opportunities for strengthening Ukraine's capabilities to ensure information security in the context of globalization of the information space. In view of this, the relevance of studying Ukraine's information security is enhanced in the context of using the world information space as an arena for international confrontation, political influence, strategic planning and the implementation of innovations, as well as in the context of the transformation of the security situation as a result of the armed aggression of the Russian Federation against Ukraine. Ukraine, as a state with an open information space and a geopolitically vulnerable position, appears not

only as an object of external information influence, but also as an active actor of information confrontation, and the strategic significance of its information security requires strengthening the capabilities to ensure national security.

It is noted that information security is considered by the author as an object-subject phenomenon that determines the conditions for the functioning of subjects in the information space constituted by globalization. At the same time, the world information space is considered as an indicator of globalization, which is influenced by integration factors and is characterized by spatiotemporal, transformational, effector and dynamic features.

Global threats and challenges to the information security of Ukraine are determined as a result of the influence of external factors, in particular, it is noted that demographic and technological factors have a catalytic effect on globalization processes, political factors have a retarding and moderating effect, and environmental factors have a mediating effect. Global challenges to the information security of Ukraine are considered to be the complex nature of information influences and the rapid development of information technologies, and a threat of a global and national scale is the information operations of the Russian Federation. It has been established that the internal threat to the information security of Ukraine is the lack of a system for detecting and effectively responding to information influences, which forms the basis for the transformation of external threats into internal dangers and negatively affects the implementation of national interests and the functioning of the information space.

The paper analyzes the regulatory and institutional support for Ukraine's information security and reveals the short-term and problem-oriented nature of strategic goals, the fragmentation of the functional integrity of the system and its uneven security, the need to strengthen the effectiveness of coordination of the activities of national structural units and create a system of operational response to information impacts based on the use of digital scientific and analytical development. In addition, the author considered information space management as a mechanism for the protective level of ensuring Ukraine's information security in the context of the phenomenological paradigm.

It was found that political factors have become decisive for information security, since they influence the trends of its development. At the same time, understanding the internal factors determining the adequacy of Ukraine's information security is important for developing measures to strengthen it in conditions of state and political stagnation, when it can act as an obstacle to the effective functioning of the country's information security system both from the point of view of its reform and the implementation of measures for its strategic development.

According to the results of the study, an integral projective system of information security of the state was determined, which is based on the principle of duality and the foundations of projective geometry and involves the construction of a projective information space. The integrity of the system is ensured by the use of artificial intelligence systems, which will allow automating part of the processes and expanding the technical and technological approach to ensuring information security. The implementation of the system will contribute to continuous monitoring of the information space, ensure rapid detection of threats and prompt response to them, allow predicting and preventing the negative consequences of information impact and increase the coordination of the work of various structural units. It is noted that the integral projective system of information security can contribute to the intensification of international cooperation in the field of information exchange, unification of monitoring standardization systems and prompt response to threats.

The practical use of the results of the dissertation can be considered when updating the Information Security Strategy of Ukraine and the action plan, since the current version of the document is designed for the period until the end of 2025.

Key words: globalization, information space, information security, challenges, threats, cultural peculiarities, artificial intelligence, martial law, Ukraine.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України

1. Дубовський, О. Г. (2024). Особливості світового інформаційного простору в контексті критеріального аналізу феномена глобалізації. *Acta de historia & politica: saeculum XXI, VIII*, 99–107.

2. Дубовський, О. Г. (2024). Управління світовим інформаційним простором: можливості та обмеження. *Міжнародні відносини, суспільні комунікації та регіональні студії*, 1(18), 16–27.

3. Дубовський, О. Г. (2024). Інформаційна безпека: суб'єктність та штучний інтелект. *Journal of Innovations and Sustainability*, 8(2). https://doi.org/10.51599/is.2024.08.02.09

Праці, які засвідчують апробацію матеріалів дисертації

1. Дубовський, О. Г., & Степанишин Р. Д. (2023). Розвиток технологій штучного інтелекту та його вплив на міжнародну інформаційну безпеку. *Матеріали Всеукраїнської науково-практичної конференції молодих вчених, ад'юнктів, слухачів, курсантів і студентів «Молодіжна військова наука у Київському національному університеті імені Тараса Шевченка»*. ВІКНУ, с. 436–437 (Особистий внесок автора: 0,12 авт. аркш.).

2. Дубовський, О. Г. (2021). Психологічна війна: юридичні та етичні аспекти. *Матеріали XVII міжнародної науково-практичної конференції «Військова освіта і наука: сьогодення та майбутнє».* ВІКНУ, Т. 2, с. 18–19.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Глобалізація, охопивши всі сфери суспільного буття, сприяла трансформації світового інформаційного простору і безпекових умов його існування. З огляду на це, актуальність дослідження інформаційної безпеки України підсилюється у контексті використання світового інформаційного простору як арени для міжнародного протиборства, політичного впливу, стратегічного планування та впровадження інновацій, а також в умовах трансформації безпекової ситуації внаслідок збройної агресії Російської Федерації проти України. Україна як держава з відкритим інформаційним простором і геополітично вразливим становищем постає не лише об'єктом зовнішнього інформаційного впливу, але й активним актором інформаційного протиборства, а стратегічна значущість її інформаційної безпеки потребує посилення спроможностей забезпечення національної безпеки.

Аналіз наукових досліджень свідчить, що наразі забезпечення інформаційної безпеки є проблемною сферою з високим ступенем невизначеності, що зумовлюється варіативністю та різнорідністю чинників детермінації, зростаючим масштабуванням загроз та різнорівневістю їхніх наслідків, технологічною складністю загроз, швидкістю появи нових технологій та проблемою розробки систем виявлення загроз, інституційною суперечливістю забезпечення національної політики і проблемами адаптивного правового регулювання. Концептуально джерелом такої невизначеності є особливості функціонування і регулювання світового інформаційного простору. Відповідно зменшення невизначеності та підвищення адаптивності системи інформаційної безпеки України залежить від її політичної, соціальної та технологічної стійкості.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дослідження виконане в межах комплексної програми науково-дослідних робіт Київського національного університету імені Тараса Шевченка і науково-дослідної теми Навчально-наукового інституту міжнародних відносин Київського національного університету імені Тараса Шевченка №19БФ048-02 (державний

реєстраційний номер 0119U100336) «Стратегія протистояння геополітичним викликам і загрозам національній безпеці України в умовах становлення нового світопорядку».

Мета й завдання дослідження. Мета дослідження полягає у визначенні тенденцій та можливостей посилення спроможностей України щодо забезпечення інформаційної безпеки в умовах глобалізації світового інформаційного простору.

Для досягнення поставленої мети було передбачено розв'язання таких дослідницьких **завдань**:

- охарактеризувати теоретико-методологічну базу дослідження інформаційної безпеки та стан її розробленості;
- проаналізувати глобальні та національні виклики і загрози інформаційній безпеці України, а також її імплементаційну достатність;
- визначити можливості та обмеження управління інформаційним простором як механізму забезпечення інформаційної безпеки України;
- виявити рівень достатності інформаційної безпеки України з огляду на актуальні загрози і виклики;
- розробити концептуальну модель інтегральної проєктивної системи інформаційної безпеки України та її потенційний вплив на трансформацію міжнародної безпеки.

Відповідно, **об'єктом дослідження** є міжнародна інформаційна безпека, а **предметом дослідження** є інформаційна безпека України в умовах глобалізації світового інформаційного простору.

Методи наукового дослідження. Для досягнення мети та реалізації завдань дисертаційної роботи використано такі загальнонаукові методи, як порівняння та узагальнення – для визначення на основі огляду наукових публікацій проблемних аспектів забезпечення інформаційної безпеки України, контекстуальних особливостей та тенденцій глобалізації (Розділ 1); аналіз – для визначення особливостей світового інформаційного простору (підрозділ 1.3), глобальних та національних загроз та викликів інформаційній безпеці України (підрозділ 2.1), особливостей її забезпечення та достатності (підрозділи 2.2 та 2.3), можливостей та

обмежень управління інформаційним простором України (підрозділ 2.4), технологічних можливостей розробки системи інформаційної безпеки України з метою забезпечення оперативного та ефективного реагування на інформаційні загрози (підрозділ 3.2); синтез – для інтеграції концептуальних основ при розробці інтегральної проєктивної системи інформаційної безпеки України (підрозділи 3.2).

Для аналізу емпіричних даних використано статистичні методи: кореляційний аналіз – для виявлення зв'язків між інтенсивністю глобалізації політичної, економічної, соціальної сфер та розвитком інформаційної безпеки, а також визначення особливостей взаємодії внутрішніх і зовнішніх чинників інформаційної безпеки (підрозділ 3.1); аналіз гістограм розподілу частот – для виявлення тенденції посилення інформаційної безпеки при зміні безпекової ситуації в світі (підрозділ 3.1); аналіз діаграм розсіювання – для визначення особливостей впливу національних культурних вимірів на інтенсивність глобалізаційних процесів (підрозділ 3.1); регресійний аналіз – для визначення впливу внутрішніх чинників (вимірів національної культури та індексу сприйняття корупції) на розвиток інформаційної безпеки України та її готовності до нових викликів (підрозділ 3.1).Програмне забезпечення: IBM SPSS Statistics 23.0, jamovi 2.6.13. Інформаційна база: публікації вітчизняних та зарубіжних науковців; бази даних KOF (KOF Index of Globalization, 2023), NCSI (National Cyber Security Index by e-Governance Academy, 2023), The Culture Factor Group (Country comparison tool, The Culture Factor Group, 2023), IMF (AI Preparedness Index (AIPI) International Monetary Fund, 2023), the Corruption Perceptions Index (CPI) Transparency International (Corruption Perceptions Index, 2023). Надійність та достовірність результатів дослідження забезпечувалися поєднанням якісного й кількісного аналізу даних, застосуванням статистичних методів аналізу даних за допомогою сучасного програмного забезпечення.

Наукова новизна одержаних результатів полягає в тому, що визначено та обґрунтовано концептуальну основу удосконалення системи інформаційної безпеки України з урахуванням внутрішніх і зовнішніх загроз. У проведеному дослідженні:

Вперше:

− запропоновано та обґрунтовано концептуальну модель інтегральної проєктивної системи інформаційної безпеки України як потенційної спроможності посилення рівня національної безпеки держави та активізації міжнародної співпраці;

− визначено рівень готовності держави до використання штучного інтелекту в умовах поглиблення цифровізації інформаційного простору та нестабільності міжнародної безпекової системи.

Удосконалено:

−теоретичне осмислення впливу глобалізації на сучасну систему міжнародної безпеки та уточнено особливості впливу демографічних та технологічних чинників як каталізуючих, політичних – як ретардаційних і модераційних та екологічних – як медіаційних аспектів функціонування системи;

−розуміння спроможностей посилення інформаційної безпеки України через призму індивідуалізму та довгострокової орієнтації як сприятливих детермінацій, а також поблажливості як компенсаторного чинника особливостей реалізації заходів стратегічної значущості у безпековій сфері.

Набуло подальшого розвитку:

−розуміння глобальних викликів і загроз як негативних ефектів поглиблення інтеграційної взаємодії між акторами, а також національних викликів і загроз як слабких аспектів функціонування системи інформаційної безпеки, що дозволяє переосмислити ефективність стратегії України;

−твердження про необхідність удосконалення нормативно-правового та інституційного забезпечення інформаційної безпеки України внаслідок короткостроковості та проблемно-орієнтованості стратегічних цілей, фрагментарності функціональної цілісності, нерівномірності системної захищеності та потреби посилення координації діяльності національних структурних підрозділів.

Практичне значення результатів дослідження. Теоретичне значення роботи полягає в удосконалені теоретико-методологічних засад дослідження

інформаційної безпеки через уточнення особливостей глобалізаційного впливу на національну і міжнародну безпекову систему, а також поглиблення знань щодо внутрішніх і зовнішніх чинників детермінації забезпечення інформаційної безпеки держави. Практичне використання результатів дисертації може бути враховано при оновлені Стратегії інформаційної безпеки України та плану заходів, оскільки діюча редакція документу розрахована на період до кінця 2025 року. Теоретичні та емпіричні результати дисертаційної роботи можуть бути використані для підготовки лекційних занять із дисципліни «Інформаційно-психологічна боротьба у воєнній сфері».

Особистий внесок здобувача. Дисертаційна робота є самостійним науковим дослідженням. Усі наведені в рукописі дисертації висновки та результати одержані автором особисто. З наукових праць, опублікованих у співавторстві, використані лише ті ідеї та положення, які є результатом особистих досліджень здобувача.

Апробація матеріалів дисертації. Основні положення дисертаційної роботи апробовані у формі участі у міжнародних науково-практичних конференціях, зокрема Першій науково-практичній міжнародній конференції з питань кібердипломатії (м. Київ, 15-16 травня 2024 року; участь в обговоренні); Всеукраїнській науково-практичній конференції молодих вчених, ад'юнктів, слухачів, курсантів і студентів «Молодіжна військова наука у Київському національному університеті імені Тараса Шевченка» (м. Київ, 27 квітня 2023 року; виступ і публікація тез); XVII міжнародній науково-практичній конференції «Військова освіта і наука: сьогодення та майбутнє» (м. Київ, 26 листопада 2021 року; виступ і публікація тез).

Публікації. За результатами дослідження опубліковано 5 наукових праць, з яких 3 наукових статті у фахових виданнях України та 2 публікації, які додатково відображають наукові результати дисертаційної роботи.

Структурно дисертація складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації – 207 сторінок, в тому числі основний текст – 174 сторінки, список використаних джерел складається з 235 найменувань.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Концептуальні та методологічні аспекти дослідження інформаційної безпеки

В умовах розвитку інформаційного суспільства та глобалізації інформаційна безпека стає підґрунтям стабільного функціонування різних сфер суспільного буття як окремої людини, держави, так і світового співтовариства в цілому. Інформаційна безпека є об’єктом наукового пізнання не тільки в технічних, а й соціально-гуманітарних дослідженнях, актуальність яких все більше зростає та сприяє оформленню окремої комплексної галузі знань. Сучасні інформаційні перетворення суспільства зумовлені науково-технічним прогресом, що й визначає первинність технічно орієнтованого знання з опорою на використання математичних методів прогнозування, моделювання, необхідність інформаційно-аналітичного забезпечення дослідження. Однак розширення сфер значущості інформаційної безпеки та проблемність її забезпечення зумовили необхідність більш масштабного її наукового осмислення та прикладного дослідження.

Кожна з галузей наукового знання акцентує на певному аспекті інформаційної безпеки:

- на системі правових гарантій захищеності особи і суспільства, забезпеченні їх життєдіяльності, прав і свобод (в юриспруденції), наприклад, А. Ю. Нашинець-Наумова (2017), О. Д. Довгань (2018), Т. Ю. Ткачук (2019), П. Д. Біленчук та М. І. Малій (2022), К. Є. Ковальов (2023), О. М. Вінник (2022) та ін.;

- на особливостях сприймання, ставлення, переживання та відповідності забезпеченню важливих потреб і інтересів людини (в психології), наприклад, В. М. Петрик та ін. (2018), О. В. Морозов та Т. Р. Морозова (2019), В. І. Алещенко (2022) та ін.;

- на тенденціях розвитку, умовах життєдіяльності соціуму та його структур за оптимального співвідношення свободи і необхідності (в філософії), наприклад, Н. М. Авер'янова та Т. Воропаєва (2020), Є. О. Архипова (2011), П. В. Квіткін (2021) та ін.;

- на властивостях та результатові діяльності систем і органів державної влади (в політології), наприклад, Д. Ю. Арабаджиєв (2020), Д. В. Дубов (2010), І. О. Валюшко (2018) та ін.

При такому мультидисциплінарному дослідженні поняття інформаційної безпеки стає інтегруючим для різних сфер суспільного буття та галузей наукового знання. В умовах зростаючої практичної доцільності дослідження проблематики інформаційної безпеки та його міждисциплінарного характеру виникає питання його теоретичного та методологічного підґрунтя. Зазвичай теоретичну основу дослідження інформаційної безпеки складають: теорія інформації, теорія технологічного детермінізму, теорія соціотехнічних систем, теорії інформаційних правовідносин (Тихомиров, 2014а).

Теорія інформації визначає особливості передачі, перетворення, зберігання, кількісного представлення інформації через використання математико-статистичного апарату. Одним із фундаментальних понять теорії інформації є ентропія, яка дозволяє кількісно представити невизначеність випадкової величини. Вимірювання інформації часто представляється через розподіл випадкових величин. Також використовується поняття взаємної інформації, що визначається для двох випадкових величин та відповідає спільній інформації, що може бути використана для опису їхньої кореляції. До інших важливих понять у теорії інформації належать пропускна спроможність каналу, відносна ентропія, кодування, помилки, надмірність та ін. (Bloch & Barros, 2011). Перевагою використання даної теорії як концептуальної основи дослідження інформаційної безпеки є об'єктивність. Інформація підлягає кількісному вираженню на основі аналізу ймовірнісних характеристик джерела інформації. Визначення кількості інформації не залежить від її джерела. Використання математико-статистичного апарату та моделювання дозволяє вирішувати завдання забезпечення безпеки,

ефективності та конфіденційності передачі, зберігання та збору інформації (Liang et al., 2009).

Теорія технологічного детермінізму надає визначальну роль технологіям та науково-технічному прогресу як чинникам розвитку суспільства. В межах даної теорії інформаційна безпека досліджується через її техніко-технологічну складову щодо достатності та надійності всіх компонентів систем обробки, зберігання, обміну інформацією. В даному контексті інформаційна безпека часто ототожнюється з кібербезпекою та має об'єктне спрямування, оскільки орієнтована на впровадження заходів захисту певного значущого об'єкта обробки, зберігання інформації тощо, забезпечення достатності, оптимальності, надійності функціонування відповідних комп'ютерних систем. Техніко-технологічним виміром інформаційної безпеки є захищеність інформації та підтримуючої інфраструктури від впливів природного чи штучного характеру, випадкової чи навмисної природи (Нестеряк, 2014). В межах даної теорії захист інформації є основою інформаційної безпеки. Визначальними є техніко-технологічні спроможності та фахова підготовка відповідальних структурних підрозділів забезпечення національної безпеки.

Теорія соціотехнічних систем надає визначального значення у дослідження інформаційної безпеки взаємодії людини і техніки, їхнім взаємовпливам. При цьому вивчаються такі підсистеми, як: технічна, до якої належать пристрої, технологічне обладнання, що забезпечують функціонування системи інформаційної безпеки; соціальна, до якої належать люди, суб'єкти забезпечення інформаційної безпеки, їхні знання, навички та вміння, особистісні та психофізіологічні особливості, цінності та мотиви, які можуть впливати на виконання посадових обов'язків та ефективність працівника. Відповідно можна визначити інформаційно-технічну й інформаційно-психологічну безпеку (Тихомиров, 2014а). Життєдіяльність соціотехнічних систем відбувається в інформаційному середовищі, яке характеризується динамічністю, глобальністю, великою кількістю латентних загроз. Відповідно захищеність соціотехнічних систем визначається ефективністю реагування на загрози даного середовища.

Поняття інформаційного простору та середовища використовуються в даному випадку як синоніми. Значущість інформації визначається соціальною цінністю, тому пов'язана із певним суб'єктом. Саме суб'єктивний вимір визначає достатність інформаційної безпеки, як певний рівень необхідного забезпечення чи стандарт, тому він може відрізнятися залежно від організації, галузі, країни. Така суб'єктивність в розумінні інформаційної безпеки дозволяє розширити її зміст в порівнянні з об'єктивністю теорії інформації, в межах якої інформаційна безпека розглядається виключно в аспекті захищеності несуб'єктивованої інформації (Тихомиров, 2014а). Можна виокремити три складові інформаційної безпеки в межах теорії соціотехнічних систем:

- техніко-технологічна, що визначається технічними та технологічними можливостями в інформаційній сфері;
- інформаційно-психологічна, що пов'язана з особливостями сприймання інформації та відповідного реагування на неї;
- правова, що відповідає за регулювання інформаційних відносин.

Окрім складових, О. О. Тихомиров (2014а) визначає також рівні інформаційної безпеки. Індивідуальний рівень стосується особистого захисту від інформаційних загроз. Прикладами визначених складових можуть бути відповідно доступ та навички використання сучасного програмного забезпечення, критичне ставлення до інформації та рівень розвитку правової культури. Загальний рівень відповідає умовам, що визначають інформаційну розвиненість суб'єктів та інформаційне середовище їхнього функціонування. Прикладами відповідних складових цього рівня будуть розвиток технічної бази інформаційного простору, популяризація національної культури та нормативно-правове забезпечення регулювання інформаційної сфери. Третій рівень є захисним, його складає система захисних механізмів в інформаційній сфері. Прикладами складових даного рівня відповідно будуть технології забезпечення захисту певних категорій інформації чи об'єктів інформаційної інфраструктури, протидія дезінформації та маніпуляції, передбачена юридична відповідальність за правопорушення в інформаційній сфері.

Теорії інформаційних правовідносин визначають місце та правову природу норм регулювання відносин в інформаційній сфері. Прикладами таких теорій є: теорія інформаційних прав як цивільно-правового інституту, теорія інформаційного права як галузі права, теорія інформаційних відносин як інституту комплексного галузевого законодавства, пропрієтарна теорія (Кохановська, 2013). Поява даних теорій зумовлена глобалізацією та розвитком інформаційного суспільства, зростаючою при цьому впливовістю інформації в порівнянні з енергією та матерією в економічній, політичній, військовій та духовній сферах як у внутрішньодержавному, так і в міжнародному плані. Предметом правового регулювання при цьому є відносини з приводу інформації, а не сама інформація. Інформаціє є об'єктом правових відносин.

Л. В. Борисова та ін. (2018) виділять специфічні ознаки інформації, що мають значення для права та які слід враховувати при формуванні законодавства щодо правового регулювання в інформаційній сфері. Такими ознаками є: самостійність відносно матеріального носія, властивості якого не мають визначального впливу на організацію інформації; можливість багаторазового використання; невичерпність при багаторазовому використанні; нееквівалентність передавання інформації передаванню речей; непідлегліть фізичному зносу, можливе старіння інформації, її моральний знос чи втрата актуальності; кількісна визначеність; системність.

Значущість інформації в сучасному світі та розвиток інформаційного простору зумовили також появу правової інформатики як комплексної концепції до вивчення інформаційних відносин та обороту світової інформації в контексті правового середовища. Правова інформатизація передбачає використання інформаційних технологій у праві, наприклад, для управління адміністративними системами, для функціонування баз даних юридичних документів, для розробки правових експертних систем (Юдкова, 2014).

В методологічному аспекті інформаційну безпеку можна досліджувати через призму різних підходів: системного, структурно-функціонального, феноменологічного та діяльнісного (Шемчук, 2019). Системний підхід, часто

вживається синонімічно системно-структурний підхід, визначає інформаційну безпеку як компонент національної безпеки. Даний підхід передбачає, що об'єкт дослідження складається з одиниць чи елементів, які входять до його складу і утворюють певну структуру. Відповідно передбачається, що дослідження інформаційної безпеки здійснюється через призму національної безпеки як структури вищого порядку. Наявність зв'язків та взаємовідношень між елементами всередині структури та між структурами дозволяє досліджувати об'єкти як складні системи. Методологічна специфіка підходу полягає у вивченні механізмів та закономірностей поєднання окремих елементів в цілісну систему. Відповідно інформаційна безпека розглядається через зв'язки з іншими структурними елементами національної безпеки, наприклад, з економічною, енергетичною, воєнною, та через механізми забезпечення її цілісності. Зазвичай метою дослідження з використанням даного підходу є вивчення закономірностей і механізмів утворення складного об'єкта. До принципів системного підходу належать (Кустовська, 2005):

1. Принцип генеральної мети, що полягає в направленості всіх складових системи на забезпечення єдиної мети, що в дослідженні інформаційної безпеки може бути визначено як захист державного суверенітету. Зміни в системі мають обов'язково узгоджуватися з визначеною генеральною метою.

2. Принципи єдності полягає у вивченні системи в зв'язаності її структурних компонентів.

3. Принцип ієрархії передбачає можливість аналізу рівнів, наприклад, дослідження інформаційної безпеки на нижчому структурному рівні передбачає вивчення її складових компонентів, як кібербезпека, комунікаційна безпека, медіабезпека, та на вищому структурному рівні в системі національної безпеки.

4. Принцип розвитку передбачає можливість вдосконалення системи, ступінь її модернізації має визначатися доцільністю.

5. Принцип емерджентності полягає у відмінності властивостей цілісної системи від властивостей її структурних компонентів, що може виражатися у

розбіжності оптимумів елементарного та глобального рівнів досягнення цілі системи.

6. Принцип децентралізації забезпечує здатність системи реагувати на впливи зовнішнього середовища через окремі структурні компоненти. Співвідношення централізації та децентралізації визначається генеральною метою системи та особливостями зовнішнього середовища. Посилення централізації системи зменшує її гнучкість та швидкість реагування на зміни умов. Посилення децентралізації ускладнює забезпечення узгодженості функціонування елементів щодо досягнення генеральної мети.

Системний підхід найбільш поширеним є в дослідженні правових аспектів інформаційної безпеки. Можливість підходу вивчати забезпечення інформаційної безпеки на різних рівнях та її механізмів зумовила його популярність в наукових дослідженнях механізмів правового регулювання, державного управління тощо. Б. А. Кормич визначає інформаційну безпеку як «систему органів державної влади загальної та спеціальної компетенції, задіяних у процесі формування та реалізації політики інформаційної безпеки, внутрішні й зовнішні ролі та відносини якої регулюються системою правових норм і принципів» (Шемчук, 2019, с. 54). Ефективність інформаційної безпеки держави залежить від кожної складової її державно-правового механізму, який складається з трьох взаємопов’язаних елементів: державних інституцій інформаційної безпеки; ролей та правових відносини в реалізації політики інформаційної безпеки; правових норм та принципів, які регулюють реалізацію політики інформаційної безпеки.

За А. Ю. Нашинець-Наумовою (2017, с. 29), «система забезпечення інформаційної безпеки – це внутрішня структура, систематизована сукупність, єдність, взаємозв’язок і диференціацію окремих її елементів (об’єкт, суб’єкти, основні характеристики, рівні інформаційної безпеки та перелік загроз)». Ключовими для забезпечення інформаційної безпеки елементами є рівні інформаційної безпеки та загрози.

На основі узагальнення міжнародного досвіду Л. О. Євдоченко (2011) розглядає систему інформаційної безпеки в контексті динаміки глобалізаційних

процесів як комплексний механізм реалізації та захисту національних інтересів в інформаційній сфері. Г. П. Ситник (2012) розглядає інформаційну безпеку як складову системи національної безпеки, структуру якої формують суб'єкти забезпечення національної безпеки, наприклад, органи державної влади, посадові особи, інститути громадянського суспільства тощо, та сукупність механізмів, наприклад, правові, організаційні тощо. О. С. Зозуля (2017) визначає систему державного управління інформаційною безпекою структурним елементом системи забезпечення інформаційної безпеки.

Структурно-функціональний підхід співвідносить структурні одиниці зі способами їхнього функціонування, визначаючи зв'язки між елементами та цілим. Це дозволяє на основі зв'язків визначати актуальні та потенційні стани системи, функціональне навантаження елементів, вразливі місця та умови збереження структурної цілісності. Функція виявляє важливі елементи всередині системи та визначає особливості взаємодії системи з її оточенням. Функція визначає структуру об'єкта, відповідно вона має бути вихідною точкою при його дослідженні. Поява нових функцій передбачає зміни в структурі об'єкта. За Т. Парсонсом, життєздатна та ефективна система повинна відповідати таким функціональним вимогам (Литовченко, 2012):

- адаптації, що забезпечує її пластичність та можливість реагування на зміни зовнішнього середовища;

- ціледосягнення, що полягає в визначеній доцільності її функціонування;

- інтеграції, що виявляється у взаємоузгодженості функціонування елементів системи;

- латентності, що полягає у відтворюваності структури та в забезпеченні інформаційної безпеки може виявлятися в інформаційній культурі та освіченості суспільства.

Структурно-функціональний підхід оперує поняттями функції та дисфункції, явної та латентної функції. За Р. Мертоном, функція сприяє збереженню стабільності та інтеграції в суспільстві, а дисфункція зменшує адаптивність та регуляторну здатність системи, перешкоджає задоволенню потреб суспільства

(Литовченко, 2012). Явні функції усвідомлюються суб'єктами та характеризуються доцільністю, спрямовані на регулювання системи. Латентні функції є чи прихованими, чи випадковими, чи ненавмисними. Корупційні ризики є проявами латентних функцій, які мають деструктивне значення. Дисфункція системи інформаційної безпеки може виражатися у недостатності технологічного забезпечення, в організаційних прорахунках та у відсутності конкретизованої мети.

На основі даного підходу В. І. Алещенко (2022) визначає зовнішні та внутрішні чинники інформаційного впливу на особистісному, суспільному та державному рівні. Аналізуючи критерії інформаційної безпеки та особливості інформаційного впливу, його наслідки для морально-психологічного стану, пропонує структурно-функціональну модель інформаційної безпеки особистості. Д. В. Вєдєнєєв та О. Р. Копієвська (2021) здійснили аналіз організаційних та правових засад, форм і методів протидії гібридним загрозам та запобіганню деструктивним впливам у соціокультурній сфері України. В дослідженні проблеми інформаційної безпеки дітей завдяки застосуванню структурно-функціонального підходу виділено сім підстав для класифікації дитячого сегменту українського Інтернету та його основні соціальні функції, визначено основні ризики для суспільства та ювенальної вікової групи (Біловус, 2020).

Феноменологічний підхід визначає інформаційну безпеку як прояв захищеності інформаційного середовища та розробленості правового регулювання. Безпека розглядається як явище, як складний соціально-політичний феномен. Феноменологічний підхід розгляд проблему інформаційної безпеки через життєвий досвід та особистісні сенси, інтерсуб'єктивні значення предметів в результаті співвідношення декількох точок зору на об'єкти та події. Умовою ефективного забезпечення інформаційної безпеки є знання механізмів конструювання інтерсуб'єктивної реальності, можливостей виявлення латентних ознак, фонових подій та знань, що лежать в основі інтерпретації інформації. О. А. Панченко (2020) вважає, що феноменологічний підхід в забезпеченні інформаційної безпеки є важливим при оцінці подій та явищ як ризикованих, при визначенні ступеня небезпеки для суспільства, держави, міжнародних відносин.

Феноменологія Е. Гуссерля спрямована на розуміння сприймання світу та виявлення структур, що лежать в основі досвіду, виявлення сутності явищ через спостереження та аналіз, пошук загальних рис. Особливості відображення інформації в свідомості визначають її соціальну цінність та визначають різноманіття її суб'єктивних форм. За М. Гайдеггером внутрішня сутність речей виявляється нам у своїй буттєвій даності такою, якими вони є поза теоріями та суб'єктивними уявленнями. Приписи та директиви можуть стати для людини законом та мати реальну, а не номінальну, регуляторну здатність лише виходячи із сущого, долаючи дуалізм належного та існуючого. Природа речей несе в собі свій порядок, суще конструює належне з врахуванням значущості та важливості буття (Максимов, 2009). Відповідно в інформаційній безпеці слід виходити з сутнісного через його виявлення та визначати природні йому засоби для забезпечення ефективного функціонування відповідних систем.

Діяльнісний підхід дає змогу розглядати інформаційну безпеку як процес, діяльність органів державної влади. Методологічним підґрунтям даного підходу є теорія діяльності. Діяльність розглядається через призму пояснювального принципу, парадигми, теоретичної моделі та методу наукового дослідження, що дають можливість вивчати об'єкти та явища як прояв, форму чи результат цілеспрямованого впливу людини та суспільства на навколишній світ в процесі діяльності (Гусарєв, 2004). Основними методологічними принципами діяльнісного підходу є:

- цілеспрямованість, діяльності передбачає досягнення певної мети, вона характеризується доцільністю;

- культурно-історична зумовленість, що відображає залежність особливостей діяльності від конкретно-історичних та соціально-культурних умов, наприклад, науково-технічний прогрес забезпечив появу нових засобів діяльності у сфері інформаційної безпеки, однак зумовив і появу нових загроз;

- внутрішній та зовнішній план діяльності, наявність внутрішніх та зовнішніх її регуляторів, наприклад, в інформаційній безпеці діяльність працівників може регламентуватися наявними зовнішніми інструкціями,

дотримання яких та можливість ризикованої поведінки буде зумовлюватися внутрішніми особистісними цінностями та мотивами; на рівні державної політики у сфері інформаційної безпеки даний принцип проявляється через введення стандартів, заборон та через контроль їх дотримання, а також через освіченість, моральні норми, традиції тощо.

О. О. Тихомиров (2014а) відзначає, що діяльнісний підхід надає можливість поєднати різні аспекти дослідження інформаційної безпеки управління загрозами, системи захисних заходів, особливості функціонування суб'єктів в інформаційному середовищі, оскільки основою для їхньої інтерпретації можуть бути відповідні змістові компоненти діяльності. Використовуючи діяльнісний підхід, В. А. Ліпкан та ін. (2006, с. 161) визначають, що «забезпечення інформаційної безпеки досягається у процесі свідомої цілеспрямованої діяльності органів державного управління, із запобігання можливому порушенню їх нормального функціонування в результаті дії загроз і небезпек». Відповідно ефективність системи інформаційної безпеки забезпечується через створення нормальних умов для функціонування відповідних органів державного управління. При цьому суб'єкти управління інформаційною безпекою, спеціалізуючись на виконанні специфічних завдань, мають взаємодіяти між собою, забезпечуючи функціонування цілісної системи. Діяльність відповідних суб'єктів залежно від предметної компетенції може реалізуватися через нормативно-правові, управлінські, науково-технічні, інформаційно-аналітичні та інші заходи. Відповідно проблеми забезпечення інформаційної діяльності мають аналізуватися залежно від суб'єкта управління та особливості його діяльності, її умов та вимог. Т. Ю. Ткачук (2019, с. 114) розглядає інформаційну безпеку як діяльність щодо «недопущення шкоди властивостям об'єкта безпеки, зумовленої інформацією та інформаційною інфраструктурою, а також засобів і суб'єктів цієї діяльності». В забезпеченні інформаційної безпеки В. А. Ліпкан та ін. (2006) виокремлюють три аспекти:

1) інформаційно-технічну безпеку, що передбачає діяльність спрямовану на захист комп'ютерних мереж, телекомунікацій, технологічного забезпечення тощо;

2) інформаційно-психологічну безпеку, що забезпечується через діяльність у сфері протидії дезінформації, деструктивним інформаційним впливам тощо;

3) інформаційну безпеку у сфері прав і свобод людини, що відноситься до правотворчої та правоохоронної діяльності з метою забезпечення права на інформацію.

Розглянуті теорії та методологічні підходи в своєму поєднанні визначають ключові орієнтири та інструменти наукового дослідження, його інтерпретаційну сутність, акценти та обмеження. Для дослідження інформаційної безпеки України в умовах глобалізації світового інформаційного простору теоретичним підґрунтям визначено теорію соціотехнічнічних систем, методологічною основою – феноменологічний підхід.

1.2. Інформаційна безпека та інформаційний простір: концептуалізація понять

Дослідження інформаційної безпеки передбачає визначення даного поняття та його диференціацію від суміжних понять. Визначень інформаційної безпеки велика кількість і кожен дослідник зазвичай акцентує увагу на власному баченні найсуттєвішого чи спирається на контекст дослідження, аналізовані аспекти, конкретну галузь наукового знання, об’єктом якої стає інформаційна безпека. За результатами аналізу та узагальнення визначень інформаційної безпеки відмінності у її дефініціях можна представити у вигляді наступних сутнісних означень (Нашинець-Наумова, 2017) з доповненням відповідними прикладами конкретних науковців:

1. Інформаційна безпека як стан захищеності інформаційного простору. Акцентується увага на статичному аспекті, що визначається як загальний опис умов та обставин, що забезпечують захист інформаційного простору, середовища, сфери. Прикладом даного сутнісного означення є визначення Д. Безуглого (2018), що інформаційну безпеку можна розглядати як рівень інформаційної захищеності держави, що убезпечує національні інтереси держави та суспільство від негативних

наслідків різного роду дій щодо інформації. О. Г. Соснін (2014, с. 292) визначає інформаційну безпеку як «стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави». Відповідно таке сутнісне означення інформаційної безпеки як стану передбачає аналіз системи заходів, що його забезпечують.

2. Інформаційна безпека як процес управління загрозами, що забезпечує інформаційний суверенітет держави. Дане означення акцентує увагу на динамічному аспекті забезпечення інформаційної безпеки. Інформаційний суверенітет держави в даному аспекті передбачає здатність регулювати та контролювати власний інформаційний простір, захищати від зовнішніх зловмисних впливів. Так І. Р. Боднар (2014, с. 30) визначає інформаційну безпеку «як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз». О. Довгань (2015) визначає інформаційну безпеку як гаранта забезпечення інформаційного суверенітету держави, при цьому організаційна та технологічна складові інформаційної безпеки мають відповідати структурі інформаційного забезпечення розвитку суспільства в умовах глобалізації. І. Килимник (2023) визначає інформаційну безпеку як сукупність юридичних, технічних та організаційних методів, способів та дій, що орієнтовані на захист даних від стороннього впливу. Відповідно таке сутнісне означення інформаційної безпеки в процесуальному управлінському аспекті передбачає аналіз сукупності послідовних дій, як правило, комплексного характеру в її забезпеченні, що спрямовані на досягнення інформаційного суверенітету держави.

3. Інформаційна безпека як умова захищеності національних інтересів держави в інформаційному середовищі. Передбачається, що інформаційна безпека розглядається як необхідність для захищеності національних інтересів, що має виключне значення в умовах посилення інформатизації всіх сфер суспільного життя. Реалізація національних інтересів є основою збереження державного суверенітету та прогресивного розвитку суспільства. Прикладом такого сутнісного

означення є визначення В. В. Шемчука (2019), що інформаційна безпека забезпечує захищеність інформаційного простору та передбачає реалізацію превентивних та захисних заходів щодо інтересів як окремої людини, так і суспільства, і держави в цілому. А. Ю. Нашинець-Наумова (2017) розглядає поняття інформаційної безпеки через поєднання об'єктивних та суб'єктивних умов забезпечення захищеності інтересів суб'єктів (особи, суспільства, держави), під об'єктивними умовами розуміються стандарти безпеки, а під суб'єктивними – можливості суб'єктів усвідомлювати та контролювати умови функціонування в інформаційному просторі. О. Дзьобань (2015) визначає інформаційну безпеку через захищеність національних інтересів в інформаційній сфері, які є збалансованою сукупністю інтересів особистості, суспільства та держави. Відповідно національні інтереси представлені трьома групами: для особистості щодо прав та свобод у використанні інформації, захисту інтелектуальної власності та захисту від маніпуляцій свідомістю; для суспільства щодо розвитку інформаційного суспільства, інтелектуального потенціалу та зміцнення психологічного здоров'я; для держави щодо забезпечення інформаційного суверенітету, розвитку інформаційних технологій, інтеграції в світовий інформаційний простір. Відповідно таке сутнісне означення передбачає аналіз відповідності забезпеченості інформаційної безпеки національним, суспільним, особистісним потребам.

4. Інформаційна безпека як стан системи, що може стосуватися чи правової регуляції інформаційних процесів в державі, чи технологічних можливостей ефективного функціонування тощо. Акцентується увага на стані власне системи забезпечення інформаційної безпеки, її нормативно-правової чи технічної складової, як оцінки її функціональної спроможності. Прикладом такого означення є визначення О. М. Каплі (2023), що інформаційна безпека є конституційною нормою, що закріплена в нормативно-правових документах, а ефективність інформаційної безпеки держави залежить від законодавчого регулювання, дієвості нормативно-правового забезпечення, адаптації в до нових світових умов. Р. Бондаренко (2021, с. 97) визначає інформаційну безпеку як «стан системи, який здатний забезпечити цільові параметри безпеки» та забезпечує ефективність її

діяльності в умовах внутрішніх та зовнішніх інформаційних впливів. Б. А. Кормич (2004, с. 16) визначає інформаційну безпеку як «стан захищеності встановлених законодавством норм та параметрів інформаційних процесів та відносин, що забезпечує необхідні умови існування держави, людини та суспільства як суб'єктів цих процесів та відносин». Відповідно таке сутнісне означення інформаційної безпеки передбачає аналіз нормативно-правового, технічного її забезпечення, оцінку спроможності системи ефективно реалізовувати своє функціональне призначення.

5. Інформаційна безпека як стан суспільних відносин щодо захисту як окремого громадянина, суспільства, так і держави в цілому загроз в інформаційному просторі. Таке означення передбачає зовсім інший фокус у сутнісному визначенні інформаційної безпеки, оскільки ключовою виступає взаємодія людей, організацій, держав. Інформаційна безпека – це «стан міжнародних відносин, який виключає порушення світової стабільності та створення загрози безпеці держав і світової спільноти в інформаційному просторі» (Біленчук та ін., 2018, с. 67). Відповідно норми міжнародного права мають бути регуляторами в забезпеченні інформаційної безпеки держави, оскільки в умовах глобалізації інформаційного простору інформаційні впливи мають потенційно деструктивні наслідки не тільки для окремої держави, а й для світової спільноти в цілому. Дане означення передбачає аналіз відповідно регуляторів суспільних відносин в забезпеченні інформаційної безпеки.

6. Інформаційна безпека як вид чи складова національної безпеки. В такому означенні інформаційна безпека є одним із видів національної безпеки, реалізацією відповідної функції держави в інформаційній сфері. Наприклад, таку узагальнену дефініцію надає В. А. Ліпкан та ін. (2006) на основі аналізу визначень інформаційної безпеки у нормативно-правових актах, оскільки національна безпека є цілісною та не може бути репрезентована через сукупність складових, а тому інформаційна безпека є реалізацією властивостей національної безпеки в інформаційній сфері. Деякі ж науковці розглядають інформаційну безпеку як окрему складову національної безпеки, що тісно пов'язана з усіма іншими,

наприклад, О. М. Солодка (2020), пояснюючи, що невизначеність меж інформаційного простору держави обмежує функції держави у забезпеченні інформаційного суверенітету через неможливість забезпечення достатньої правової регламентованості сфери інформаційної безпеки, а відсутність державного суверенітету в інформаційній сфері підриває підвалини реалізації як інформаційної, так і національної безпеки в цілому. О. Виговська та Н. Бєлоусова (2017) визначають інформаційну безпеку як складову національної безпеки, яка спрямована на забезпечення розвитку соціального та державного прогресу з метою реалізації духовного та інтелектуального потенціалу країни та передбачає системну превентивну діяльність органів державного управління щодо забезпечення інформаційної безпеки на рівні особи, соціальної групи та суспільства в цілому. О. Мітенко (2019) визначає інформаційну безпеку як складову національної безпеки України, що має свою специфіку зумовлену інформаційною сферою. Інформаційна безпека спрямована на протидію та попередження реальних та потенційних загроз національній безпеці, що унеможливлюють чи ускладнюють реалізацію національних інтересів та збереження національних цінностей. Відповідно таке сутнісне означення інформаційної безпеки передбачає аналіз відповідності її завдань та заходів забезпеченню національної безпеки.

Отже, кожне з даних сутнісних означень інформаційної безпеки передбачає й відповідний фокус у вивчені проблем її забезпечення. Визначення інформаційної безпеки є достатньо багатоаспектним як з точки зору понятєвого статусу, так і цільового, контекстуального, часового. Інформаційну безпеку можна розглядати як в статичному, так і в динамічну аспекті, що визначає її як стан, процес та умову в площині функціонування як окремої системи забезпечення, чи системи суспільних відносин, чи суверенітету держави, національних інтересів, національної безпеки, чи інформаційного простору та інформаційної сфери в цілому. При цьому поняття інформаційної сфери, середовища, простору є спільними для наведених дефініцій. Виникає необхідність диференціації даних понять чи підтвердження їхньої синонімічності.

О. М. Солодка (2020) відзначає, що визначення інформаційного простору може мати пов’язаність з територією, як, наприклад, сукупність інформаційних потоків, що обмежена геополітичними кордонами держави, або як інформаційна інфраструктура та сукупність інформаційних ресурсів держави. Однак такі визначення суперечать транскордонності інформації в умовах глобалізації. О. М. Солодка (2020, с. 45) пропонує під інформаційним простором розуміти «середовище здійснення суб’єктами інформаційної сфери діяльності, пов’язаної зі створенням, збиранням, одержанням, зберіганням, використанням, поширенням, охороною та захистом інформації, на яку поширюється юрисдикція України, а також функціонуванням національної інформаційної інфраструктури».

Інформаційний простір є сукупністю баз та банків даних, технологій забезпечення їхнього функціонування, правил та принципів регулювання інформаційної взаємодії організацій і громадян та задоволення їхніх інформаційних потреб (Яруліна, 2019). О. Солдатенко (2018) визначає інформаційний простір як сукупність інформаційних об’єктів, поширення яких здійснюється суб’єктами через доступні засоби комунікації. Інформаційний простір визначається як складова частина соціального простору, як поле соціальних відносин (Коляда, 2021). Він є сукупністю індивідів, груп та організацій, об'єднаних використанням інформації за допомогою інформаційно-комунікаційних технологій.

Отже, інформаційний простір є частиною соціального простору реалізується через інформаційні процеси та забезпечується інформаційною інфраструктурою. У визначенні інформаційного простору часто використовується поняття «середовище» та «сфера». В. І. Гур’єв та ін. (2018, с. 9) зазначають, що інформаційний простір складається з інформаційного середовища, яке визначається інформаційними процесами та інформаційними відносинами, сукупності інформаційних ресурсів та інформаційної інфраструктури. Воно є усталеним поєднанням. Інформаційне середовище держави визначається системою інформаційної безпеки, розвиненістю інформаційно-телекомунікаційних систем, індустрії інформаційних послуг, системи фахової підготовки, проведенням

наукових досліджень (Солодка, 2020). Воно є частиною інформаційного простору, що має визначену територію поширення, суб'єктів взаємодії, програмно-технічне забезпечення обробки та передачі інформації та знаннями індивідів (Яруліна, 2019).

Отже, інформаційне середовище визначається функціонуванням власне інформаційної інфраструктури, відображає рівень розвитку суспільних відносин та науково-технічного прогресу. Інформаційний простір може існувати незалежно від людини, а середовище утворене взаємодією людей (Коляда, 2012).

Диференціюючи інформаційний простір та інформаційну сферу, О. М. Селезньова (2016, с. 142) зазначає, що інформаційний простір є частиною інформаційної сфери, що обмежується матеріальною та нематеріальною територією. Інформаційна сфера визначається сукупністю суб'єктів, що здійснюють інформаційну діяльність, інформацією та інформаційними відносинами, інформаційною наукою та інформаційною культурою, інформаційною інфраструктурою, інформаційним правом та інформаційним законодавством. Інформаційна сфера формується та розвивається в інформаційній діяльності (Ліпкан та ін., 2006). Вона включає інформаційну інфраструктуру, інформаційні ресурси, суб'єктів, суспільні відносини, системи правового забезпечення та інституційну систему державного управління (Солодка, 2020).

Отже, найвужчим є сутнісно інформаційне середовище, що є частиною інформаційного простору та конкретизується через інфраструктурне забезпечення та особливості інформаційних процесів. Інформаційний простір держави є простором, що знаходиться під її інформаційним суверенітетом та визначається техніко-технологічним розвитком інформаційно-телекомунікаційних систем та мереж. Він є частиною інформаційної сфери. Інформаційна сфера є найширшим поняттям, вона є діяльнісно об'єктивованою.

Функціональна наповненість інформаційної безпеки залежить від техніко-технологічного розвитку інформаційної сфери суспільного буття. Оскільки дана сфера визначається діяльністю, то відповідно розвиненість використовуваних для реалізації її завдань інформаційних технологій та технічного забезпечення є

основою повноти та ефективності захисту інформаційних ресурсів та систем, завдань та функціональної спроможності інформаційної безпеки. Розгляд історичного розвитку інформаційних технологій дозволяє прослідкувати поступові трансформації змісту інформаційної безпеки. Можна виділити такі етапи (Гур'єв та ін., 2018):

1. До 1816 року використовували природні засоби інформаційних комунікацій. Завдання інформаційної безпеки при цьому полягало в захисті відомостей про події, особистої інформації та реалізовувалось через дотримання таємниці листування, обмеження фізичного доступу до носіїв інформації.

2. З 1816 року бере початок використання технічних засобів електро- та радіозв'язку. Забезпечення інформаційної безпеки здійснювалось за допомогою застосування кодування повідомлення (сигналу).

3. З 1935 року застосовуються засоби радіолокації та гідроакустики. Забезпечення інформаційної безпеки полягало в поєднання організаційних і технічних заходів, що сприяли підвищенню захищеності засобів радіолокації від дії активних маскуючих і пасивних імітуючих радіоелектронних перешкод.

4. З 1946 року використовуються в практичній діяльності електронно-обчислювальні машини. З появою даного винаходу інформаційна безпека передбачала використання методів та способів обмеження фізичного доступу до технічних засобів обробки та передачі інформації.

5. 1965 рік ознаменував створення та розвиток локальних інформаційно-комунікаційних мереж. Забезпечення інформаційної безпеки забезпечувалось обмеженням доступу до технічного обладнання, об'єднаного у локальну мережу шляхом адміністрування й управління доступом.

6. З 1973 року використанням надмобільних комунікаційних пристроїв породило нові загрози інформаційній безпеці, виникла потреба у розробці критеріїв безпеки. Інформаційний ресурс став стратегічно важливим як на організаційному, так і на державному рівні. Формується нова галузь міжнародного права – інформаційне право.

7. З 1985 року створення та розвиток глобальних інформаційно-комунікаційних мереж та використання космічних засобів забезпечення зв'язку зумовили планетарну циркуляцію інформації у просторі та часі. Інформаційна безпека набула визначального значення для національної та міжнародної безпеки. Її забезпечення передбачає створення відповідної макросистеми на основі міжнародної консолідації.

Інтенсивність інформаційного обміну зростає, що сприяє збільшенню та посиленню зв'язків в різних сферах суспільного буття та цілісності світу. Повнота, достовірність, своєчасність інформації впливає на ефективність виробництва, зумовлює політичні ефекти, культурні та соціальні катаклізми. Підвищення ролі інформації відзначається як в житті окремої людини, так і у прийнятті державних управлінських рішень. Спостерігаються якісно-кількісні зміни глобального рівня, інформаційні потреби зростають, інформація стає базовим елементом сучасного суспільства, інформаційного суспільства. Його особливостями є: розвиненість інформаційної інфраструктури, великий обсяг інформаційних ресурсів як запасів знань, масове використання комп'ютерів, масштабність покриття телекомунікаційних мереж, поява нових форм та видів діяльності у віртуальному просторі, доступність та швидкість отримання інформації, створення єдиного простору розповсюдження інформації поза реальними геополітичними кордонами державних телекомунікаційних мереж, необхідність вдосконалення міжнародного права та формування нового законодавства адаптованого до інформаційної ери (Борисова та ін., 2018).

При зростаючому глобальному мережевому покритті та віртуалізації інформаційного простору поняття інформаційної безпеки та кібербезпеки зближуються та часом ототожнюються. В. М. Панченко (2013) на основі аналізу співвідношення даних понять визначає:

- поняття «кібернетична безпека» доцільно використовувати для позначення безпеки об'єктів, що пов'язані з комп'ютерними технологіями, цифровими мережами;

- поняття «інформаційна безпека» слід використовувати щодо безпеки об’єктів у ширшому розумінні, що передбачає використання інформаційних технологій як комп’ютерних, так і комунікативних (Панченко, 2013).

Отже, кібербезпека є складовою інформаційної безпеки. Цифровізація інформаційного простору сприяє розвитку техніко-технологічного забезпечення, зростанню питомої ваги кібербезпеки в структурі інформаційної безпеки, тому часто для об’єктивації інформаційної безпеки використовують індикатори кібербезпеки.

Проаналізувавши різні визначення інформаційної безпеки та ключові сутнісні її означення, співвідношення інформаційної безпеки та кібербезпеки, диференціювавши поняття інформаційного простору, середовища та сфери, варто розглянути ключові поняття дисертаційного дослідження через призму теорії соціотехнічнічних систем та феноменологічного підходу. Відповідно такими ключовими поняттями є інформаційний простір та інформаційна безпека. Теорія соціотехнічнічних систем та феноменологічний підхід формують теоретико-методологічну основу дисертаційної роботи.

Інформаційний простір є результатом розвитку соціотехнічних систем, взаємодіючи із зовнішнім середовищем, з іншими відкритими системами, він змінюється. Інформаційному простору притаманний синергетичний характер. Інформаційний розвиток та суспільний розвиток взаємопов’язані. Високі темпи інформаційного розвитку сприяли переосмисленню інформаційної складової національної безпеки. Інформаційна безпека визначається не як вид національної безпеки, а як наднаціональний вид всезагальної соціальної безпеки. Вона є підґрунтям нормального функціонування соціуму. Важливість інформації визначається її соціальною цінністю. Зважаючи на це, інформаційна безпека не може забезпечуватися лише державою. Вона є функцією кожного суб’єкта інформаційної системи суспільства. Держава має можливості здійснювати прямий управлінський вплив на інформаційні відносини за допомогою технічних систем та правових засобів, а також опосередкований – на соціальні процеси. Однак виявляється, що кожен елемент інформаційної системи одночасно може бути як

об’єктом, так і суб’єктом забезпечення інформаційної безпеки, як джерелом потенційних та реальних загроз, так і каналом їх поширення. Тому підвищення інформаційної культури в суспільстві має бути одним з пріоритетних завдань забезпечення інформаційної безпеки (Тихомиров, 2014b).

Інформаційну безпеку, згідно з теорією соціотехнічних систем, можна визначити як «сукупність умов функціонування суб’єктів в інформаційній сфері та суб’єктивних можливостей їх усвідомлення й контролю» (Тихомиров, 2014b, с. 63). Дане визначення не суперечить нормативно-правовому розумінню інформаційної безпеки. Інформаційна безпека України змістовно визначається Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 № 537-V, Законом України «Про національну безпеку України» від 21.06.2018 № 2469-VIII, Законом України «Про Концепцію Національної програми інформатизації» від 04.02.1998 № 75/98-ВР, Стратегією національної безпеки України, затвердженою Указом Президента України від 14.09.2020 № 392, Стратегією кібербезпеки України, затвердженою Указом Президента України від 26.08.2021 № 447. За Стратегією інформаційної безпеки, затвердженою Указом Президента України від 28.12.2021 № 685/2021, інформаційна безпека України:

- визначається складовою частиною національної безпеки;
- відображає стан захищеності «державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави»;
- забезпечує «конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації»;
- є ефективним системним утворенням задля захисту і протидії шкоди населенню через поширення негативних інформаційних впливів, наприклад, скоординоване поширення недостовірної інформації, порушення цілісності інформації з обмеженим доступом (Указ Президента України №685/2021 «Про

рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"», 2021).

Отже, інформаційна безпека об’єктивується через безпечність інформаційного середовища. Вона визначається через статичний та динамічний аспекти. Статичний аспект визначає її як актуальний стан забезпеченості, який має відповідати встановленому такому, який вважається достатнім. Розвиток інформаційних технологій передбачає розвиток й потенційних загроз інформаційній безпеці та сприяє перегляду її достатнього рівня з часом. Динамічний аспект передбачає змінність актуального рівня інформаційної безпеки та діяльність відповідних інституцій щодо підтримання достатнього рівня впродовж якнайбільш тривалого часу. Отже, в цілому мова йде про відповідність умовам, в яких розвиваються та функціонують суб’єкти інформаційного простору, реалізовується їхня діяльність в інформаційній сфері. Природа інформаційної безпеки та загроз визначає доцільність дослідження її як соціально-технічного феномену (Тихомиров, 2014b).

Спираючись на положення феноменологічного підходу інформаційну безпеку можна розглядати як предметність вищого порядку, що як елемент справжньої дійсності визначає життя суспільства. «Їх конституювання також цілком самозрозуміло веде у зворотному напрямку до конституювання просторових речевостей і психічних суб’єктів: зрештою, вони фундовані в цій реальності» (Гуссерль, 2020, с. 331). Отже, для дослідження, визначення, аналізу інформаційної безпеки як об’єктивно-суб’єктивного феномена варто звернутися до інформаційного простору. Його можна розглядати в контексті інтерсуб’єктивного світу, який визначається різноманіттям суб’єктивних сприймань, потоків свідомості та надіє єдності всім цим різноманіттям, конституюючи «об’єктивний» досвід. Це інтерсуб’єктивне існує навіть, якщо кожний суб’єкт не може перебувати з іншим у порозумінні чи «вчуванні», однак розрізнені світи досвіду через зв’язки об’єднуються в один єдиний світ (Гуссерль, 2020, с. 102).

Згідно з феноменологічним підходом інформаційний простір є конструктом свідомості людини, соціокультурним феноменом. І. Г. Коляда (2021) відзначає, що

з кінця ХХ ст. поняття простору все частіше використовується без прив'язки до фізичного розташування, актуалізується опозиція реальне-віртуальне, яка все більше посилюється з розвитком інформаційних технологій. Специфіка реального та штучно створеного, віртуального, зумовлює появу нових форм, норм у використанні інформації. Штучне може змінювати, викривлювати реальне, бути відмінним від нього.

За Е. Гуссерлєм (2020), суб'єкт діє в просторі, занурюється, вживається у те, що відбувається. «Простір наочно репрезентується та конституюється як єдність явищ, дескриптивних способів репрезентації просторового» (Гуссерль, 2020, с. 328). Конституювання означає, що «підпорядковані правилам і необхідно належні до єдності явленого ряди явищ можна інтуїтивно оглянути та теоретично схопити – попри їхню нескінченність (яку можна однозначно опанувати у визначеному «і так далі») – що їхню ейдетичну своєрідність можна проаналізувати й описати, і що можна ясно вгледіти закономірну дію кореляції між визначеним явленим як єдністю та визначеними нескінченними розмаїттями явищ, а заразом розв'язати всі відповідні загадки» (Гуссерль, 2020, с. 329). Простір характеризується протяжністю, його можна зменшувати чи збільшувати. В ньому співіснують різні об'єкти та суб'єкти, характер взаємодії між якими може змінюватися. Простір визначається різнорівневістю, зв'язністю та неперервністю, завдяки чому в його протяжності немає розривів, а простір кожної системи не є замкненим та здатний переходити у простір іншої системи, здобуваючи нові локальні особливості. Кількісні та якісні показники є необмеженими та мають зв'язки, що встановлюються людиною, соціумом, державою, тобто соціальними суб'єктами. Здатність простору переходити в інші системи, набуваючи нових властивостей, свідчить про відносність простору та чутливості до впливу інших процесів та феноменів. Таким чином, інформаційний простір можна розглядати локально, наприклад, як національний, та глобально, як світовий, на основі такої зв'язності. Світовий інформаційний простір буде позначений тенденціями глобалізації та може мати свої локальні особливості.

Феноменологічний підхід передбачає відхід від структурних теорій та зосереджує увагу на проявах сутнісного з метою «навчитися бачити, розрізняти й описувати те, що стоїть перед очима», враховуючи суб'єктивність, соціальну значущість подій у сприйнятті світу (Гуссерль, 2020, с. 13). «Феноменолог судить не онтологічно, коли пізнає онтологічне поняття або положення як вказівку на конститутивні сутнісні зв'язки, коли вбачає в ній «дороговказ» для інтуїтивного виявлення, правомірність і значимість яких міститься лише в них самих» (Гуссерль, 2020, с. 335). Відповідно в дослідженні інформаційного простору феноменологічний підхід передбачає дослідження існуючих зв'язків, явищ, проявів, які є значущими самі по собі та передбачають відповідні дії, реагування системи інформаційної безпеки без намагання визначення природи, походження. Оскільки явище має значущість лише в собі. В умовах глобалізації інформаційного простору намагання дізнатися джерело походження, сенс, задум вимагатиме багато часу в порівнянні з необхідною швидкістю та своєчасністю реагування. Загроза є загрозою сама в собі навіть без врахування джерела походження та сутнісного наміру.

Отже, проблема інформаційної безпеки є міждисциплінарною. Залежно від галузі наукового знання, в якій проводиться дослідження інформаційної безпеки її сутнісні акценти будуть відрізнятися. При цьому трансформація змісту та функціонального навантаження інформаційної безпеки залежить від інформаційного розвитку суспільства. Глобалізація інформаційного простору та його інтеграційний вплив на різні сфери суспільного буття надають визначального значення інформаційній безпеці в контексті забезпечення національної та міжнародної безпеки в сучасних умовах. Використання теорії соціотехнічних систем та феноменологічного підходу дозволяють розглянути проблему забезпечення інформаційної безпеки в новому ракурсі. Виходячи з означення інформаційної безпеки вихідним в її дослідженні передбачається інформаційний простір та його властивості, існуючі в ньому кореляції та суб'єктивні смисли, прояви інформаційних впливів та загроз.

1.3. Трансформація інформаційної безпеки під впливом глобалізації

Глобалізація, першопочатково як відповідь на появу глобальних проблем, перетворилася на сучасну світову тенденцію всеохоплюючого масштабу, що зумовило необхідність зміни засобів та підходів до вирішення вже й локальних проблем. Наслідком глобалізації стало формування світового інформаційного простору, який значно посилив вагомість інформації як політичної та економічної одиниці впливу, що актуалізувало четвертий вимір суспільного розвитку, підтверджуючи його рівність загальновідомим, таким як дипломатичному, економічному та військовому вимірам (Bortnikova et al., 2024).

Геополітичний вимір світового інформаційного простору та інтеграційні процеси в контексті кризових світових явищ актуалізують проблеми управління, зон відповідальності та глибинності впливу в контексті національної та міжнародної безпеки. Нестабільність та саморегуляція світового інформаційного простору є плідним підґрунтям конфліктогенного впливу та дестабілізації на різних рівнях суспільного буття. Стратегія національної та міжнародної інформаційної безпеки має спиратися на першопочатковий теоретико-методологічний аналіз явища глобалізації, проявом якого власне і є формування світового інформаційного простору, актуальні та прогнозовані тенденції подальшої інформатизації суспільства. З даної проблематики можна відзначити дослідження найвпливовіших чинників процесу розвитку інформатизації в умовах міжнародної глобалізації (Babenko et al., 2019), філософських аспектів інформатизації суспільства в умовах глобалізації (Oleksenko, 2015; Voronkova 2010), інформаційних технологій в контексті глобалізації (Слюсарчук, 2015; Enebeli, 2024; Sadiq et al., 2024), наслідків глобалізації інформаційного простору (Vetrov& Voznyuk, 2019; Lukyanova & Lautar, 2013), мілітаризації в контексті глобалізації (Kollias, 2024), інформаційного простору в контексті міжнародної безпеки O. Bortnikova et al., 2024).

Глобалізація охоплює все більше сфер суспільного буття, все глибше інтегрується в світовий устрій. При цьому залежно від сфери дослідження та галузі наукового знання даний феномен має своє визначення з акцентом саме на тих аспектах, що відповідають специфічній предметній області. Відповідно можна виокремити сферу інформаційних досліджень даного феномену, а також – соціально-політичних, військових, економічних, технологічних, культурологічних, екологічних. Глобалізацію можна розглядати і більш абстрактно як сучасний тренд розвитку світового устрою, як наслідок впливу інноваційних факторів, що ініціюють якісно новий етап розвитку різних форм суспільного буття в історії людства. Концептуальну основу осмислення глобалізації формують теорії (Дубовський, 2024а):

- Е. Гідденса, глобалізація як інтенсифікація всесвітніх соціальних відносин, через локальні зміни можуть мати глобальні наслідки;
- М. Кастельса, глобалізація як епоха «інформаційного віку», де глобальні мережеві структури стають основними організаторами активностей, а технологічні зв’язки та мережі впливають на соціальну, політичну та економічну динаміку на глобальному рівні;
- Т. Фрідмана, глобалізація в контексті формування «плоского світу» з рівним доступом до технологій та ринків, що дозволяє різним країнам конкурувати на рівних умовах;
- У. Бека, глобалізація як джерело нових типів ризиків, які не знають кордонів і вимагають глобальних відповідей;
- З. Баумана, глобалізація як джерело постійної невизначеності і зміни в контексті «рідкої модернізації», де традиційні структури швидко трансформуються або розпадаються.

Кожна з даних теорії фокусується на специфічному аспекті глобалізації, для цілісного розгляду даного феномена С. Дмитрук (2019) визначає найбільш загальні ознаки глобалізації, а саме: інтенсивну взаємодію та взаємозалежність держав, відкритість світу та свободу переміщення ресурсів, охопленість глобальними зв'язками соціального простору та відносність геополітичних кордонів.

Є. Тихомирова (2004) пропонує спиратися при дослідженні глобалізації на такі критерії:

- масштабність як ступінь охоплення суспільних явищ і процесів;
- характер змін в глобалізаційному процесі;
- часові та просторові особливості;
- оцінка позитивних та негативних наслідків глобалізації.

За масштабністю глобалізацію можна розглядати конкретно за сферами суспільного буття, або як світове всеохоплююче явище. За характером змін визначаються інтеграційні, трансформаційні та інтенсифікаційні аспекти впливу глобалізації. Часові особливості визначають глобалізацію в контексті історичного розвитку людства та світоустрою, визначають інтенсивні характеристики її прояву залежно від історичної епохи. Особливості прояву глобалізації в матеріальному та віртуальному просторі визначає просторовий критерій. Оцінка позитивних та негативних наслідків глобалізації передбачає аналіз амбівалентності даного явища, оскільки глобалізація сприяє розв'язанню одних проблем та одночасно виникненню інших. Амбівалентність детермінована складністю і різноманіттям акторів процесу глобалізації, суперечливістю їхніх інтересів, потенційною конфліктністю, впливаючи на певну сферу суспільного буття, вона трансформує її не фрагментарно, а діє на систему в цілому. Глобалізація об'єктивується процесом інтеграції світу, зростанням взаємозв'язків різного рівня та складності, при цьому має суб'єктивне позначення щодо зацікавленості різноманітних соціальних акторів в її окремих проявах та можливостях впливу на них.

Дані критерії дозволяють цілісно проаналізувати особливості глобалізації як феномену суспільно-історичного розвитку загального світоустрою з конкретизацією проявів за сферами, як: утворення всесвітнього ринку фінансів, товарів та послуг, транснаціональних корпорацій, глобалізація виробництва; зростання швидкості поширення інформації та масштабності її впливу, становлення світового інформаційного простору, розвитку мережевих технологій; перетворення знання в основний елемент суспільного багатства, зростання персональних контактів на транснаціональному рівні, формування світової

культури; об'єднання зусиль всіх країн світу для подолання проблем екологічної рівноваги (Юськів, 2009). Залежно від сфери суспільного буття, характер змін передбачає домінування в процесі глобалізації проявів чи взаємодії, об'єднання, взаємовпливу, взаємопроникнення, взаємозближення, чи перетворення форм організації, властивостей, чи прискорення, посилення.

Розвиваючись у багатьох сферах глобалізація не стала універсальною, прояви мають різну масштабність та глибину залежно від сфери та країни. Неоднорідність та різна швидкість глобалізаційних змін призводять до «асиметричних шоків» як, наприклад, розділення зон відповідальності, проблеми управління ефектами глобалізаційних змін, що виходять за межі геополітичних кордонів. При універсальній глобалізації її наслідки долалися б легше. Глобалізація поширюється більшою мірою на країни західної цивілізації. Окрім реального географічного простору та матеріальних проявів у вигляді трансферу технологій, товарів, міграції, глобалізація охоплює віртуальний простір (Юськів, 2009).

За часовим критерієм глобалізацію можна визначити як хвильовий процес з чергуванням фаз організації та дезорганізації, що підтверджується часовою динамікою досліджень індексу глобалізації (KOF Index of Globalization). Локальні події можуть як інтенсифікувати інтеграційні процеси, так і сповільнювати їх, формуючи зони стискання та розрідження індикаторної насиченості, підйоми та спади розвитку. В часовій динаміці відстежується загальна тенденція щодо поступового посилення глобалізації, однак кожна країна має свій темп з періодами стагнації.

За критерієм позитивних та негативних наслідків глобалізації розглянемо окремо кожну з груп. Позитивними наслідками глобалізації є: зростання кількості та поліпшення якості товарів на світовому ринку, прогрес у розвитку інформаційних технологій, створення нових робочих місць у невиробничій сфері, поліпшення взаєморозуміння між представниками різних культур, знищення стереотипів щодо способу життя різних соціальних верств населення, проведення заходів щодо вирішення глобальних екологічних проблеми на міжнародному рівні, поширення демократичних цінностей і норм міжнародного права. До негативних

наслідків глобалізації можна віднести взаємозалежність національних економік, збільшення соціально-економічного розриву між багатими і бідними верствами населення, зростання динаміки міграційних потоків, посилення економічного та політичного впливу транснаціональних корпорацій на уряди націй-держав та міжнародні організації, збільшення потенційних загроз для інформаційного суверенітету держави, складність правового регулювання та управління глобалізаційними змінами в умовах багаторівневості, масштабності, відсутності геополітичної відповідності, багатосуб'єктності та багатооб'єктності, множинності та амбівалентності наслідків глобалізації (Юськів, 2009).

В інформаційній сфері індикатором глобалізації є формування світового інформаційного простору. В наукових доробках, законодавчих та нормативних документах також використовується поняття глобального інформаційного простору. Проєкт Закону України «Про інформаційну безпеку України» № 5732 від 01.07.2004 року оперує світовим інформаційним простором як визначеним міжнародним співтовариством, введеним до міжнародно-правових документів поняттям, що означає сферу (об'ємний простір), у якій відбувається інформаційна діяльність людства, впорядкована, як правило, міжнародними конвенціями та договорами. Таким чином, світовий інформаційний простір об'єктивується інформаційною діяльністю, яка в умовах глобалізації масштабується на політичну, економічну, військову, соціально-культурну сфери, та передбачає необхідність правового регулювання на міжнародному рівні.

На основі розглянутих попередньо критеріїв глобалізації можна визначити особливості світового інформаційного простору, зважаючи на загальні тенденції та специфічні сегменти, характер змін, просторові та часові особливості, негативні та позитивні наслідки, та виокремити проблеми управління та правового регулювання. Глобалізація інформаційного простору реалізується через інтегруючі зміни як об'єднання в просторово-комунікативне й соціокультурне середовище різних сфер суспільного буття (економічної, соціальної, культурної, політичної); через інтенсифікуючі зміни як створення транскордонної, інтерактивної й мобільної комунікації різних суб'єктів, у межах якої вони здійснюють швидкий

інформаційний обмін; через трасформуючу зміну значущості традиційних ресурсів, створення нового середовища геополітичних відносин і конкуренції (Дубняк, 2015).

В часовому аспекті світовий інформаційний простір характеризується хвилеподібним розвитком, зумовленим темпами розвитку інформаційних технологій та їхньою доступністю. Відповідно зв'язок з економічною сферою визначає зони прискорення та стагнації, особливості соціально-культурної сфери визначають прийнятність інноваційних розробок. В просторовому аспекті світовий інформаційний простір відзначається відсутністю геополітичної відповідності, наявністю матеріальної та віртуальної складової. Світовий інформаційний простір не має національних та державних кордонів, більшою мірою обмежений щодо можливостей державного контролю та впливу, локалізація джерела інформації утруднюється наявністю великої кількості обхідних каналів. За таких просторових характеристик виникає проблема забезпечення державного суверенітету як незалежності у внутрішній та зовнішній політиці. Він охоплює різні сфери, визначаючи особливості взаємозв'язків між ними. Інформаційні потоки відіграють системотворчу функцію та впливають на стан і динаміку політичної, соціальної, економічної, військово-оборонної, культурної та інших сфер суспільно буття людини. Відповідно в кожній з даних сфер актуальним є забезпечення інформаційної безпеки для протидії загрозам породженим негативними наслідками глобалізації (Дубовський, 2024а).

В межах світового інформаційного простору можна розглядати специфічні сегменти як кіберпростір, комунікаційний простір, соціальний простір, освітній простір, інформаційно-технологічний простір. Зміст сегментів визначається залежно від сфери функціонування інформаційної інфраструктури.

Багатосуб'єктність є визначальною особливістю світового інформаційного простору, оскільки, окрім більш звичних для інших сфер глобалізації міжнародних організацій, транснаціональних корпорацій, держав, політичних партій, релігійних організацій, окремих політиків й громадських діячів, фактично може бути будь-хто, спроможний створювати та поширювати інформаційні повідомлення. Висока

проникність та насиченість інформаційних потоків при великій кількості потенційних акторів підвищують ступінь невизначеності в забезпеченні інформаційної безпеки (Дубовський, 2024а).

Світовий інформаційний простір надає переваги та породжує проблеми. Позитивні наслідки глобалізації в інформаційній сфері пов'язані із мірою інтеграції інформаційних технологій в різні сфери суспільного буття: створення нових робочих місць, розвиток ринку професій; зменшення часових витрат у фінансово-промисловій сфері; підвищення рівня життя; розширення можливостей самореалізації, свободи слова і творчості; скорочення транспортних комунікацій з метою обміну інформацією; доступ до світових інформаційних ресурсів в сфері освіти та науки; удосконалення державного управління через розвиток засобів взаємодії з соціумом. До негативних наслідків глобалізації в інформаційній сфері належать: складність цензурування контенту через високу швидкість розповсюдження інформації; розповсюдження психологічних і політико-психологічних наративів конфліктогенного змісту; встановлення глобального інформаційного контролю над менш розвиненими державами, ідеологічна та культурна експансія; збільшення ролі інформації зі зменшенням її надійності; посилення економічної та соціальної нерівності через різну доступність інформаційних технологій; суперечність між глобальними та національними цінностями; загроза хакерських атак на офіційні веб-сайти державних та фінансових установ; викрадення й продаж конфіденційної інформації; розповсюдження аморального та зловмисного контенту (Чмир, 2020).

На основі критеріального аналізу особливостей глобалізації можна визначити світовий інформаційний простір як процес та наслідок розширення, поглиблення та інтенсифікації взаємозв'язків у різних сферах суспільного буття, що відзначається багаторівневістю, масштабністю, відсутністю геополітичної відповідності, неоднорідністю та сегментованістю, багатосуб'єктністю та багатооб'єктністю, множинністю та амбівалентністю наслідків кількісних та якісних змін форм в часовій динаміці. Таким чином, можна виділити просторово-часові, трансформаційні, ефекторні та динамічні особливості глобалізованого

інформаційного простору. Просторово-часовими особливостями є всеохоплюючий та сегментарний характер, системоутворюючий вплив на різні сфери суспільного буття та змістовна відповідність сфері функціонування інформаційної інфраструктури, зумовленість темпами розвитку інформаційних технологій, відсутність геополітичної відповідності, наявністю матеріальної та віртуальної складової.

Трансформаційними особливостями визначено контекстуальність, амбівалентність, змінність значущості традиційних ресурсів. Ефекторними особливостями є багатосуб'єктність та багатооб'єктність, висока проникність, висока ступінь довіри, складність правового регулювання через високу змінність, гнучкість та геополітичну, культурну суперечність правових норм. Динамічними особливостями є висока швидкість розповсюдження інформації, залежність від інформаційно-технологічного розвитку та доступності технологій, інтерактивність і мобільність комунікації.

Формування світового інформаційного простору є наслідком глобалізації, глибинність та масштабність розвитку якої впроваджує новий світовий порядок. Процеси глобалізації та інформатизації є основою інформаційної безпеки будь-якої держави та визначають її як невід'ємну складову міжнародної інформаційної безпеки (Виговська & Бєлоусова, 2017). Глобалізація інформаційного простору реалізується через інтегруючі зміни різних сфер суспільного буття, а саме економічної, соціальної, культурної, політичної, технологічної. Відповідно світовий інформаційний простір є реактивним щодо змін світового порядку та чутливим до подій та трендів як глобального, так і локального масштабів, які можуть сприяти інтенсифікації, стримуванню, регулюванню тенденцій розвитку світового інформаційного простору та визначати. Світовий інформаційний простір розширюється відповідно масштабності глобалізаційних процесів, визначається її змістовністю та відображає її негативні та позитивні ефекти. Актуальні тенденції глобалізації впливають на розвиток світового інформаційного простору. Політичні та соціальні відносини в XXI столітті демонструють зростаючу складність, що відзначається альтернативністю реалізації актуальних тенденцій в майбутньому.

Оскільки окрім ключових тенденції, можна виділити ще й зони невизначеності, масштабність яких може бути різною. Глобалізація як взаємозалежність держав відкриває не тільки можливості, вона породжує й ризики для національної безпеки. Серед актуальних тенденцій глобалізації можна визначити:

- цифровізацію фінансової системи;

- масове переміщення населення внаслідок збройних внутрішніх конфліктів, політичних, економічних або екологічних причин;

- розширення кіберпростору, яке передбачає масштабнішу віртуалізацію соціальних відносин, наприклад, через активність розвитку технологій Інтернету речей;

- проблемність самодостатності технологій в оборонній промисловості за рахунок зростаючої глобалізації промисловості та логістики.

Дані тенденції розвиваються контекстуально. Світові тенденції, проблеми, події можуть мати:

- каталізуючий вплив, тобто пришвидшувати, посилювати та поглиблювати як глобалізацію в цілому, так і її негативні чи позитивні ефекти;

- ретардаційний вплив, тобто стримувати, затягувати, вповільнювати як глобалізацію в цілому, так і її негативні чи позитивні ефекти;

- медіаційний вплив, тобто опосередковувати, вводити умови реалізації окремих напрямків;

- модераційний вплив, тобто визначати контроль за дотриманням встановлених правил, домовленостей, вимог.

Серед світових чинників глобалізації можна визначити демографічні, екологічні, технологічні та політичні. Їхній вплив на глобалізацію позначається і на світовому інформаційному просторі, відповідно є значущим для забезпечення інформаційної безпеки.

Демографічні чинники глобалізації виявляються у поєднанні дії таких ідентифікаторів як міграція населення, співвідношення рівня народжуваності та смертності, старіння населення, розвиненість освіти, економічна нерівність, урбанізація. Очікується посилення світових демографічних диспропорції при

зростанні загального населення земної кулі. У 2045 році населення світу досягне піку в 10,5 мільярдів (Global Strategic Trends: Out to 2055, 2024). При цьому більшість молодого населення планети буде припадати на країни, що розвиваються, в той час як в розвинених економіках будуть спостерігатися процеси старіння та гостра втрата населення в 2030-х і 2040-х роках. Наявність великого сегменту молоді в населенні є потенційною економічною перевагою, якщо буде забезпечено конкурентоспроможний рівень освіти, розвинено ринок праці. Однак зважаючи на особливості країн, що матимуть найбільший демографічний приріст, вірогіднішим буде ризик нестабільності таких суспільств через неможливість національної економіки реалізувати такий людський капітал (Global Strategic Trends: Out to 2055, 2024). Демографічні зміни, спричинені низькою народжуваністю і збільшенням тривалості життя, виявлятимуться в старінні населення більшості економічно розвинених країн. Потенційне зниження продуктивності праці може спричинити втрату економічної конкурентноспроможності. Менша частка населення працездатного віку сприятиме руйнуванню робочих місць та кадровим проблемам оборонного сектору. В країнах, що розвиваються, очікується зростання частки середнього класу, він буде економічно вразливим, однак дасть приріст категорії населення, що матиме ресурси, необхідні знання та прагнення для міграції (Jordan, 2017). Відповідно підйом середнього класу вплине на інтенсивність міграційних потоків, що за таких умов сприятиме посиленню мультинаціональності суспільств та зростанню можливості політичної напруженості, дестабілізації суспільства, поширенню негативних суспільних настроїв тощо (Global Trends 2040: a more contested world, 2021).

Світовий інформаційний простір в такій ситуації зазнаватиме посилення значимості соціальних мереж, що сприятиме підтриманню національної ідентичності, згуртованості та єдності (Запорожець & Бєлоусова, 2022), що на локальному рівні посилюватиметься географічно віддаленими суб'єктами. В умовах же зростаючої політичної напруженості соціальні медіа можуть набувати політичного значення, забезпечуючи прозорість дебатів чи то підлягаючи

маніпулятивним впливам. Питання про ідентифікацію дезінформації при швидкості та оперативності розповсюдження інформації вимагатимуть розвитку специфічних інструментів інформаційної безпеки, підвищення освіченості та медіаграмотності населення. Наявність великої кількості інформації та джерел вимагає розвитку специфічних навичок осмисленого знання, що тільки посилюватиметься в майбутньому та забезпечуватиме при їхній низькій розвиненості благодатне підґрунтя для пропаганди та маніпуляцій. Наприклад, такими можливостями може скористатися інша держава, яка прагне посилити сепаратистські настрої, делегітимізувати геополітичного суперника, вплинути на світову громадську думку, засновуючись на мультинаціоанльності суспільств.

Отже, демографічні чинники каталізують глобалізаційні процеси, основним наслідком їхньої дії є поява мультинаціональних суспільств. Інтенсифікація міграції посилює ризики інформаційних загроз. Інформаційні впливи можуть загострювати міжетнічні конфлікти, проблеми інтеграції мігрантів, сприяти дестабілізації суспільства, прихильності до радикальних та екстремістських організацій через використання фейкових новин, пропаганди, маніпуляцій щодо дискримінації, негативних стереотипів, упередженості щодо мігрантів.

Екологічні чинники виявляються через природні та антропогенні впливи на глобалізаційні процеси. Сучасні екологічні проблеми потребують формування спільної екологічної політики та посилення міждержавних відносин (Бєлоусова & Євдомаха, 2019). Найбільшим їхнім ідентифікатором природніх впливів екологічних чинників є кліматичні зміни, їхня швидкість та масштабність, додаватимуть мільйони людей до міграційних потоків. Антропогенні впливи позначаються на глобалізації економічної сфери, яка будучи шляхом вирішення проблеми вичерпності ресурсів, їхнього ефективного розподілу, може мати і негативні ефекти, як навмисне розірвання ланцюгів постачання та спекуляція енергією. Глобалізація в промисловому секторі та логістиці створює серйозні загрози для оборонної промисловості, як то потенційна залежність від геополітичних суперників, можливість перебоїв в постачанні комплектуючих, недостатність потужностей оборонної промисловості країн, що розвиваються.

Політичне і правове прийняття певних технологічних досягнень для деяких суспільств може бути більш вільним, ніж для інших, що може дати стратегічну перевагу відповідним урядам щодо розвитку оборонної промисловості (Jordan, 2017). Попит на енергію очікувано зросте вдвічі у 2045 році, що тільки посилить впливовість країн-постачальників енергоресурсів та важливість енергетичної інфраструктури. Зростатиме також попит на рідкісні мінерали, які є необхідними для багатьох побутових технологій, як комп'ютери, мобільні телефони, та і для військових технологій, як супутниковий зв'язок, дистанційно керована зброя. В даний час КНР володіє більш ніж 85% таких корисних копалин і тому користується майже монопольним становищем (Jordan, 2023). Значне зростання попиту на критичні корисні копалини може сприяти геостратегічному суперництву та напруженості у регіонах.

Зміни клімату та потреба в ресурсах вже використовуються для впливу, а зі зростанням проблем така тенденція може посилитися. Вони можуть бути основою для тиску та реалізації політичних інтересів, приводом для воєнних конфліктів, підґрунтям для появи радикальних ідеологічних рухів, дестабілізації суспільств шляхом загострення релігійних, економічних та культурних розбіжностей. Існує ризик політичної та соціальної поляризації, екотероризму. Виникає парадоксальна ситуація. Зміна клімату, погіршення стану навколишнього середовища та вичерпність ресурсів являють собою спільні глобальні виклики, що мають посилювати глобалізацію, однак вони можуть навпаки сприяти зростанню глобальної конкуренції за владу (Global Strategic Trends: Out to 2055, 2024).

Проблема контролю над простором також буде загострюватися, Антарктида, міжнародні води і повітряний простір, космічний простір, а також інформаційний простір та кіберпростір (Global Trends 2040: a more contested world, 2021). Для функціонування глобальних економік проблема спільного простору є критичною.

Отже, наявність глобальних проблем сприятиме об’єднанню зусиль щодо їх вирішення, однак може посилити суперництво та дезінтеграційні процеси в світі. Екологічні чинники мають медіаційний вплив, вони створюють умову для реалізації тенденцій глобалізації, чи посилюючи її, чи стримуючи. Світовий

інформаційний простір як такий що є спільним, набуватиме все більшої значущості. Його особливості дозволяють здійснювати вплив приховано та планомірно. Розростання інформаційного простору визначає швидкість поширення та охоплення аудиторії, що може використовуватися для збільшення масштабів впливу екологічних рухів, енергоощадність та розвиток взаємозалежних економік підвищує ризик та наслідки кібератак. Володіння ресурсами необхідними для розвитку інформаційних технологій надає перевагу як щодо впливовості в технологічному забезпечення інформаційної сфери, так і в її захисті.

Технологічні чинники ідентифікуються через розвиток технологій та інновацій, які впливають на глобалізаційні процеси в різних сферах суспільного буття. Технологічний прогрес, окрім пришвидшення економічної глобалізації, може сприяти посиленню владної та економічної нерівності за рахунок різної швидкості впровадження технологій та неоднорідного доступу до їхніх можливостей (Піпченко, 2019). Технологічні досягнення можуть підвищувати рівень безробіття за рахунок знищення робочих місць, однак можуть і сприяти розвитку ринку праці за рахунок появи нових професій, створення нових сфер діяльності та сприяти економічному зростанню, збагаченню інтелектуального потенціалу, реалізації креативного потенціалу розвитку системи людина-машина.

Використання інформаційних технологій є одними з визначальних аспектів інтеграційних процесів, що передбачає міжнародне співробітництво в інформаційній сфері, спрямоване на розвиток цифрових технологій та наукових інноваційних досліджень (Pipchenko et al. 2021). Значущість розвитку інформаційних технологій зростає з масштабами цифровізації різних сфер суспільного буття, що посилює важливість забезпечення як кібербезпеки, так й інформаційної безпеки в цілому. Економічна глобалізація сприяє збереженню ресурсів, розвиток технологій її інтенсифікує через цифровізацію фінансової системи, однак це посилює взаємозалежність країн. Фінансова система стає мультилокально високореактивною, що підвищує ризик негативних наслідків таких злочинних дій, як викрадення, модифікація даних, дезінформація, локальне блокування фінансових систем. Глобалізації є джерелом нових можливостей, однак

і породжує нові ризики. Інформаційна безпека як на національному, так і на міжнародному має бути готовою до таких загроз. Наприклад, використання квантових комп'ютерів вплине на розвиток інформаційної сфери, не тільки змінить спосіб обробки даних, але спричинить появу нових загроз для систем інформаційної безпеки, що засновані на класичних алгоритмах.

Розвиток технологій збільшуватиме взаємодію мільйонів людей по всій планеті, посилюватиме значимість інформації, сприятиме розвитку віртуальної та доповненої реальності. Повсюдна присутність пристроїв, підключених до Інтернету, загострюватиме проблему приватності. Розвиток великих мовних моделей сприятиме посиленню мовної транспарантності світу. Однак розвиток технологій сприятиме швидкому старінню в професії, посиленню невизначеності професійного майбутнього, що може спричинити посилення вимог до соціальних гарантій. Розвиток біотехнологій сприятиме старінню населення, падінню зайнятості, глибинним етичним дискусіям, в умовах глобалізації можливому ідеологічному розколу, породженню нових ідеологічних рухів. Етичні питання використання штучного інтелекту вимагатимуть відповідей на питання визначення ключових цінностей, регуляторних правил, суб'єктності у визначенні налаштувань, меж використання, відмінностей у дозволеному та забороненому залежно від країни, відповідно це вимагатиме удосконалення нормативно-правових основ як використання даних технологій, так відповідно й забезпечення інформаційної безпеки. Множинність суб'єктів в світовому інформаційному просторі не тільки буде посилюватися, а сприятиме формуванню впливових та авторитетних об'єднань політиків, бізнес-лідерів, науковців, лідерів суспільних думок тощо. Мультинаціональність об'єднань потенційно може мати стримуючий ефект щодо військових інтервенцій. Такого роду недержавні організації матимуть геополітично необмежену можливість підтримки, з потенційними спроможностями формулювати нові соціальні вимоги, визначати проблеми і пропонувати рішення, що виходять за рамки окремої держави (Андрєєва & Бовкунович, 2021).

Такі тенденції посилюватимуть зміщення питань забезпечення національної безпеки в позадержавний сектор. Зростаюча залежність економічної, політичної та

соціальної сфер від технологій підвищить попит на послуги з кібербезпеки не тільки державного, а й приватного сектору. Необхідність забезпечення необхідного рівня кібербезпеки як стратегічно важливих ресурсів держави (збройних сил, державного управління, критичної інфраструктури) та водночас приватних інтересів не завжди матиме можливість для більшості країн на рівні державного управління. Це потребуватиме співпраці з спеціалізованими на кіберзахисті компаніями, що призведе до розвитку ринку відповідних послуг. В умовах світового інформаційного простору насиченість його технологічними можливостями сприятиме як зростанню потенційних ризиків для інформаційної безпеки, так і новим можливостям для захисту. Забезпечення інформаційної безпеки на міжнародному рівні може вирішуватися шляхом розробки відповідних правових основ та міжнародних інституцій (Global Strategic Trends: Out to 2055, 2024). Успішно реалізовані потенційні вектори розвитку технологічного прогресу задаватимуть контекст необхідних заходів в інших проблемних сферах світового устрою.

Отже, велика потенційність розвитку технологій водночас є і великою непередбачуваністю реалізації нових спроможностей. Технології в сьогоденні та майбутній перспективі визначаються як основа глобалізації різних сфер суспільного буття, як ефективний інструмент, та змінюють звичні підходи до вирішення типових проблем, створюють нові, здатні як стабілізувати, так і дестабілізувати будь-яку зі сфер суспільного буття. Однак загальний їх вплив можна визначити як каталізуючий, оскільки вони сприяють утворенню глобального інформаційного суспільства, розширенню та поглибленню світового інформаційного простору, трансформації інформаційної безпеки з секторної до наскрізної.

Політичні чинники визначають зміни політичної конфігурації світового устрою. Статус відносин між великими державами, зміщуючись в діапазоні співпраця-суперництво, може задавати зовсім різні конфігурації світового устрою. Світові тенденції передбачають більший розподіл відносних сил між великими державами. Якщо тенденція до більшого розподілу сил збережеться, то США

будуть одним з основних гравців у міжнародній системі за новою моделлю, хоча їх верховенство буде дедалі більше підриватися піднесенням інших великих держав, насамперед КНР. В майбутньому США очікувано матиме ключовий вплив на глобальну стратегію та світову політику. США традиційно покладатимуться на охопленість фінансових ринків, технологічну перевагу, наукові дослідження, розмір ресурсів, розвиненість збройних сил. При цьому влада величезних корпорації та технологічних гігантів може зрости до такого рівня, що вони потенційно конкуруватимуть зі структурами державного управління (Global Strategic Trends: Out to 2055, 2024).

Очікується, що КНР стане провідною економікою світу, якщо зможе перетворити економічну міць на військову міць (ESPAS, 2024). КНР ймовірно намагатиметься розширити свою систему військових баз для захисту своїх економічних інвестицій і доступу до світових торгівельних шляхів. Глобальна стратегія КНР спрямована на обмеження зон впливу конкурентів, контроль інформаційного простору. Використання економіки взаємозалежності, підкріпленої військовою силою, є основним засобом досягнення стратегічних цілей. Великі економічні інвестиції та торгові ініціативи КНР спрямовані на посилення цієї економічної інтеграції. Рівень розвитку технологій може надати КНР можливість відігравати провідну роль у встановленні стандартів і регулюванні світового інформаційного простору через «розумні міста», техніку, впливові ігри, кіноіндустрію тощо.

Індія має стати ще одним великим гравцем, у 2045 році витрати Індії на оборону можуть перевищити витрати всієї Європи (Jordan, 2017). Щодо Російської Федерації, то незалежно від того, виживе нинішній режим чи ні, майбутні російські лідери ймовірні докладатимуть всіх зусиль для відновлення сили та позицій РФ в міжнародній системі. Відновлення може посилити залежність від підтримки з боку КНР, Індії, Ірану, за таких умов вона може бути включена в китайську сферу впливу, що стане серйозним викликом для глобальної стабільності. Війна між великими державами є можливою, гострі форми вирішення наявних протиріч можуть виявлятися в збройних конфліктах у відповідних регіонах, занепадом

великих держав та утворенням нових міжнародних об'єднань. В будь-якому випадку наслідки таких подій будуть відчутними на рівні світового устрою. Воєнний конфлікт між Сполученими Штатами та КНР в Азійсько-Тихоокеанському регіоні потенційно дестабілізує світову економіку та глобальну безпеку. Розпад Російської Федерації з діленням зон впливу відокремленими державами та намаганням втримати найбільшу владу з потенційним застосуванням атомної зброї створить ризик суттєвих кліматичних та екологічних зміни. Економічна взаємозалежність стримує агресивну поведінку великих держав, однак може використовуватися для спекуляцій і не убезпечує від прямого збройного конфлікту. Геополітична конкуренції наразі виявляється через кризи, військову ескалацію в регіонах перетину владних інтересів (Східна Європа, Азійсько-Тихоокеанський регіон тощо). Посилення суперництва між великими державами сприятиме обмеженню функціонування системи безпеки через більш часте використання права вето в Раді Безпеки ООН, тим самим ускладнюючи функціонування системи безпеки (Global Trends 2040: a more contested world, 2021).

«Середні» держави до 2055 року очікувано матимуть здатність впливати на глобальний баланс сил на основі поєднання міжнародної політики, системи правового забезпечення, економічного впливу та військових ресурсів. Глобальна правова та нормативна база при дотримуванні країнами своїх міжнародних юридичних зобов'язань є потужним стримуючим фактором навіть для великих впливових країн, хоча війна РФ та України продемонструвала, що їхня імплементація може бути дуже контекстуальною. Ескалація глобальної конкуренції за енергетику ще більше похитне ефективність та підтримку глобальних інституцій. Великі держави можуть ставати все більш вибірковими, дистанціюючись від невигідних для них реформ, відходячи від дотримання договорів. Стабільність та визначеність світового устрою може похитнутися через прихильність до неофіційних умовних домовленостей. Очікуваним в таких умовах є утворення вибіркових політичних альянсів. Як альтернатива, може спостерігатися зростання конкуренції між державами, створюючи більш складну глобальну динаміку (Global Strategic Trends: Out to 2055, 2024).

На протилежність великим державам існують слабкі, що є більш залежними і керованими, цілісність їхніх територій знаходиться в зоні ризику та більшою мірою залежить від активності посягань країн-агресорів та підтримки зі сторони великих держав, розподілу їхніх зон впливу. Високий рівень корупції, слабкі інститути управління, обмеженість демократичних свобод обмежуватимуть конкурентноспроможність в глобальній економіці та сприятимуть зростаючому невдоволенню та внутрішній нестабільності. При зміщенні відносин між великими державами в сторону конфронтації саме такі держави можуть стати ареною опосередкованої війни в регіонах суперечності інтересів, як збройна агресія Російської Федерації проти України, зміст якої виходить далеко за межі декларованого агресором. Разом з тим, у прямих або опосередкованих збройних конфліктах продовжуватиметься використання гібридних стратегій, з розвитком технологій використання світового інформаційного простору буде посилюватися. Технології є основою військового потенціалу, а наявність глобалізованого інформаційного простору збільшує потужність транснаціонального впливу застосовуваної тактики. Ворожі дії в сірій зоні між миром і війною ускладнюють міжнародне врегулювання криз, оскільки вони підривають ефективність традиційних інструментів, таких як дипломатія і стримування (Jordan, 2022).

До політичних чинників належить також поява впливових недержавних акторів. Недержавні організації як альтернатива державним установам матимуть значущий вплив на громадську думку, особливо за умови недостатності державних ресурсів для вирішення наявних проблем (Андрєєва & Бовкунович, 2021). Терористичні організації та інші впливові недержавні актори можуть мати збільшення можливостей впливу через технологічний прогрес. Світовий інформаційний простір надає нову арену для терористичної і злочинної діяльності. Технології, пов’язані з віртуальною товариськістю, соціальні мережі, можуть слугувати основою для організації та поширення соціальних протестів, які виходять за межі геополітичних кордонів організатора. Державні та недержавні суб’єкти можуть використовувати їх для оцінювання вираженості та предметності соціального невдоволення в своїй країні і в країні-конкуренті, а потім

використовувати їх при застосуванні механізмів соціальної атрибуції, контрастного соціального порівняння тощо. Наприклад, націоналізм використовуваний для консолідації автократичного уряду Російської Федерації, є ідеологічною основою збройної агресії проти України. Один і той же суспільний атрибут одночасно використовується в наративах в контрастно позитивному та негативному забарвленні.

Недержавні організації чи нерегулярні напіввійськові, кримінальні формування невизначеної належності можуть використовуватися для реалізації завдань блокування, захоплення державних і військових установ, протидії заходам офіційних органів влади. Подібні формування можуть комплектуватися з місцевого населення, представників спеціальних підрозділів чи злочинних угруповань. При використанні такого зовнішнього ресурсу силових впливів реальний агресор може використовувати власні регулярні збройні сили для тиску під виглядом проведення військових навчань, забезпечення контролю над своїми прикордонними територіями, захисту власного населення під виглядом антитерористичних, миротворчих чи стабілізаційних операцій (Дмитрук, 2019). Можлива поява нових насильницьких ідеологій через контрастуючі відмінності при зштовхуванні різних культур (Global Trends 2040: a more contested world, 2021). Етичні відмінності щодо можливості використання певних технологій сприятимуть більш легкому їх впровадженню та розвитку в менш демократизованих країнах. Хоча оснащеність армії все ще залежатиме від економічної потужності держави, однак вона матиме тенденцію до зменшення, зважаючи на очікувано більшу гнучкість та стратегічну інноваційність недержавних супротивників. Їхня діяльність як пряма загроза національній та міжнародній безпеці посилить потребу в вирішенні питань міжнародної безпеки в інформаційному просторі, що матиме очікувано модераційний вплив. Отже, його активація зумовлюється появою нових недержавних акторів світового інформаційного простору та необхідністю консолідації зусиль в забезпеченні міжнародної безпеки з дотриманням встановлених правил, домовленостей та вимог міжнародною спільнотою.

Наразі фактично лише на національному рівні можливим є встановлення регуляторів інформаційного простору як зобов'язань та заборон в інформаційній сфері, наприклад, КНР має свій внутрішній регульований інформаційний простір таким чином захищений від зовнішніх впливів та загроз. Відносини в глобальній мережі Інтернет не мають уніфікованих обов'язкових міжнародно-правових стандартів, засади їхньої регламентації кожна держава може визначати на внутрішньодержавному рівні (Шемчук, 2019).

Отже, політичні чинники мають здебільшого ретардаційний вплив на глобалізаційні процеси, оскільки класичний світоустрій з геополітичними кордонами, національним суверенітетом суперечить уніфікації та інтеграції, а веде до нової конфігурації політичних відносин. З розростанням та збільшенням значущості світового інформаційного простору як продукту глобалізації все більшої актуальності набуває забезпечення саме інформаційного суверенітету держави та відповідно інформаційної безпеки. Однак в умовах глобалізації саме ці чинники можуть мати модераційний вплив, оскільки високі темпи інформаційного розвитку розширюють розуміння інформаційної складової національної безпеки до всезагальної міжнародної безпеки. З посиленням глобалізаційних процесів інформаційна безпека не може забезпечуватися ефективно лише державою, а вимагає узгодженої дії всієї світової спільноти.

Таким чином, вплив світових чинників глобалізації, повнота реалізації її тенденцій можуть в поєднанні зумовлювати специфічність ландшафту поширення глобалізації, посилюючи, стримуючи, контролюючи, зумовлюючи її позитивні чи негативні ефекти. При цьому базові тренди реалізуються в площині ключових невизначеностей, які стосуються особливостей впливу та взаємодії світових чинників глобалізації. Демографічні та технологічні чинники в цілому мають каталізуючий вплив на глобалізаційні процеси, політичні чинники – ретардаційний вплив, однак при актуалізації міжнародної небезпеки в інформаційному просторі матимуть очікувано модераційний вплив. Екологічні чинники мають медіаційний вплив. Швидкість і масштаби зміни клімату, ступінь співпраця чи суперництво між великими державами, технологічний прогрес у галузі штучного інтелекту,

економічні кризи у взаємозалежному світі, діяльність глобальної терористичної організації, демографічний дисбаланс населення економічно розвинених держав – всі ці зміни можуть мати різну інтенсивність впливу залежно від конкретних подій. Кожен чинник визначає загрози та виклики інформаційній безпеці через вплив на глобалізацію, проявом якої є світовий інформаційний простір, який реагує на особливості глобалізаційних процесів. Серед таких глобальних загроз та викликів можна виділити: суперництво між великими державами; озброєння недержавних суб'єктів, посилених новими технологіями; глобальну конкуренцію за природні ресурси; великі демографічні дисбаланси та міграційні потоки; стрімкий розвиток технологій; економічну взаємозалежність різних країн. Таким чином, в умовах посилення масштабності та інтенсивності глобалізації при актуалізації визначених тенденції в розвитку інформаційної сфери інформаційної безпеки набуватиме все більшого не секторального, а наскрізного значення для національної безпеки держави.

Світовий інформаційний простір став стратегічно важливою зоною впливу та одним з пріоритетних напрямів національної та міжнародної безпеки. Розбудова системи інформаційної безпеки має враховувати особливості світового інформаційного простору та стрімкий розвиток інформаційних технологій, таких як штучний інтелект, що дасть змогу створити систему конгруентну об'єкту моніторингу, впливу та прогнозування. В умовах глобалізації інформаційного простору та тотальної цифровізації виникає проблема суб'єктності. Хто є актором інформаційного простору як щодо продукування інформації, так і реагування на її появу та наслідки? Чи можемо ми обмежуватись фізичним суб'єктом, чи організацією? Використання штучного інтелекту як аналітичного алгоритму щодо виявлення загроз та прийняття рішень, як генератора інформаційних повідомлень різної модальності вимагає переосмислення традиційного розуміння суб'єктності в контексті інформаційної безпеки національного та міжнародного масштабу.

З даної проблематики можна відзначити дослідження етичних проблем використання штучного інтелекту J. Wu et al. (2024), факторів формування державної системи інформаційної безпеки S. Hlobenko (2023), моделей

кібербезпеки K. Buhaichuk et al. (2023), глобального інформаційного простору як інфраструктурного середовища та чинника актуалізації інформаційної безпеки держави Y. Chmyr et al. (2023), штучного інтелекту як інструмента державного управляння інформаційною безпекою V. Bondar (2023), критеріїв достатності інформаційної безпеки O. Bortnikova et al. (2024), загроз в інформаційному просторі для національної безпеки та стратегій протидії V. Ievdokymov et al. (2024), штучного інтелекту як інструменту інформаційної безпеки T. Hovorushchenko et al. (2024), R. Upreti et al. (2024), A. Zacharis et al. (2024), феномена глобалізації та її концептуальних засад Б. Юськів (2009), правових проблем захисту інформаційного простору в умовах збройних конфліктів H. Lahmann (2020), технологічного забезпечення виявлення інформаційних загроз D. Schlette et al. (2021), проблем формування ситуаційної обізнаності у військовій сфері F. Skopik et al. (2022).

На основі аналізу даних наукових доробків можна зробити висновок, що забезпечення інформаційної безпеки є проблемною областю з високим ступенем невизначеності: висока варіативність та різнорідність впливаючих факторів (Hlobenko, 2023), масштабування загроз та різнорівневість їхніх наслідків від національної безпеки до поширення тривожних та депресивних станів у суспільстві (Buhaichuk et al., 2023), зростаюча технологічна складність загроз (Ievdokymov et al., 2024), швидкість появи нових технологій та проблема розробки систем виявлення загроз (Schlette et al., 2021), інституційна суперечливість (Chmyr et al., 2023), зростаюча кількість інформації та її джерел (Skopik et al., 2022), проблеми правового регулювання (Lahmann, 2020). Штучний інтелект, як і будь-яка технологія, є нейтральною за своєю природою, однак залежно від контексту використання вона може бути як джерелом загроз, так й інструментом протидії. Як інструмент, системи штучного інтелекту мають відповідати усталеним етичним нормам та мати правове підґрунтя (Wu et al., 2024), бути безпечними, якісними (Ievdokymov et al., 2024), захищеними технологічно та соціально (Bondar, 2023). В такому контексті аналіз інтеграційних можливостей штучного інтелекту через призму особливостей інформаційного простору потенційно може бути шляхом до зменшення невизначеності, підвищення швидкості та пластичності систем

інформаційної безпеки в динамічних світових умовах. Використання штучного інтелекту може посилити конгруентність систем інформаційної безпеки тенденціям світового інформаційного простору.

Якщо розглянути принципи, яким має відповідати формування системи інформаційної безпеки, то в практичній реалізації кожного з них буде актуалізовуватися зона невизначеності, що може стати тіньовим коридором для злочинної діяльності, конфліктогенних впливів чи владної переваги. Концептуально розбудова системи інформаційної безпеки має відповідати даним принципам, які визначають її формально-процесуальні особливості, змістове ж наповнення має спиратися на сформовану політику інформаційної безпеки та державну стратегію її реалізації. До таких принципів належать:

1. Принцип законності передбачає розробку системи інформаційної безпеки на основі чинного законодавства та нормативно-правової бази, що регулює як національний інформаційний сектор, так і міжнародні відносини (Bortnikova et al., 2024). Однак динамічність та пластичність світового інформаційного простору потребує трансформації звичних інституцій та структур, що актуалізує потребу в інституційних інноваціях, які можуть суперечити усталеним правовим засновкам та управлінським структурам (Юськів, 2009). Правове регулювання в такому випадку має сліпі зони через недостатню адаптивність.

2. Принцип верховенства норм міжнародного права передбачає пряме застосування міжнародних норм та стандартів без національних правових обмежень в забезпеченні інформаційної безпеки (Bortnikova et al., 2024). Однак існує ризик юрисдикційних розбіжностей, що ускладнює створення єдиного міжнародного правового поля (Lahmann, 2020). Ці розбіжності можуть мати глибинні культурні чи релігійні засновки, наприклад, в регулюванні питань цензури, приватності.

3. Принцип права власності передбачає забезпечення права суб'єкта на інформацію, що регулюється чинними нормативно-правовими актами (Bortnikova et al., 2024). Проблемою в межах реалізації даного принципу є регулювання обміну інформацією між іноземними партнерами щодо об'єктів права власності,

використання програмного забезпечення іноземного походження, розташування хмарних сховищ та серверів.

4. Принцип економічної доцільності систем захисту інформації ґрунтується на заходах і необхідності збереження таємниці та конфіденційності інформації, пов'язаної з власністю споживача (Bortnikova et al., 2024). Зважаючи на швидкість поширення інформації, використання штучного інтелекту для продукування дезінформації, розширення поля потенційної суб’єктності та домінуючі цінності в суспільстві, величина економічних витрат та масштабність покриття є дискусійним питанням.

5. Принцип об’єктивності в оцінці реальних та потенційних загроз інформаційній безпеці, стану нормативно-правової та організаційної бази, а також реальних можливостей використання матеріально-технічних, людських та фінансових ресурсів (Bortnikova et al., 2024). Основою реалізації є цілісність сприймання інфраструктурного середовища та моделі інформаційної безпеки, що має враховувати глибинний аналіз національного та світового інформаційного простору.

6. Принцип безперервності забезпечення інформаційної безпеки полягає в постійному моніторингу безпекової ситуації в інформаційному секторі з супутнім застосуванням загальних та специфічних заходів реагування на виявлені загрози (Bortnikova et al., 2024). Це потребує високої адаптивності, оскільки швидкий розвиток інформаційних технології потребує відповідного реагування на появу нових загроз.

О. Bortnikova et al. (2024) пропонує такі критерії достатності державного регулювання для реалізації політики інформаційної безпеки:

1) визначення національних зовнішніх і внутрішніх політичних інтересів в умовах глобалізації світових відносин;

2) правосвідомість членів суспільства;

3) формулювання параметрів моделі інформаційного розвитку з врахуванням національних інтересів та ресурсів інформаційної безпеки;

4) визначення пріоритетів і сфери виключно державного регулювання інформаційного, інтелектуального і технологічного розвитку в рамках обраної національної моделі.

Дані критерії визначаються дискусійними, оскільки держава є обмеженою в повноті їхньої реалізації, наприклад, виступаючи гарантом прав та свобод населення, або ж у разі інформаційної війни, в протидії якій не можна обмежитися лише національними ресурсами. Виявленні обмеження визначаються специфікою національного інформаційного простору в умовах глобалізації, однією з актуальних тенденцій якого є масштабування загроз інформаційній безпеці.

K. Buhaichuk et al. (2023) виділяє емпіричним шляхом ієрархічну структуру чинників масштабування загроз інформаційній безпеці, наведено в табл. 1.1.

Таблиця 1.1

Впливовість чинників масштабування загроз інформаційній безпеці

Ранг	Чинники	Зміст
1	Освітньо-кваліфікаційні	освіченість та інформованість населення щодо загроз та заходів інформаційної безпеки
2	Психологічні	психологічна готовність до глобальних викликів та стресостійкість
3	Національно-політичні	визначення механізмів інформаційної безпеки як елементу захисту національних інтересів як держави в цілому, так і окремого громадянина
4	Техніко-технологічні	наявність інструментів, механізмів, ресурсів забезпечення інформаційної безпеки
5	Нормативно-правові	наявність ефективних механізмів правового регулювання інформаційної безпеки
6	Соціально-економічні	рівень життя, доходів населення

Джерело: сформовано автором на основі дослідження K. Buhaichuk et al. (2023).

Оцінка впливовості чинників масштабування загроз узгоджується з критеріями достатності державного регулювання для реалізації політики інформаційної безпеки. Кожен з критеріїв позначається впливом якогось з чинників масштабування загроз інформаційній безпеці, що безумовно детермінує проблемність адаптивності державного регулювання до динамічності світового інформаційного простору. Наприклад, правосвідомість членів суспільства залежить від освіченості, інформованості населення, психологічної готовності різних вікових груп та відповідного правового забезпечення, активності просвітницької роботи. При цьому освітньо-кваліфікаційні чинники визначаються найпершими по впливовості на масштабування загроз інформаційної безпеки. Стрімкий розвиток технологій формує дедалі зростаючий розрив між поколіннями. Відсутність відповідного технологічним змінам інформування про заходи безпеки та надання доступу до засобів безпеки утворюють нерівномірність в підготовленості населення до динамічних змін світового інформаційного простору залежно від рівня економічного розвитку країни. Підвищення освіченості населення сприяє не лише використанню засобів захисту персональних даних, розумінню загроз, відповідальній поведінці в цифровому просторі, а й зростанню кількості суб’єктів спроможних використовувати технологічні можливості сучасності задля забезпечення персональних потреб на межі моральних та правових норм. Введення освітніх короткострокових програм, курсів, інструктажів на робочому місці щодо заходів інформаційної безпеки дозволить стримати масштабування загроз.

Технології стрімко розвиваються, визначаючи як нові загрози, так і нові можливості захисту. Швидке зростання генеративного програмного забезпечення на основі штучного інтелекту ускладнює загальний технологічний ландшафт розгортання системи інформаційної безпеки. При цьому збільшення кількості користувачів, залучених до інформаційних процесів, підвищує інтенсивність впливу та масштабність. Поняття суб’єктності розширюється, а геополітичні кордони стають умовністю. Суб’єкт може бути фізичною особою, організацією або псевдосуб’єктом. Тип суб’єкта щодо властивостей (легкість входження,

технологічність, ступінь довіри тощо) та щодо можливостей впливу визначає рівень його складності чи то в контексті інформаційної, чи кібернетичної, чи апаратно-програмної загрози. Суб'єктність розглядається і в контексті потенційних загроз, і в контексті управління інформаційною безпекою. Поява штучного інтелекту вводить дуальність в технологічність інформаційного простору як загрози та захисту. Штучний інтелект, як трансформаційна технологія, розширює поняття суб'єктності, удосконалює людські можливості та змінює масштабність загроз (Дубовський, 2024c). Технологічна розвиненість інформаційної сфери породжує проблему реверсивності суб'єктності в інформаційному просторі, що полягає в можливості трансформації, зникнення, спростування суб'єктності. Кожен користувач є потенційно суб'єктом інформаційного впливу, генеруючи відповідний контент, однак і є об'єктом впливу прихованих алгоритмів, сторонньої активності, інформаційних фільтрів та моделей відбору контенту (Андрєєва & Бовкунович, 2021). Суб'єктність стає результатом динамічної взаємодії потоків інформації. Ця двосторонність посилюється ще й появою псевдосуб'єктів, втратою першоджерела або його прихованістю через опосередкований вплив, що формує основу для активних інформаційних впливів поза зоною відповідальності та зазначення істинного авторства інформації при використанні її як зброї в отриманні стратегічних переваг на міжнародній арені.

Виникає необхідність переходу від моделі реагування до проактивного передбачення. Створення базової уніфікованої системи ризиків на основі наукової методології дозволяє розробити цільові прогностичні моделі, однак ця система потребує постійного оновлення. Таке оновлення має бути засноване на співпраці як національного, так і міжнародного масштабу. Співпраця, заснована на обміні наявними даними про загрози за допомогою відповідних платформ, допомагає поширювати знання про поточні загрози. Мета впливу часто має широку суспільну охопленість. Визначення такого типу загроз пов'язане з формуванням ситуаційної обізнаності, яку можна визначити як особливості сприймання елемента в часі та просторі з розумінням його значення та прогнозуванням його статусу в найближчому майбутньому (Skopik et al., 2022). Такого виду платформи є основою

для кластерізації загроз термінального характеру або процесуальних загроз з встановленими кінцевими негативними ефектами. Вони стосуються більшою мірою кіберпростору. Однак модель інформаційної безпеки має бути ширшою та враховувати загрози з відстроченими негативними ефектами, що часто ґрунтуються на дезінформації, діпфейках, маніпуляціях тощо.

Однак відповідні формати часто є складними та великими, що призводить до недостатньої читабельності для експертів у галузі інформаційної безпеки. Для їхньої ефективної роботи необхідна репрезентативна узгодженість, надійність джерела походження даних, достовірність самого набору даних та достатній обсяг даних. Проблеми швидкості впровадження заходів у відповідь на актуальні загрози, моніторингу індикаторів загроз, дублювання даних, контролю якості платформ обміну даними зводяться до визначальної впливовості людського фактору (Schlette et al., 2021).

Ситуаційну обізнаність можна розглядати на оперативному, тактичному та стратегічному рівнях (Skopik et al., 2022). Кожен з них має свої специфічні завдання, цілі та методи реалізації. Ситуаційна обізнаність стратегічного рівня передбачає аналіз світового інформаційного простору через призму державних інтересів, міжнародного становища, національної безпеки, реалізації довгострокових стратегій. Оперативний рівень ситуаційної обізнаності передбачає аналіз інформаційних одиниць внутрішньодержавного управління в різних сферах та реалізації конкретних програм, стратегічних напрямів, ініціатив, реформ. Тактичний рівень ситуаційної обізнаності стосується локальних подій, проєктів, персоналій.

Ситуаційна обізнаність є основою управління інформаційною безпекою, однією зі складових прийняття рішень. Стратегічне управління передбачає формування політики інформаційної безпеки. Тактичне управління передбачає розробку та впровадження системи інформаційної безпеки відповідно до вимог політики. Оперативне управління включає підтримку та моніторинг виконання політик інформаційної безпеки (White, 2009).

Криза поширення дезінформації, яку часто називають «інфодемією», впливає на ситуаційну обізнаність кожного з рівнів. Орієнтація в складному ландшафті дезінформації, позначеного багатосуб'єктністю світового інформаційного простору, передбачає аналіз великих обсягів інформації. Циклічний зв'язок між довірою, інформацією та комунікацією передбачає синхронне управління цими елементами для ефективного управління інформаційною безпекою. Вседозволеність у ЗМІ, як наслідок, некомпетентне поширення інформації та дезінформація вимагають регулювання як на юридичному рівні з передбаченням адміністративної та кримінальної відповідальності, так і на технологічному рівні, зокрема з використанням штучного інтелекту (Pipchenko & Darnytskyi, 2024). Людські ресурси є обмеженими щодо швидкості реалізації такого формату завдань. Ситуаційна обізнаність передбачає також об'єктивність, цілісність, повноту даних через збирання інформації, перевірку, співвідношення, видалення дублікатів, збагачення, що засноване на аналізі великого об'єму даних. Технологічним рішенням забезпечення ситуаційної обізнаності відповідної такому переліку критеріїв може бути застосування штучного інтелекту.

Алгоритми штучного інтелекту із застосуваннями методів розвідки з відкритим кодом (OSINT) ефективно опрацьовують безперервні потоки нефільтрованої інформації. Інформація, отримана із загальнодоступних джерел, становить 80-90% основи усієї розвідувальної діяльності, що визначає зміст ситуаційної обізнаності. Контрольоване машинне навчання дозволяє вивчати залежності змінних із санкціонованої сукупності даних, щоб ідентифікувати схожі шаблони в невидимих даних (Ghioni et al., 2023). Штучний інтелект та машинне навчання все частіше залучається як інструмент забезпечення інформаційної безпеки, оскільки надають можливість обробляти величезну кількість даних, виявляти закономірності та порушення, а також розробляти оперативні та точні рішення, що виходять за межі людських здібностей. Наприклад, штучний інтелект використовується для прогнозування загроз та їхніх наслідків. Такий автоматизований аналіз і прогнозування можуть точніше симулювати реальні сценарії та оцінювати здатність систем інформаційної безпеки реагувати на нові

загрози. Керована штучним інтелектом методологія аналізу загроз точніше визначає поточні та нові тенденції з їхнім потенційним впливом у різних секторах із будь-якого набору даних (Zacharis et al., 2024).

Використання штучного інтелекту в критично важливих програмах, таких як державне управління, автономна зброя, судова система, охорона здоров'я тощо, має спиратися на математично перевірену або підтверджену різними видами тестів, безпечну модель. Надійність рішень штучного інтелекту можна перевірити як технічно, так і соціально (High-Level Expert Group on Artificial Intelligence of the European Commission. Ethics guidelines for trustworthy AI, 2019). Відсутність упередженості рішень на основі штучного інтелекту засновується на достатній кількості даних, чим більше даних є основою для навчання, тим надійнішою є модель. Дефіцит даних чи їхня обмеженість в певному аспекті сприяє викривленню моделі.

Незважаючи на експоненціальне впровадження рішень на основі штучного інтелекту, дослідження виявляють вразливості безпеки та конфіденційності, пов'язані з системами штучного інтелекту (Upreti et al., 2024). Моделі штучного інтелекту не мають позбуватися свого людського компоненту, повинні бути розроблені «спільні когнітивні системи» для досягнення оптимального балансу між аналітиками та алгоритмами (Ghioni et al., 2023). Кожна система, яка працює в цьому світі, підпадає під дію певних правил і законів, і штучний інтелект не є винятком. Існують різні види правил і законів, створених Європейським Союзом та іншими відповідальними установами на національному та міжнародному рівнях. Компанії повинні враховувати ці закони при розробці, розгортанні та використанні систем штучного інтелекту. Розробка рішення за визначеними законами допомагає підтримувати надійний штучний інтелект. Однак не все можна охопити законами в умовах динамічності технологічної сфери, тому окреслюють етичну перспективу (Upreti et al., 2024).

Концепція етичного штучного інтелекту передбачає (High-Level Expert Group on Artificial Intelligence of the European Commission. Ethics guidelines for trustworthy AI, 2019):

- Повагу до людської автономії. Системи штучного інтелекту завжди повинні розроблятися на основі принципів проектування, орієнтованих на людину, щоб доповнювати та розширювати людські когнітивні, соціальні та культурні навички.
- Безпеку та захищеність. Система не повинна завдавати, посилювати шкоду людям та бути відкритою для будь-якого виду зловмисного використання.
- Конфіденційність. У сучасному цифровому світі конфіденційність користувачів стала серйозною проблемою, зловмисники використовують різні методи, такі як змагальні атаки, атаки на визначення членства та зв'язування даних, щоб розкрити інформацію користувачів із рішень штучного інтелекту.
- Справедливість. Рішення штучного інтелекту не повинні бути упередженими, дискримінаційними чи стигматизованими щодо окремої людини чи групи людей. Справедливість також стосується свободи вибору, наданої користувачам, щоб вирішити, чи можуть бути використані їхні дані в системах на основі штучного інтелекту, з можливістю відмови з часом в разі наданої згоди.
- Підзвітність. Опис всіх етапів від розробки до розгортання системи штучного інтелекту з зазначенням можливих негативних ефектів алгоритму.
- Зрозумілість. Створення інструментів для пояснення причин рішень моделі штучного інтелекту, наприклад, використання ігри, щоб визначити внесок кожної функції в рішення та надати пояснення за допомогою візуалізації та природної мови. Це допомагає зміцнити довіру користувачів.
- Прозорість. Доступність інформації про архітектуру моделі, функції кожного рівня, статистику навчання, дані, які використовуються, тощо.

Використання штучного інтелекту, як і будь-якої технології, має регулюватися правилами. Впровадження моделей надійного та етичного штучного інтелекту дозволяє мінімізувати потенційні ризики, збільшити довіру суспільства та зменшити невизначеність. Системи штучного інтелекту мають інтеграційні можливості забезпечення відповідності систем інформаційної безпеки особливостям інформаційного простору. Використання штучного інтелекту сприятиме більш повному розгортанню системи інформаційної безпеки. Завдяки синергетичним ефектам, характерним для інформаційного простору, розвиток

моделі інформаційної безпеки сприятиме розвитку систем штучного інтелекту, а використання штучного інтелекту підвищить ефективність інформаційної безпеки. Як технологія дії та протидії, штучний інтелект дозволяє підвищити об'єктивність, швидкість формування та повноту ситуаційної обізнаності. Ефективність використання моделей штучного інтелекту залежить від збереженості людського компоненту, розробка «спільних когнітивних систем» є оптимальним балансом між аналітиками та алгоритмами (Дубовський, 2024с).

Отже, отримані узагальнення поглиблюють дослідження проблеми забезпечення інформаційної безпеки з точки зору методологічних основ, феноменології та концептуальної розробленості, оскільки принципи, критерії, чинники інформаційної безпеки розглядаються через призму особливостей глобалізованого інформаційного простору. Світовий інформаційний простір є об'єктом інформаційної безпеки, оскільки він охоплює глобальні інформаційні потоки, цифрові платформи, мережі передачі даних тощо. В умовах глобалізації інформаційна безпеки трансформується відповідно до світових тенденцій, реагуючи на появу нових викликів та загроз. Дієвість каталізуючих глобалізацію технологічних чинників в різних сферах суспільного буття інтенсифікує розростання та поглиблює важливість інформаційного простору. Вплив розвитку інформаційних технологій на розвиток інформаційного простору передбачає й необхідність відповідного технологічного забезпечення інформаційної безпеки, зокрема використання технологій штучного інтелекту. Складність та проблемність забезпечення інформаційної безпеки в таких умовах виявляється в неконгруентності її моделі особливостям світового інформаційного простору. Ефективність системи інформаційної безпеки залежить від її адаптивності та оперативності, що передбачає врахування при її розробці відповідності природі простору її функціонування та його особливостям, тобто інформаційного простору. Врахування даних особливостей сприятиме зменшенню невизначеності систем інформаційної безпеки та перегляду усталених принципів їхньої розробки щодо відповідності актуальним умовам зростаючої цифровізації світу.

Висновки до Розділу 1

Задля забезпечення повноти реалізації мети дослідження було проаналізовано основоположні концепції теоретичного осмислення інформаційної безпеки, що дозволило визначити теорію соціотехнічних систем як основу інтеграції техніко-технологічного та соціально-психологічного аспектів забезпечення інформаційної безпеки в умовах глобалізації інформаційного простору. Ключовими для дисертаційної роботи визначено положення, що: інформаційний простір є середовищем життєдіяльності соціотехнічних систем; захищеність соціотехнічних систем є результатом ефективності реагування системи інформаційної безпеки на загрози середовища їхнього функціонування; визначення достатності інформаційної безпеки та цінності інформації характеризується суб'єктивністю; інформаційна безпека має індивідуальний, загальний та захисний рівні функціонування; управління інформаційним простором як механізм забезпечення інформаційної безпеки відповідає захисному рівню її функціонування.

Методологічне підґрунтя дослідження складає феноменологічний підхід, відповідно до якого інформаційна безпека визначається як предметність вищого порядку, що як елемент справжньої дійсності визначає життя суспільства. Конституювання інформаційної безпеки веде до конституювання просторових речевостей та психічних суб'єктів, що відповідає визначанню інформаційного простору об'єктом інформаційної безпеки та узгоджується з положеннями теорії соціотехнічних систем.

В результаті аналізу визначень інформаційної безпеки встановлено, що дане поняття є багатоаспектним як з точки зору понятєвого статусу, так і цільового, контекстуального, часового. Інформаційну безпеку можна розглядати як в статичному, так і в динамічну аспекті. Вона визначається як стан, процес чи умова в площині функціонування чи окремої системи забезпечення, системи суспільних відносин, чи суверенітету держави, національних інтересів, національної безпеки, чи інформаційного простору та інформаційної сфери в цілому. Відповідно до

теоретико-методологічних засад дисертаційної роботи інформаційна безпека є об'єктно-суб'єктним феноменом, що визначає умови функціонування суб'єктів в інформаційному просторі, конституйованому глобалізацією.

Світовий інформаційний простір є індикатором глобалізації. Глобалізація інформаційного простору реалізується через інтегруючі зміни різних сфер суспільного буття, інтенсифікуючі зміни обміну інформацією та трансформуючі зміни значущості традиційних ресурсів. Визначено просторово-часові, трансформаційні, ефекторні та динамічні особливості світового інформаційного простору.

Актуальні тенденції розвитку світового інформаційного простору реалізовуються в контексті ключових невизначеностей, які стосуються особливостей впливу та взаємодії чинників глобалізації. Демографічні та технологічні чинники в цілому мають каталізуючий вплив на глобалізаційні процеси. Політичні чинники – ретардаційний вплив, однак при актуалізації міжнародної безпеки в інформаційному просторі – очікувано модераційний, екологічні – медіаційний. Кожен чинник безпосередньо чи опосередковано визначає загрози та виклики інформаційній безпеці, оскільки світовий інформаційний простір реагує на особливості глобалізаційних процесів. Інтенсивність та масштабність глобалізаційних процесів трансформують зміст інформаційної безпеки та її значущість для забезпечення національної та міжнародної безпеки. Демографічні чинники глобалізації опосередковано збільшують ризики та впливовість інформаційних загроз через розвиток мультинаціональних суспільств. Розвиток інформаційних технологій посилює значущість інформаційної безпеки для різних сфер суспільного буття, трансформуючи її з секторної в наскрізну, та визначає її технологічні можливості. Вплив екологічних чинників глобалізації на інформаційну безпеку опосередковано виявляється через актуалізацію питань контролю над спільним простором, до якого належить також інформаційний, через володіння ресурсами необхідними для розвитку інформаційних технологій, що визначають спроможності інформаційної безпеки. Політичні чинники впливають на визначення моделі інформаційної

безпеки, актуалізують змістовну значущість інформаційного суверенітету держави та інформаційної безпеки вже не як складової національної безпеки, а як її виду, що реалізується в інформаційній сфері.

Ефективність системи інформаційної безпеки в умовах глобалізації залежить від її адаптивності та оперативності, що передбачає врахування при її розробці відповідності природі простору її функціонування та його особливостям, тобто інформаційного простору. Інтеграційні можливості забезпечення такої відповідності мають технології штучного інтелекту, використання яких сприятиме більш повному розгортанню системи інформаційної безпеки.

РОЗДІЛ 2
ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: ЗАБЕЗПЕЧЕННЯ, ЗАГРОЗИ ТА ВИКЛИКИ

2.1. Глобальні та національні виклики та загрози інформаційній безпеці України

В умовах розвитку інформаційного суспільства та глобалізації інформаційна безпека стає підґрунтям стабільного функціонування різних сфер суспільного буття як окремої людини, держави, так і світового співтовариства в цілому. Визначення загроз та викликів є основою відповідного реагування та «забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина» (Указ Президента України №685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"», 2021).

Виклики являють собою тенденції, явища чи події, що визначають необхідність реалізації відповідних заходів локального та глобального масштабів, вимагають від людини, суспільства, держави адаптивних змін та нововведень. Вони є реалізацією спонукання до дії з метою забезпечення національної чи міжнародної безпеки. Загрозами є потенційні чи реальні явища, тенденції, чинники, що мають негативний вплив на людину, суспільство, державу та можуть завдати шкоди інтересам держави, її національній безпеці та обороні.

Оскільки інформаційна безпека України забезпечується шляхом захисту національного інформаційного простору від інформаційних загроз зі сторони інших держав, а також передбачає забезпечення розвитку інформаційного простору відповідно до світових тенденцій та особливостей інформаційного суспільства, що

сприятиме європейській та євроатлантичній інтеграції України, то аналіз тенденцій глобалізації, її інтенсивності та масштабності є важливими для визначення глобальних загроз інформаційній безпеці України.

В межах завдань національної та міжнародної безпеки саме негативні наслідки глобалізації зазвичай складають найбільший інтерес та викликають активні дії щодо попередження чи готовності до потенційних викликів та загроз. Чинники глобалізації мають різноспрямовані вектори впливу: чи то посилюючи, чи стримуючи, чи обмежуючи дію один одного. Їхній кумулятивний вплив визначає інтенсивність процесів глобалізації, що може мати локальні відмінності. Чим більшою є інтенсивність глобалізації, тим більш актуальними стають породжувані її негативними ефектами загрози, тим впливовішими є чинники масштабування загроз, що діють контекстуально. Світовий інформаційний простір набуває більшого інтеграційного навантаження, а інформація – більшої економічної та політичної вагомості. Відповідно достатній рівень інформаційної безпеки буде відрізнятися залежно від інтенсивності глобалізаційних процесів. Світовий інформаційний простір масштабується з розвитком інформаційних технологій, масштабуються разом з ним і загрози інформаційній безпеці.

Прогностична регресійна модель загроз інформаційній безпеці, представлена в дослідженні K. Buhaichuk et al. (2023), засвідчила подальше зростання масштабування загроз. На основі оцінки 200 респондентів, професійна діяльність яких стосується безпосередньо систем захисту інформації, було впорядковано за значимістю наслідки масштабування загроз інформаційній безпеці. Найбільшою сферою ураження експертами визначено національну безпеку, оскільки зростання інтенсивності інформаційних загроз проявляються як на рівні окремого громадянина, так і держави в цілому, наприклад, від захисту персональних даних до кібернетичних атак на об’єкти критичної інфраструктури, від блокування доступу до соціальних послуг до психологічного впливу на маси з метою викривлення суспільної думки та поширення конфліктогенних наративів. Результати ранжування наслідків масштабування загроз інформаційній безпеці наведено в табл. 2.1.

Таблиця 2.1

Ранжування наслідків масштабування загроз інформаційній безпеці

Ранг	Наслідки масштабування	Зміст
1	Національна безпека	вплив на захищеність населення та державної території
2	Фінансові та економічні	вплив на фінансові системи, підприємницьку діяльність, ділову поведінку тощо
3	Технічні та технологічні	вплив на техніко-технологічне забезпечення життєдіяльності населення
4	Соціальні	вплив на доступність соціальних послуг
5	Психологічні	вплив через збільшення невизначеності, фрустрацію потреб в безпеці та стабільності

Джерело: сформовано автором на основі дослідження K. Buhaichuk et al. (2023).

Серед визначених наслідків масштабування загроз найбільш значущими є впливи на захищеність державної території та населення. Суперництво між великими державами за перерозподіл зон впливу може реалізуватися протистоянням в зоні перетину інтересів. Використання при цьому гібридних сценаріїв сприяє анексії територій та порушенню суверенітету держав шляхом цілеспрямованих стратегічно вивірених впливів в інформаційному просторі. Поширення сепаратистських настроїв, наративів обмеження чи гноблення, маніпулювання фактами та поширення дезінформації дозволяє здійснювати зловмисні дії приховано та опосередковано. Через сприяння внутрішньодержавним конфліктам, громадянським війнам, революціям, що ґрунтуються на внутрішніх суперечностях в суспільстві, які посилюються та провокуються ззовні. Глобалізація таким чином може мати різні наслідки для різних країн, що можуть використовувати її можливості для реалізації власних інтересів при цьому

контролюючи її проникнення в стратегічно важливі сфери власного національного простору.

Розвиток глобалізації змінює як геополітичні інтереси держав, так і шляхи їхньої реалізації, тому процеси глобалізації – це не однонаправлений вектор посилення світової інтеграції, а складна система інтеграційних та дезінтеграціних тенденцій. Посилення чи стримування тенденцій глобалізації та породжуваних ними загроз визначається особливостями суспільно-політичних трансформацій, що визначають внутрішню політику геополітичних акторів системи світового порядку.

В Стратегії інформаційної безпеки України (Указ Президента України №685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"», 2021) визначено глобальні виклики та загрози, а саме :

1. «Збільшення кількості глобальних дезінформаційних кампаній». Використання світового інформаційного простору дозволяє діяти приховано та дистанційно як урядам конкуруючих країн, так і недержавним організаціям з метою реалізації своїх інтересів, впливаючи на суспільні настрої, світову громадську думку, маніпулюючи свідомістю мас. Інформація є пластичною мультизадачною зброєю, часом ефективнішою, ніж прямий воєнний конфлікт.

2. «Інформаційна політика Російської Федерації – загроза не лише для України, але й для інших демократичних держав». Світовий інформаційний простір дозволяє здійснювати вплив не лише локально, а й масштабувати локальні ефекти, підтримуючі зловмисні наративи глобальною поширеністю та опосередкованим підтвердженням. Інформаційні операції Російської Федерації не обмежуються лише однією зоною впливу в межах війни з Україною, вони в цілому спрямовані на реалізації більш глибоких питань щодо владної світової конфігурації, впливовості великих держав, розподілу зон впливу та конкуренції, а відтак є глобальною загрозою дистабілізації світового порядку.

3. «Соціальні мережі як суб’єкти впливу в інформаційному просторі». Глобалізація та пандемія COVID-19 сприяли посиленню віртуалізації соціальних відносин. В результаті соціальні мережі отримали значний приріст

розповсюдженості та впливовості. Швидке поширення інформації, розмивання кордонів приватності, висока транспарантність, проблеми етичності та нормативно-правового регулювання даного простору соціальних відносин свідчать про високий ступінь його невизначеності. Лідери думок, які отримують статус на основі кількісної підтримки, вподобань, відсутність контролю дезінформації сприяють викривленням сприймання, псевдоекспертизам, маніпулюванням та підміні статусів, понять, групових приналежностей.

4. «Недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій». Необхідність розвитку критичності сприймання та аналітичності мислення тільки зростає зі збільшенням об’ємів доступної інформації. Володіння основами індивідуальної інформаційної безпеки на загал дає приріст національній інформаційній безпеці. При цьому підготовленість населення залежить від освітньої та інформаційної політики держави, її економічної спроможності та плановості у введенні відповідних заходів. Обізнаність населення може забезпечуватися як формальними заходами, наприклад, освітні програми, тренінги, підвищення кваліфікації, так і неформальними, наприклад, лідері думок, референтні групи, Інтернет-контент.

Визначені загрози та виклики можна конкретизувати через тенденцію посилення цифровізації, оскільки інформаційна безпеки України, за визначенням Стратегії інформаційної безпеки, передбачає існування ефективної системи «захисту та протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом», а простором таких зловмисних дій в сучасному світі є саме цифровізований світовий інформаційний простір (Указ Президента України №447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"», 2021). Технологічні аспекти загроз національній безпеці України в інформаційній сфері зазначаються в Стратегії кібербезпеки України.

Відповідно з розвитком технологій штучного інтелекту зростання кількості глобальних дезінформаційних кампаній забезпечується генеративними можливостями технологічного забезпечення та швидкістю розповсюдження інформації. Створення новин, реалістичних зображень, відео, аудіо або тексту в поєднанні з технологіями машинного навчання для адаптації, вивчення та оптимізації стратегій впливу з врахуванням зворотного зв'язку та реакції від цільової системи або аудиторії (Admass et al., 2024) перетворюють такі кампанії на реальну загрозу, а їхнє зростання стає викликом для спроможності системи інформаційної безпеки ефективно діяти за тенденції подальшого посилення цифровізації та розвитку технологій в інформаційній сфері.

Відповідно інформаційні операції Російської Федерації, які синергетичні використовуваним гібридним стратегіям, передбачають спонсоровані інформаційні впливи зі сторони інших держав, лідерів думок з метою отримання економічних, політичних та стратегічних переваг; створення, підміну та викривлення інформації з метою впливу на критичну інфраструктуру та цільові значимі галузі, суспільство в цілому; кібератаки на державні та недержавні організації. Тенденції розвитку світового інформаційного простору свідчать про більшу значущість повідомлень про диверсії, за руйнування ними спричиненими (Jordan, 2024). Якщо диверсії, що передбачають фізичні руйнування, у розслідуваннях мають об'єктивну доказовість, то інформаційні впливи знаходяться наразі в сірій зоні як щодо доведення вини, так і притягнення до відповідальності. Проблема реверсивності суб'єктності в інформаційному просторі передбачає можливість трансформації, скасування суб'єктності, втрати джерела при відчутних ефектах впливу повідомленої інформації, наслідків, що мають значно меншу можливість відміни. Цим активно користується Російська Федерація в своїх інформаційних впливах, маючи дієві відпрацьовані стратегії заперечення власної причетності до подій як фізичного та цифрового світу. В умовах посилення тенденції цифровізації при актуальних регуляторах світового інформаційного простору інформаційні операції Російської Федерації є значущими загрозами інформаційній безпеці України.

Популярність соціальних мереж з розвитком цифровізації інформаційного простору, віртуалізації соціальної взаємодії, забезпечує можливість масового поширення неправдивої інформації, таргетингу, розвитку ботоферм, використання автоматизованих сторінок, множення псевдосуб'єктів, підміни суб'єктів, збору цільових аудиторій, застосування фільтрів блокування окремих інформаційних тем (Guo et al., 2020). Вони формують постійно зростаючу базу даних для розвитку та застосування інструментів соціальної інженерії, що передбачає вивчення особливостей людської поведінки, використання різних методів переконання та обману, для отримання необхідної інформації. Актуальні спроможності використання соціальних мереж з метою інформаційного впливу дозволяють розглядати їхню популярність як загрозу інформаційній безпеці України, тим паче в умовах війни.

Недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій є викликом інформаційній безпеці, оскільки актуальні тенденції цифровізації будуть лише посилювати аспекти індивідуальної відповідальності та освіченості громадян в забезпеченні суспільної інформаційної безпеки. Залежність від хмарних сервісів та спільність інфраструктури створюють ризики витоку, втрати даних та збоїв в діяльності відповідних сервісів та структур. Розвиток Інтернету речей, технології яка з'єднує мільярди електронних пристроїв з Інтернетом для обміну даними, наразі має слабкі протоколи безпеки і є вразливою, тому може використовуватися для прослуховування, перехоплення або модифікації даних через атаки сніфінгу трафіку. Витік та використання особистої інформації на основі цифрових слідів та надмірної віртуалізації особистого життя може мати наслідки як індивідуальні, так і загальнодержавні. Відповідно інформування про сучасні ризики, прищеплення медіакультури та цифрової грамотності є необхідними превентивними заходами загроз для посилення інформаційної безпеки України

Глобальні виклики та загрози інформаційній безпеці України позначені особливостями глобалізації економічної, соціальної та політичної сфер. Динаміка розвитку глобалізаційних процесів суперечлива, оскільки вони розвиваються не

стихійно, а регулюються конфронтацією з інтересами суверенних держав та з їхньою міжнародною політикою. Розвиток інформаційних технологій каталізує глобалізаційні процеси особливо в сфері найменших обмежень та проблемності нормативно-правового регулювання, що складає спільний світовий інформаційний простір.

Виявлені глобальні тенденції та відповідні загрози інформаційній безпеці України складають зовнішній простір її реалізації, який ґрунтується на внутрішніх можливостях. Обмеженість або слабкі сторони таких можливостей визначають національні загрози та виклики, що визначені в Стратегії інформаційної безпеки України (Указ Президента України №685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"», 2021). Серед визначених значиться інформаційний вплив Російської Федерації на населення України та її інформаційне домінування на окупованих територіях як держави-агресора. Активна довготривала інформаційна інтервенція Російської Федерації спрямована на дестабілізацію суспільства, підрив української державності, поширення панічних настроїв, враження національної безпеки в умовах війни провадиться не менш інтенсивно, маючи підготовлене роками підґрунтя. Обмеження та контроль інформаційного простору агресором на тимчасово окупованих територіях, активна дезінформаційна політика, маніпулювання свідомістю значно ускладнюють можливості протидії, сприяючи активному насадженню викривленої альтернативної реальності, що виправдовує насильницькі дії та сприяє формуванню антагоністичних настроїв проти української державності. Розвиток інформаційного простору та можливостей інформаційної сфери підтримують актуальність даної загрози, яка була однією з визначальних для інформаційної безпеки України ще задовго до 2014 року. Російська Федерація тривалий час використовувала інформаційний простір України для поширення проросійських настроїв, маніпулювання та пропаганди з подальшим сприянням поглибленню розколу в суспільстві, спекуляції мовним питанням, загострення відмінностей між україномовним та російськомовним населенням, поширенням сепаратиських настроїв. З розвитком інформаційного

простору розвиваються як можливості інформаційної дії, так і протидії, які мають активно використовуватися як у розробці конкретних заходів забезпечення інформаційної безпеки, так функціонування її системи в цілому. Відсутність ефективної системи реагування на зовнішні та внутрішні інформаційні загрози сприяє перетворенню їх на небезпеки.

Захист національного інформаційного простору в таких умовах забезпечується також системою стратегічних комунікації, що передбачає узгодженість усіх органів державної влади, залучених до реалізації заходів протидії інформаційним загрозам. Формування єдиного інформаційного потоку, його стратегічного планування потребує об'єднання усіх ключових суб'єктів інформаційних відносин. Однак такої ефективної координації діяльності в національному інформаційному просторі поки ще не досягнуто. Це впливає на ефективність антикризової та кризової комунікації, що особливо актуально під час війни та активного використання світового та національного інформаційного простору Російською Федерацією для впливів.

Дієвість даної загрози посилюється недосконалістю регулювання відносин в інформаційній сфері, що впливає на об'єктивність висвітлення інформації, уможливлює тиск на журналістів та викривлення інформації залежно від політичних переконань та індивідуальних інтересів власника інформаційних ресурсів чи представників місцевої влади. Дотримання балансу між свободою слова та відповідальністю за суспільні наслідки інформаційного впливу є основою для безпечного та відкритого інформаційного середовища. Однак складність об'єктивізації наслідків інформаційного впливу, його ступеня, сприяє активному використанню пропаганди та маніпулювання суспільною думкою. Зокрема сприяння розладу в суспільстві, поширенню суперечливої інформації щодо європейської та євроатлантичної інтеграції може проявлятися в негативних суспільно-політичних ефектах, в перешкоджанні необхідному реформуванню та підриві репутації України на міжнародному рівні.

Недостатній рівень інформаційної культури та медіаграмотності створює плідне підґрунтя для протидії маніпулятивним та інформаційним впливам.

Стрімкий розвиток цифрових технологій посилює значущість інформації, однак і підвищує вимоги щодо її відповідального використання як на індивідуальному, так і на державному рівні. Обізнаність щодо потенційних загроз, заходів інформаційної безпеки, необхідного програмного забезпечення та алгоритмів дій в найбільш розповсюджених ситуаціях зловмисного впливу є запорукою не тільки забезпечення індивідуальної інформаційної безпеки, а й національної.

Д. О. Мельник (2021) зазначає, що національні загрози інформаційній безпеці є індикаторами її ефективності та розкривають слабкі сторони системи її забезпечення. Такі загрози без реалізації відповідних заходів можуть перерости у небезпеки як прояв неефективності функціонування системи інформаційної безпеки. Відповідно аналіз актуального стану інформаційної безпеки, її достатності та індикаторів забезпеченості ґрунтується на визначених національних викликах та загрозах як можливості інформаційної безпеки України бути ефективною в контексті глобальних визначальних тенденцій розвитку інформаційної сфери.

Отже, світові тенденції глобалізації сприяють швидкості розповсюдження загроз інформаційній безпеці України та їхньому масштабуванню. Глобальними викликами для інформаційної безпеки України можна вважати складний комплексний характер інформаційних впливів (багатовекторні інформаційні атаки, поліморфне шкідливе програмне забезпечення, використання технологій машинного навчання тощо) та стрімкий розвиток інформаційних технологій (експлойти нульового дня, підвищення вимог до інформаційної та технологічної грамотності). Зовнішньою загрозою глобального та національного масштабу є інформаційні операції Російської Федерації. Внутрішньою національною загрозою інформаційній безпеці України є відсутність системи виявлення та ефективного реагування на інформаційні впливи, несформованість системи стратегічних комунікацій та недосконалість регулювання діяльності в інформаційній сфері, що формують плідне підґрунтя для реалізації зовнішніх загроз інформаційній безпеці України у внутрішні небезпеки як негативні явища щодо реалізації національних інтересів в інформаційній сфері та функціонуванні національного інформаційного простору.

2.2. Нормативно-правове забезпечення інформаційної безпеки України

Ефективність та відповідність актуальним умовам глобалізації інформаційної безпеки України передбачають наявність достатнього нормативно-правового забезпечення для: регулювання інформаційних відносин в різних сферах суспільного буття; визначення прав, обов'язків та відповідальності суб'єктів інформаційної безпеки; впровадження необхідних заходів забезпечення інформаційної безпеки та регулювання їхньої реалізації. Нормативно-правові акти визначають законність функціонування системи інформаційної безпеки, визначають її правове поле.

Нормативно-правове забезпечення інформаційної безпеки України ґрунтується на сукупності законів та підзаконних актів національного законодавства, а також на міжнародних договорах, обов'язковість дотримання яких визнана Верховною Радою України. Нормативно-правове забезпечення інформаційної безпеки України доцільно розглянути за рівнями. Найвищу юридичну силу має Конституція України, відповідно вона представляє перший рівень нормативно-правового забезпечення та визначає основоположні засади інформаційної безпеки:

- ч. 1 ст. 17 передбачає, що забезпечення інформаційної безпеки є однією з найважливіших функцій держави, «справою всього Українського народу» (Конституція України, 1996);

- ст. 31 гарантує таємницю телефонних розмов, листування та можливість винятків;

- ч. 2 ст. 32 регулює використання, поширення, зберігання, збирання конфіденційної інформації та ч. 4 ст. 32 визначає захист права на спростування недостовірної інформації, а також відшкодування завданих нею збитків;

- ч. 1 ст. 34 гарантує право кожного на «свободу думки і слова, на вільне вираження своїх поглядів і переконань» (Конституція України, 1996) та ч. 2 ст. 34 визначає право кожного «вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір» (Конституція

України, 1996), також в ч. 3 ст. 34 визначено, що дані права може бути обмежено у визначених законом випадках, наприклад, з метою забезпечення національної безпеки, територіальної цілісності тощо;

- ч. 2 ст. 50 гарантує право на доступ до інформації про стан довкілля, якість предметів побуту та харчових продуктів як реалізації права на безпечне життя, а також про неможливість засекречення такої інформації;

- ст. 107 визначає, що «Рада національної безпеки і оборони України є координаційним органом з питань національної безпеки і оборони при Президентові України» (Конституція України, 1996), оскільки однією з сфер національної безпеки та оборони України є інформаційна.

Положення Конституції України є вихідними для розробки нормативно-правового забезпечення інформаційної безпеки, яке відповідно не може суперечити Основному Закону України. Другий рівень у нормативно-правовому забезпеченні інформаційної безпеки України складають закони, що визначають її конститутивні положення.

Закон України «Про національну безпеку України» № 2469-VIII від 21.06.2018 (редакція від 09.08.2024) визначає повноваження державних органів в забезпеченні інформаційної безпеки. Керівництво у сферах національної безпеки і оборони, зокрема і в інформаційній безпеці, здійснює Президент України, видає відповідні укази та розпорядження, саме указами Президента України затверджено Стратегію інформаційної безпеки України та Стратегію кібербезпеки України. Рада національної безпеки і оборони України здійснює координацію у сферах національної безпеки і оборони, зокрема й в інформаційній сфері. Служба безпеки України як орган спецпризначення забезпечує контррозвідувальний захист кібербезпеки й інформаційної безпеки. Державна служба спеціального зв’язку та захисту інформації України забезпечує «формування та реалізацію державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації» (Закон України «Про національну безпеку України»), відповідно до чинного законодавства.

Демократичний цивільний контроль за сектором безпеки здійснюють Президент України, Верховна Рада України, Рада національної безпеки і оборони України, Кабінет Міністрів України, органи виконавчої влади та органи місцевого самоврядування, судового контролю, громадського нагляду. Предметом контролю є дотримання вимог Конституції та законів України у діяльності органів сектору інформаційної безпеки, ефективності використання ресурсів, укомплектованості та оснащеності органів інформаційної безпеки, змісту та стану реалізації Стратегії інформаційної безпеки, Стратегії кібербезпеки та відповідних планів заходів.

Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» № 537-V від 09.01.2007 визначає важливість забезпечення інформаційної безпеки в умовах розвитку глобалізаційних процесів та інформатизації в усіх сферах життя. Інформаційна безпека визначається у розділі III як «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» (Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» № 537-V від 09.01.2007, п. 13 розділ III).

Визначено напрямки вирішення проблеми інформаційної безпеки, що передбачає розвиток інформаційної інфраструктури та забезпечення її захисту, забезпечення координації діяльності відповідальних державних органів щодо оперативності виявлення, прогнозування, запобігання загрозам інформаційній безпеці, міжнародне співробітництво, вдосконалення нормативно-правового регулювання в інформаційній сфері, забезпечення цілісності функціонування інформаційної системи та конфіденційності інформації. У розділі IV в пункті 3 зазначається, що визначальним для забезпечення реалізації засад розвитку інформаційного суспільства в Україні є інтеграції її в глобальний інформаційний

простір, зокрема шляхом міжнародного науково-технічного співробітництва та інтеграції України в глобальний культурний інформаційний простір.

Закон України «Про інформацію» № 2657-XII від 02.10.1992 (редакція від 15.11.2024) визначає принципи інформаційних відносин, суб'єктів та інформацію як об'єкти інформаційних відносин, види інформації та інформаційної діяльності. Його положення є основою для регулювання відносин в інформаційній сфері. Забезпечення інформаційної безпеки визначається в ст. 3 як один з основних напрямів державної інформаційної політики.

Закон України «Про Концепцію Національної програми інформатизації» № 75/98-ВР від 04.02.1998 (редакція від 01.01.2022) та Закон України «Про Національну програму інформатизації» № 2807-IX від 01.12.2022 визначають стратегічні завдання інформатизації, її принципи та забезпечення, регулюють реалізацію державної політики, спрямованої на розвиток інформаційного суспільства, впровадження інформаційно-комунікаційних технологій та відповідності забезпечення потреб суспільства відповідно до актуальних тенденцій цифровізації. «Головною метою Програми є забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією на основі широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави» (Закон України «Про Концепцію Національної програми інформатизації» № 75/98-ВР від 04.02.1998 (редакція від 01.01.2022), розділ IV). Одним з основних завдань Програми визначено інтеграцію України у світовий інформаційний простір, що передбачає створення умов відповідно до сучасних тенденцій інформаційної геополітики, державної безпеки та обороноздатності.

Інформаційна безпека визначається як невід'ємна частина національної безпеки та її складових, оборонної, економічної, політичної тощо. Її об'єктами є «інформаційні ресурси, канали інформаційного обміну і електронної комунікації, механізми забезпечення функціонування електронних комунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни» (Закон України «Про Концепцію Національної програми інформатизації» № 75/98-ВР від 04.02.1998 (редакція від 01.01.2022), ст. 3 розділ VI).

Закон України «Про електронні комунікації» № 1089-IX від 16.12.2020 (редакція від 05.01.2025) регулює права, обов'язки та відповідальність користувачів електронних комунікаційних послуг. Згідно з ст. 2 п. 7, безпека мереж і послуг передбачає протидію загрозам доступності та цілісності самих мереж і послуг, а також конфіденційності їхніх даних та пов'язаних з ними послуг (Закон України «Про електронні комунікації» № 1089-IX від 16.12.2020 (редакція від 05.01.2025), ст. 2. п. 7). Згідно з ст. 4 п. 5, одним із завдань державного управління та регулювання є забезпечення безпеки електронних комунікаційних мереж та послуг. Відповідальними за безпеку визначено в ст. 31 постачальників електронних комунікаційних мереж, що передбачає забезпечення цілісності мереж та убезпечення від несанкціонованого доступу до інформації. Згідно з ст. 32, в умовах воєнного стану передбачається створення національного центру оперативно-технічного управління електронними комунікаційними мережами України, його повноваження визначаються Кабінетом Міністрів України. В умовах воєнного стану в ст. 32 передбачаються особливості оперативно-технічного управління електронними комунікаційними мережами, а саме створення Національного центру оперативно-технічного управління електронними комунікаційними мережами України, повноваження якого визначаються Кабінетом Міністрів України. Згідно з ст. 128, метою міжнародного співробітництва в даній сфері є інтеграція електронних комунікацій України у глобальні та забезпечення відповідного міжнародно-правового захисту.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 05.07.1994 (редакція від 28.06.2024) регулює відносини щодо забезпечення захисту інформації в інформаційно-комунікаційних, інформаційних та електронних комунікаційних системах, визначає ключові поняття щодо захисту та систем захисту, несанкціонованих дій, доступу, обробки, знищення інформації, а також повноваження відповідальних органів. Галузеві та цільові профілі безпеки розробляються та затверджуються Службою безпеки України та Міністерством оборони України в порядку, що встановлюється Кабінетом Міністрів України.

Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 (редакція від 28.06.2024) регулює забезпечення захисту у кіберпросторі, визначає об'єкти кібербезпеки, суб'єктів та їхні повноваження, принципи та правові основи, цілі та напрями державної політики. Згідно зі ст. 5, Рада національної безпеки і оборони України здійснює координацію діяльності у сфері кібербезпеки. В ст. 8 ч. 1 визначається, що «національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури» (Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 (редакція від 28.06.2024), ст. 8 ч. 1).

Закон України «Про медіа» № 2849-IX від 13.12.2022 (редакція від 01.01.2025) регулює: реалізацію права на вираження поглядів, доступу до достовірної та різнобічної інформації, її поширення та оперативного отримання; діяльність медіа; функціонування Національної ради України з питань телебачення і радіомовлення.

Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010 (редакція від 18.01.2025) регулює відносини, що передбачають обробку персональних даних, міжнародне співробітництво та передачу персональних даних.

Закон України «Про державну таємницю» № 3855-XII від 21.01.1994 (редакція від 30.10.2024) визначає, яка інформація вважається державною таємницею, порядок засекречення та розсекречення, відповідальні державні органи, надання дозволу на провадження діяльності, пов'язаної з державною таємницею, контроль за збереженням державної таємниці та відповідальність у випадку порушення. Забезпечення охорони державної таємниці здійснює Служба безпеки України.

Закон України «Про доступ до публічної інформації» № 2939-VI від 13.01.2011 (редакція від 08.10.2023) регулює реалізацію права доступу до інформації, що має суспільний інтерес, та інформації суб'єктів владних повноважень, зокрема регулює доступ до інформації та його обмеження, принципи забезпечення, визначає розпорядників інформації та їхні зобов'язання, здійснення запитів на інформацію.

Закон України «Про захист суспільної моралі» № 1296-IV від 20.11.2003 (редакція від 31.03.2023) регулює забезпечення права захисту від розповсюдження інформації, що може негативно впливати на мораль в суспільстві. Згідно з ст. 2, забороняється продукція продукції, що пропагує війну, зміну територіальної цілісності України шляхом насильства, глорифікує осіб, що причетні до здійснення та забезпечення збройної агресії Російської Федерації проти України, виправдовує збройну агресію Російської Федерації, зокрема представлення її «як внутрішнього конфлікту, громадянського конфлікту, громадянської війни, заперечення тимчасової окупації частини території України» (Закон України «Про захист суспільної моралі» № 1296-IV від 20.11.2003 (редакція від 31.03.2023), ст. 2). Визначаються відповідальні за дотримання положень даного закону органи державної влади: Міністерство внутрішніх справ України, Державний комітет телебачення і радіомовлення України, Національна поліцію, Національна рада України з питань телебачення і радіомовлення, а також відповідальні центральні органи виконавчої влади згідно зі сферою реалізації повноважень.

Закон України «Про заборону пропаганди російського нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну» № 2265-IX від 22.05.2022 (редакція від 23.09.2024) у ст. 1 ч. 1 п. 3 визначається, що забороненою пропагандою є поширення інформації щодо підтримки, виправдання, заперечення злочинної діяльності Російської Федерації та причетних до неї осіб, глорифікації такої діяльності, а також використання символіки ідеології «русского міра» та воєнного вторгнення в Україну (Закон України «Про заборону пропаганди російського

нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну» № 2265-IX від 22.05.2022 (редакція від 23.09.2024), ст. 1 ч. 1 п. 3).

До третього рівня нормативно-правового забезпеченні інформаційної безпеки України належать закони, що визначають діяльність державних органів, що належать до інституційного забезпечення інформаційної безпеки України, а саме Закон України «Про Раду національної безпеки і оборони України» № 183/98-ВР від 05.03.1998 (редакція від 29.07.2023), Закон України «Про Службу безпеки України» № 2229-XII від 25.03.1992 (редакція від 09.01.2025), Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» № 3475-IV від 23.02.2006 (редакція від 28.06.2024), Закон України «Про Національну поліцію» № 580-VIII від 02.07.2015 (редакція від 16.08.2024), Закон України «Про оборону України» № 1932-XII від 06.12.1991 (редакція від 05.01.2025), Закон України «Про Збройні Сили України» № 1934-XII від 06.12.1991 (редакція від 05.01.2025), Закон України «Про Службу зовнішньої розвідки України» № 3160-IV від 06.12.1991 (редакція від 23.04.2021), Закон України «Про центральні органи виконавчої влади» № 3166-VI від 17.03.2011 (редакція від 15.11.2024), Закон України «Про правовий режим воєнного стану» № 389-VIII від 12.05.2015 (редакція від 08.02.2025) тощо.

Четвертий рівень нормативно-правового забезпечення інформаційної безпеки формують підзаконні акти, а саме укази Президента України, постанови та розпорядження Кабінету Міністрів України. Розглянемо основоположні нормативно-правові акти даного рівня. Стратегія національної безпеки України в розділі II визначає поточні та прогнозовані загрози національній безпеці та національним інтересам України, серед яких можна виокремити ті, що стосуються власне забезпечення інформаційної безпеки (Указ Президента України № 392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України"», редакція від 07.01.2025):

- визначається стрімкий розвиток технологій, зокрема розробки у сфері штучного інтелекту (ст. 9);

- зростаюча роль інформаційних технологій у всіх сферах суспільного життя; розробка нових систем озброєнь з використанням інформаційних технологій (ст. 9);

- зростаюча глобалізація та відсутність дієвих інструментів глобального управління (ст. 8 та 10);

- посилення міжнародної конкуренції з використанням кіберзасобів та засобів інформаційного впливу та кібервпливу (ст. 14);

- використання інформаційної «зброї» Російською Федерацією для зміцнення своїх позицій в Європі та впливу на внутрішньополітичну ситуацію в європейських державах (ст. 16);

- деструктивна пропаганда, що має дестабілізуючий суспільний вплив, та відсутність цілісної інформаційної політики держави (ст. 20).

В розділі ІІІ Стратегії національної безпеки України серед основних напрямків діяльності держави щодо забезпечення національної безпеки в ст. 45 визначається необхідність захисту від невоєнних загроз як з боку Російської Федерації, так від інших держав, зокрема важливість активної та ефективної протидії інформаційним операціям та кібератакам, розвідувально-підривній діяльності, російській пропаганді. В ст. 49 визначається необхідність розвитку інклюзивного політичного діалогу, медіакультури суспільства, інформаційних послуг, створення системи стратегічних комунікацій. В ст. 52 визначається важливість розвитку системи кібербезпеки в умовах цифрової трансформації. Стратегія національної безпеки України є основною та вихідною для наступних документів, положення яких визначають можливості її реалізації.

Стратегією воєнної безпеки України в комплексі заходів щодо оборони України передбачено превентивні дії та протидію агресору в кіберпросторі та в інформаційному просторі. На глобальному рівні серед основних аспектів воєнної безпеки визначено боротьбу за ресурси та міждержавну конкуренцію з використанням інструментів інформаційного впливу, зростання значущості

розвитку інформаційних технологій. На національному рівні головним аспектом воєнної безпеки є гібридна війна Російської Федерації проти України з використанням пропаганди та інших інформаційно-психологічних засобів. Серед основних завдань державної політики у воєнній сфері зазначаються: розробка системи комплексного стратегічного аналізу воєнних загроз; відповідно до тенденції цифровізіції впровадження сучасних інформаційних технологій; використання єдиного інформаційного простору; формування єдиної захищеної інформаційної мережі в поєднанні джерел інформації, органів управління, військових частин та підрозділів (Указ Президента України № 121/2021 «Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України"»).

Стратегія передбачає реформування Збройних Сил України та відповідність їх визначеним критеріям, серед яких спроможність до стратегічної мобільності, до непрямих та багатосферних дій, що нівелюють чисельну перевагу противника, зокрема в інформаційному просторі та кіберпросторі. Серед ймовірнісних сценаріїв, що передбачають необхідність застосування сил безпеки та оборони України, визначається можливе застосування воєнної сили проти України як при ескалації збройної агресії Російською Федерацією, так і з боку інших держав. Такі сценарії враховують активність проведення супутніх інформаційних кампаній, кібероперацій та інформаційно-психологічних операцій (Указ Президента України № 121/2021 «Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України"»).

Стратегія цифрового розвитку інноваційної діяльності України на період до 2030 року визначає стратегічні цілі та завдання державної політики у сфері цифрового розвитку інноваційної діяльності, що має визначальне значення для європейської інтеграції України. Сприяння науковим дослідженням і розробкам, трансферу технологій, особливо в сфері інформаційних технологій, посилить національну безпеку України. Стратегічні цілі 9, 15 та 17 визначають значущість цифрових інновацій у сфері оборони, кібербезпеки та для розвитку інформаційного простору, його розширення через розвиток імерсивних технологій розширеної

реальності, штучного інтелекту та комунікаційних мереж (Розпорядження Кабінету Міністрів України № 1351-2024-р від 31.12.2024 «Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025-2027 роках»).

Національна стратегія із створення безбар'єрного простору в Україні на період до 2030 року передбачає в напрямі 3 забезпечення цифрової безбар'єрності (Розпорядження Кабінету Міністрів України № 366 від 14.04.2021 «Про схвалення Національної стратегії із створення безбар'єрного простору в Україні на період до 2030 року»). Реалізація даного напряму сприятиме збільшенню національного інформаційного простору та підвищенню значущості забезпечення інформаційної безпеки. Стратегічні цілі в межах цього напряму передбачають збільшення доступності швидкісного Інтернету, цифрових послуг та необхідність розвитку цифрової грамотності населення.

Стратегія інтегрованого управління кордонами на період до 2025 року передбачає необхідність забезпечення оперативного обміну інформацією між суб'єктами системи інтегрованого управління кордонами, сприяння транскордонному співробітництву та інтеграції України до єдиного інформаційного простору, розвитку інформаційної інфраструктури відповідно до тенденцій цифровізації (Розпорядження Кабінету Міністрів України № 687-2019-р від 24.07.2019 «Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року» (редакція від 21.07.2023)).

Кіберпростір є сегментом інформаційного простору, а відповідно кібербезпека є частиною інформаційної безпеки, тому Стратегія кібербезпеки України змістовно в цілому відображає також проблемні аспекти розвитку інформаційної безпеки. Вона визначає глобальні аспекти кібербезпеки, що передбачає зростання питомої ваги кіберзагроз у зв'язку з розвитком інформаційних технологій та штучного інтелекту, мілітаризацію кіберпростору, поділ державами сфер впливу у кіберпросторі з метою реалізації, гібридну війну проти України, посилення тенденції ведення розвідувально-підривної діяльності у кіберпросторі, швидкість змін у цифровізованому світі. За таких умов національна

система кібербезпеки має бути гнучкою та більш збалансованою. Національні загрози кібербезпеці становлять: збільшення арсеналу кіберзброї Російською Федерацією проти України у кіберпросторі, об’єктами кібератак є інформаційно-комунікаційні системи державних органів України та критична інформаційна інфраструктура, здійснення розвідувально-підривної діяльності.

Чинниками актуалізації даних загроз є: технологічна залежність України від іноземної продукції в сфері інформаційно-комунікаційних технологій; недосконаліть нормативно-правової бази у сфері інформаційної безпеки та кібербезпеки; недостатня кількість відповідних структурних підрозділів та кадрового забезпечення; відсутність критеріїв достатності інформаційної безпеки та системи її незалежного аудиту; відсутність державного реєстру об’єктів критичної інформаційної інфраструктури; необхідність розвитку організаційно-технічної моделі кіберзахисту; необхідність реалізації системного підходу щодо підвищення цифрової грамотності населення; відсутність системи інформаційно-аналітичного забезпечення кібербезпеки (Указ Президента України №447/2021 "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України", 2021). Засадами розбудови національної системи кібербезпеки визначено: відповідність глобальним трендам, проактивність та ризик-орієнтований підхід. Однією з пріоритетних цілей розвитку кібербезпеки визначено європейську та євроатлантичну інтеграцію.

Стратегія інформаційної безпеки України є основним змістовним документом щодо забезпечення інформаційної безпеки, оскільки вона конкретизує виклики та загрози національній безпеці в інформаційній сфері, визначає стратегічні цілі та завдання посилення спроможностей держави, визначає відповідальні за їхню реалізацію державні органи. Стратегічними цілями інформаційної безпеки визначено:

- протидія дезінформації та інформаційним операціям держави-агресора;

- забезпечення розвитку української культури та громадянської ідентичності з метою консолідації українського суспільства;

- підвищення рівня медіакультури та медіаграмотності населення з метою запобігання деструктивному впливу дезінформації та маніпуляцій, забезпечення соціально відповідального споживання інформації;

- забезпечення прав особи на інформацію, свободу вираження поглядів і переконань, забезпечення захисту приватного життя, захисту прав журналістів;

- інформаційна реінтеграція до українського інформаційного простору громадян України тимчасово окупованих та прилеглих до них територій України;

- розвиток інформаційного суспільства (Указ Президента України №685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"», 2021).

Реалізація Стратегії здійснюється через відповідний цілям розроблений План заходів та передбачає такі результати: захищеність інформаційного простору України; підвищення ефективності функціонування системи стратегічних комунікацій; ефективність протидії поширенню незаконного контенту; підвищення рівня медіаграмотності та медіакультури населення; інформаційна реінтеграція громадян України, що перебувають на тимчасово окупованих територіях України; забезпечення прав на вільне вираження своїх поглядів і переконань, а також захист приватного життя; захист прав журналістів; формування української громадянської ідентичності (Указ Президента України №685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"», 2021). Нормативно-правове забезпечення реалізації Стратегії інформаційної безпеки України передбачає системний перегляд та внесення змін до відповідних нормативно-правових актів в інформаційній сфері.

Указ Президента України № 187/2021 від 07.05.2021 «Питання Центру протидії дезінформації» визначає Центр протидії дезінформації робочим органом Ради національної безпеки і оборони України, що задіяний у розробці та реалізації Стратегії інформаційної безпеки України, здійснює аналіз стану її реалізації, ефективності передбачених заходів щодо протидії дезінформації, забезпечує координацію органів виконавчої влади щодо реалізації стратегічних цілей

забезпечення інформаційної безпеки (Указ Президента України № 187/2021 від 07.05.2021 «Питання Центру протидії дезінформації»).

Також до нормативно-правового забезпечення інформаційної безпеки належать міжнародні договори. Серед міжнародних правових актів можна виділити: Конвенцію про кіберзлочинність (Convention on Cybercrime, 2001), основний міжнародний договір, який визначає стандарти для боротьби з кіберзлочинністю та сприяє міжнародному співробітництву у цій сфері; Міжнародний пакт про громадянські і політичні права (International Covenant on Civil and Political Rights, 1966), в якому Ст. 19 гарантує право на свободу вираження поглядів, включаючи право на доступ до інформації через будь-які засоби масової інформації; Конвенція ООН про права дитини (Convention on the Rights of the Child, 1989), що забезпечує права дітей, доступ до відповідної інформації та захист від шкідливого контенту; Резолюції Генеральної Асамблеї ООН щодо інформаційної безпеки (Resolution on Information Security, 2021).

До регіональних правові актів можна віднести: Регламент Європейського Союзу про захист персональних даних (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, 2016), що регламентує захист персональних даних громадян ЄС і встановлює вимоги до обробки даних; Європейська конвенція про права людини (European Convention on Human Rights, 2010), в якій Ст. 10 гарантує право на свободу вираження, що включає свободу отримувати та передавати інформацію без втручання державних органів незалежно від кордонів; Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981), що встановлює стандарти для захисту персональних даних у країнах-учасницях.

Двостороння безпекова угода між Україною та Сполученими Штатами Америки від 13.06.2024 строком до 13.06.2034 визначає в статті II основи співробітництва у сфері безпеки з метою її зміцнення та забезпечення стабільності в Європі, протидії загрозам. Для реалізації даної мети передбачено: співпрацю у

сфері досліджень та науково-технічних розробок; сприяння протидії дезінформації та російській пропаганді, посиленню цих спроможностей України; поглиблення співпраці між розвідувальними службами та обміну інформацією (Двостороння безпекова угода між Україною та Сполученими Штатами Америки, № 840_001-24 від 13.06.2024, ст. II).

П’ятий рівень нормативно-правового забезпечення складають відомчі накази, положення та інструкції в інформаційній сфері, які приймають міністерства та відомства України на основі чинного законодавства в межах своїх компетенції та відповідальності; нормативні та директивні акти місцевих органів влади щодо забезпечення інформаційної безпеки України.

Отже, нормативно-правове забезпечення інформаційної діяльності ґрунтується на положеннях Конституції України, в якій інформаційна безпека визначається як одна з найважливіших функцій держави, включає закони, що визначають конститутивні засади інформаційної безпеки, а також закони, що визначають її інституційне забезпечення, регулюють діяльність відповідних державних органів, містить також стратегічні правові акти як дотичні щодо забезпечення інформаційної безпеки, так і прямого функціонального призначення. Стратегічні акти характеризуються цільовим, програмним характером та короткостроковою реалізацією, визначають стратегічні цілі та завдання правового регулювання інформаційної сфери, конкретизують проблеми та визначають основні напрями діяльності, заходи та прогнозовані результати. Однак серед нормативно-правових актів в забезпеченні інформаційної безпеки немає концептуальних, як, наприклад, для кібербезпеки Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 (редакція від 28.06.2024), що регулює забезпечення захисту у кіберпросторі, визначає об’єкти кібербезпеки, суб’єктів та їхні повноваження, принципи та правові основи, цілі та напрями державної політики, основоположні принципи, структуру та функціонування національної системи кібербезпеки. Оскільки кібербезпека є зростаючою складовою інформаційної безпеки в умовах цифровізації усіх сфер суспільного буття, широкого використання комп’ютерних систем та

комунікаційних мереж, то дані засади визначають фрагментарно й інформаційну безпеку.

Спроби розробки таких концептуальних актів були, однак Доктрина інформаційної безпеки України (2017) за змістом положень мала стратегічний характер, а розроблений проєкт Концепції інформаційної безпеки України (2015) не був затвердженим за результатами правового аналізу відповідності міжнародним стандартів та зобов'язань ОБСЄ (Найман-меткалф, 2015). Наявність доктринального, чи концептуального, акту дозволила б визначити систему ідей, принципів та механізмів державної політики в інформаційній сфері, актуальні напрями розвитку інформаційної безпеки, що стали б концептуальним підґрунтям нормотворчої та правозастосовної діяльності, визначення стратегічних цілей та їхньої реалізації. Відповідно наслідками відсутності такого концептуального підґрунтя є проблемність реалізації цілісного підходу до удосконалення нормативно-правового забезпечення інформаційної безпеки з відсутністю термінологічної визначеності, зокрема щодо інформаційного суверенітету, з недостатньою інтеграцією міжнародних норм та адаптованістю до сучасних загроз, з визначенням лише короткострокових стратегічних завдань та їхньою проблемно-орієнтованістю.

2.3. Інституційне забезпечення інформаційної безпеки України

Інституційне забезпечення інформаційної безпеки України здійснюється на основі передбачених для реалізації Стратегії інформаційної безпеки України механізмів реалізації передбачених стратегічних цілей та завдань, регулюється відповідними інститутивними та конститутивними законами нормативно-правового забезпечення інформаційної безпеки, що були розглянуті в попередньому підрозділі. До системи інформаційної безпеки України належать:

1. Рада національної безпеки і оборони України, яка здійснює забезпечення національної безпеки України в інформаційній сфері шляхом координації діяльності органів виконавчої влади. Закон України «Про Раду національної

безпеки і оборони України» № 183/98-ВР від 05.03.1998 (редакція від 29.07.2023) в ст. 4 визначає компетенції Ради національної безпеки і оборони України, яка зокрема приймає рішення щодо заходів відповідно до масштабу реальних та прогнозованих загроз національним інтересам та безпеці України в інформаційній сфері, а також щодо визначення концептуальних засновків забезпечення національної безпеки в інформаційній сфері.

2. Центр протидії дезінформації, який є робочим органом Ради національної безпеки і оборони України та забезпечує реалізацію заходів щодо протидії реальним та прогнозованим загрозам національним інтересам та безпеці України в інформаційній сфері, маніпуляціям суспільною думкою, пропаганді та деструктивним інформаційним впливам. Основними завданнями Центру протидії дезінформації є моніторинг інформаційного простору України та світового інформаційного простору, виявлення загроз інформаційній безпеці України, прогнозування загроз та оцінка наслідків для національної безпеки України, координації діяльності органів виконавчої влади щодо забезпечення інформаційної безпеки, визначення концептуальних підходів та методології у сфері протидії деструктивним інформаційним впливам, участь у розробці інтегрованої системи оцінки інформаційних загроз та забезпечення оперативного реагування на них, визначення пріоритетних напрямів залучення міжнародної технічної допомоги щодо забезпечення інформаційної безпеки (Указ Президента України № 187/2021 від 07.05.2021 «Питання Центру протидії дезінформації»).

3. Кабінет Міністрів України, який відповідає за інформаційну політику держави, забезпечення інформаційного суверенітету, фінансування відповідних програм щодо інформаційної безпеки, розробку плану заходів щодо реалізації стратегічних завдань інформаційної безпеки та координацію роботи міністерств та інших органів виконавчої влади щодо їхньої реалізації.

4. Міністерство оборони України, що забезпечує моніторинг інформаційного простору, виявлення та прогнозування інформаційних загроз національній безпеці у воєнній сфері; проведення інформаційних заходів оборонного характеру; розробку цільових профілів безпеки для інформаційних, електронних

комунікаційних та інформаційно-комунікаційних систем; висвітлення інформації щодо ситуації у районах бойових дій та Збройних Силах України.

5. Генеральний штаб Збройних Сил, який відповідно до ст. 11 Закону України «Про оборону України» № 1932-XII від 06.12.1991 (редакція від 05.01.2025) може в особливий період використовувати та здійснювати контроль за інформаційним простором держави;

6. Служба безпеки України, зокрема функціональні підрозділи контррозвідки, військової контррозвідки, контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, яка здійснює моніторинг світового інформаційного простору з метою виявлення загроз національній безпеці України; протидію спеціальним інформаційним операціям проти суверенітету, суспільно-політичної стабільності та територіальної цілісності України (Закон України «Про Службу безпеки України» № 2229-XII від 25.03.1992 (редакція від 09.01.2025)).

7. Розвідувальні органи України, які у процесі своєї діяльності здійснюють виявлення та забезпечують протидію зовнішнім інформаційним загрозам у сфері безпеки та оборони держави (Закон України «Про Службу зовнішньої розвідки України» № 3160-IV від 01.12.2005 (редакція від 23.04.2021))

8. Державна служба спеціального зв'язку та захисту інформації України, до обов'язків якої належить забезпечення впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» № 3475-IV від 23.02.2006 (редакція від 28.06.2024), ст. 14)

9. Національна поліція, діяльність якої передбачає забезпечення відповідальності за протиправне використання інформаційних ресурсів, порушення прав особи, пов'язаних з обробкою інформації (Закон України «Про Національну поліцію» № 580-VIII від 02.07.2015 (редакція від 16.08.2024), ст. 28)

10. Національна рада України з питань телебачення і радіомовлення, яка забезпечує захист українського інформаційного простору від пропаганди держави-агресора, сприяє забезпеченню українського телерадіомовлення на тимчасово окупованих територіях України.

11. Центральні органи виконавчої влади, що забезпечують реалізацію державної політики в інформаційній сфері, здійснюють нормативно-правове регулювання, визначають пріоритетні напрями розвитку та перспективи України у сфері інформаційної безпеки, сприяють популяризації України у світових та національних інформаційних ресурсах, зокрема Міністерство культури та стратегічних комунікацій, створений при ньому Центр стратегічних комунікацій та інформаційної безпеки, Міністерство закордонних справ України.

12. Наукові та науково-дослідні установи, які залучаються з метою науково-аналітичного та експертного супроводження формування та реалізації державної інформаційної політики, зокрема Національний інститут стратегічних досліджень.

До суб'єктів забезпечення інформаційної безпеки також можна додати Національний центр оперативно-технічного управління електронними комунікаційними мережами України, створення якого передбачається в умовах воєнного стану з метою забезпечення централізованого оперативно-технічного управління електронними комунікаційними мережами загального користування для цілей оборони та безпеки держави (Постанова Кабінету Міністрів України № 75-2025-п від 24.01.2025 «Деякі питання оперативно-технічного управління електронними комунікаційними мережами в умовах надзвичайної ситуації, надзвичайного або воєнного стану»).

Стратегія інформаційної безпеки передбачає розроблений План заходів, спрямований на реалізацію визначених нею стратегічних цілей та завдань (Розпорядження Кабінету Міністрів України від 30 березня 2023 року № 272-р "Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року", 2023). Кожний захід передбачає визначення відповідального за його виконання інституції та індикатори реалізації. Для досягнення прогнозованих результатів Стратегії інформаційної безпеки України та реалізації відповідних стратегічних завдань розроблено близько 128 заходів, за виконання яких відповідають органи державної влади, державні установи та підприємства, загальним обсягом в 35 структурних одиниць, така кількість демонструє впливовість інформаційного простору та осяжність в розумінні необхідності

забезпечення інформаційної безпеки. Інформаційний простір об’єднує різні сфери суспільного буття та соціальних відносин, його масштабність буде лише зростати за сприяння активного розвитку тенденції цифровізації світу. На основі даного Плану та зазначених відповідальних органів за реалізацію передбачених заходів визначено структуру забезпечення інформаційної безпеки України як реалізації її основних стратегічних цілей (рис. 2.1). Зв’язки визначено на основі змісту заходів. Структурне забезпечення виконання стратегічних завдань включає державні органи спецпризначення, які задають визначальний безпековий аспект в умовах війни з Російською Федерацією інформаційній політиці України, центральні органи виконавчої влади, координаційні органи, які сприяють взаємоузгодженості реалізації стратегічних завдань, суб’єктів інформаційної діяльності та науково-аналітичне супроводження. Поряд з кожним визначеним суб’єктом реалізації Стратегії інформаційної безпеки України зазначено в дужках передбачене Планом заходів функціональне навантаження, що визначається кількістю передбачених заходів, до реалізації яких залучено даного суб’єкта. Найбільша задіяність передбачається для Міністерства культури та стратегічних комунікацій, що відповідає основним напрямам діяльності даного центрального органу виконавчої влади – інформаційній політиці та безпеці. Найменша – припадає на науково-аналітичне супроводження.

О. Д. Довгань (2015) вважає, що глобалізація та тенденції розвитку суспільства передбачають в забезпеченні інформаційної безпеки необхідність активного використання результатів науково-дослідної роботи в інформаційній сфері. Це сприятиме розвитку національних інформаційних ресурсів, дієвості механізмів функціонування інформації та забезпеченню суверенності національного інформаційного простору. Однак в забезпеченні заходів реалізації стратегічних завдань інформаційної безпеки України науково-аналітичне супроводження має найменше функціональне навантаження, потенційні можливості якого забезпечуються актуальним рівнем розвитку інформаційних технологій та відповідають найбільш активному чиннику інтенсифікації глобалізації та масштабування інформаційного простору.

Рис. 2.1. Структура державного забезпечення виконання заходів з реалізації Стратегії інформаційної безпеки України

Джерело: сформовано автором на основі Плану заходів з реалізації Стратегії інформаційної безпеки України.

В цілому виконавча забезпеченість Стратегії інформаційної безпеки України вказує на масштабність, мультиканальність та узгодженість її реалізації. Практична реалізація інституційного забезпечення інформаційної безпеки виявилася ширшою в межах конкретизованих завдань та заходів. Інституційне забезпечення інформаційної безпеки має відповідати можливості функціональної реалізації єдності трьох її складових: захисту інформації, захисту та моніторингу національного та світового інформаційного простору, забезпеченню інформаційної достатності (Шемчук, 2019). Аналіз нормативного та практичного інституційного забезпечення визначає функціональну відповідність даним складовим інформаційної безпеки. Функціонування даних складових та їхнє навантаження щодо передбачених завдань інформаційної безпеки реалізується відповідно до визначених загроз та викликів сьогодення як глобальних, так і національних. Однак при цьому варто зазначити наявність дублювання завдань для різних державних органів, повноваження яких та функціональне призначення передбачають необхідність ефективної координації та інтегральної системи моніторингу загроз, створення єдиного інформаційного поля як основи узгоджених дій.

2.4. Управління інформаційним простором як механізм забезпечення інформаційної безпеки України

Інтенсивність та масштабність глобалізації з відповідними загрозами інформаційній безпеці та визначальне значення інформаційного простору актуалізують питання механізмів та засобів забезпечення інформаційної безпеки України. Інформаційна сфера впливає на стан складових національної безпеки будь-якої держави та є системоутворюючим чинником життя суспільства (Сагайдак, 2010). Глобалізація різних сфер суспільного буття супроводжується розширенням інформаційних мереж, інтенсифікацією інформаційних потоків, збільшенням значення та вартості інформації. Розвиток інформаційних технологій об’єктивує інформаційний простір як кіберпростір, паралельну реальність, суб’єктивне відображення дійсності, екзопсихіку, інтерсуб’єктивний світ.

Стабільність та захищеність економічної, політичної, соціальної, духовно-культурної та військово-оборонної сфер залежать від урегульованості та захищеності інформаційного простору, який є джерелом дестабілізуючих та конфліктогенних впливів в умовах невизначеності зон відповідальності, правового забезпечення, механізмів управління та його суб'єктності.

З даної проблематики можна відзначити дослідження правових аспектів захисту світового інформаційного простору в умовах збройних конфліктів H. Lahmann (2020), детермінант інформаційних загроз в світовому інформаційному просторі O. Kuzmenko et al. (2021), шляхів забезпечення захисту інформаційного простору держави S. Hlobenko (2023), інформаційного простору в контексті міжнародної безпеки K. Buhaichuk et al. (2023), світового інформаційного простору як інфраструктурного середовища інформаційної безпеки держави Я. Чмира (2020), штучного інтелекту як інструмента державного управляння інформаційною безпекою V. Bondar (2023), критеріїв достатності інформаційної безпеки O. Bortnikova et al. (2024), інформаційних загроз та стратегій протидії V. Ievdokymov et al. (2024).

Глобалізація створила плідні умови для проростання інформаційних потоків у різні сфери суспільного буття, надаючи інформації нової економічної та політичної ваги. Інформаційні відносини актуалізували четвертий вимір суспільного розвитку (Bortnikova et al., 2024). Глобалізація інформаційного простору породила також окремий вимір злочинності – кіберзлочинність: хакерські атаки, фішинг, зломи даних, поширення шкідливого програмного забезпечення, збір, зберігання та використання персональних даних без згоди користувачів. Її масштабність може сягати кібертероризму з атаками на критичну інфраструктуру держави та нового типу війни, яка порівняно з реальними військовими операціями є менш ризикованою та ресурсовитратною. Інформаційний простір може використовуватися для поширення дезінформації та пропаганди з метою впливу на суспільну думку, політичні процеси, економічні рішення та суспільну стабільність (Chmyr et al., 2023). Неоднаковий доступ до інформаційних технологій та Інтернету створює цифровий розрив між різними соціальними групами та країнами,

породжує культурну гомогенізацію через домінування певних культурних продуктів та медіа, сприяє монополізації ринку інформаційних ресурсів великими транснаціональними корпораціями. Соціальні мережі відкривають нову реальність соціального життя, звичні правила та закони якого тут не працюють (Buhaichuk et al., 2023). Псевдоособистості, вплив на контент, великий ступінь довіри, лідери думок, генерування контенту штучним інтелектом, нейронні мережі та комерційні інтереси, викривлення сприймання формують нові виклики для розробки та впровадження правового регулювання та зон відповідальності.

Зважаючи на різноплановість та різномасштабність загроз світовий інформаційний простір потребує управління та правового регулювання. Національний інформаційний простір України не є ізольованим і не може існувати відокремлено, в умовах глобалізації управління світовим інформаційним простором відкриває можливість забезпечення як національної, так і міжнародної безпеки (Слюсарчук, 2015).

Управління передбачає процес забезпечення глобальними акторами нівелювання негативних і посилення позитивних для людської спільноти ефектів глобалізації шляхом використання засобів і механізмів, які діють на різних рівнях – локальному, національному, регіональному і глобальному (Юськів, 2009). Такий підхід передбачає врахування особливостей світового інформаційного простору, що зумовлені загальними глобалізаційними процесами та суспільною природою механізмів його саморегуляції. Особливостями світового інформаційного простору є: всеохоплюючий та сегментарний характер, системоутворюючий вплив на різні сфери суспільного буття та змістовна відповідність сфері функціонування інформаційної інфраструктури, багатосуб’єктність та багатооб’єктність, висока проникність, відсутність геополітичної відповідності, висока ступінь довіри, залежність від темпів інформаційно-технологічного розвитку та доступності технологій, складність правового регулювання через високу динамічність, гнучкість та геополітичну, культурну суперечність правових норм (Дубовський, 2024а).

Враховуючи визначені особливості світового інформаційного простору управління ним має мати такі властивості: поліцентричність, що передбачає відсутність верховної інстанції та систему розподілених суверенітетів з колективними пошуками рішень і взаєморозумінням урядів країн високого рейтингу глобалізації; плюралістичність, що відповідає багатосуб'єктності, яка передбачає залучення різних учасників – урядів, міжнародних і неурядових організацій, підприємницьких структур; специфічність предмета і методів, що зумовлена перетином національних інтересів і владних відносин; багаторівневість, яке передбачає регулювання на локальному, національному, регіональному і глобальному рівнях; інституційна інноваційність, яка зумовлена динамічністю та пластичністю світового інформаційного простору і потребує трансформацій звичних інституцій та структур (Юськів, 2009).

Принципами реалізації управління світовим інформаційним простором можуть бути: принцип законності, що передбачає використання механізмів та технології управління на основі чинного законодавства та нормативно-правової бази, що регулює як суспільні інформаційні відносини, так і міжнародні відносини у сфері інформаційного співробітництва; принцип примату норм міжнародного права над національним законодавством, що полягає в прямому застосуванні загальновизнаних принципів і норм міжнародного права, міжнародних договорів на території конкретної країни залежно від специфіки інформаційного ресурсу, який поширюється без кордонів; принцип права власності на інформацію; принцип економічної доцільності систем захисту інформації, зважаючи на величину економічної шкоди та тяжкість негативних наслідків в контексті національних та глобальних інтересів; принцип неупередженості оцінки реальних і потенційних загроз інформації та її обігу, стану правової та організаційної бази; принцип безперервності, що передбачає постійне застосування загальних та специфічних заходів і методів регуляції, моніторингу, контролю в межах системного підходу до управління світовим інформаційним простором (Bortnikova et al., 2024).

І. Забара (2013) зазначає про важливість дотримання принципу неподільності безпеки. В умовах світового інформаційного простору безпека кожної з держав

пов’язана із безпекою усіх інших, що передбачає відповідальність за власний національний інформаційний простір та інформацію, що в ньому поширюється. При цьому жодна з держав не має зміцнювати власну безпеку за рахунок нанесення шкоди безпеці інших держав.

Правове забезпечення регулювання світового інформаційного простору включає в себе комплекс міжнародних, регіональних та національних правових актів, що визначають правила і стандарти для застосування різних аспектів інформаційних технологій та використання кіберпростору.

До діючих суб’єктів потенційного управління світовим інформаційним простором можна віднести: Internet Corporation for Assigned Names and Numbers (ICANN), що відповідає за координацію системи доменних імен та IP-адрес, забезпечуючи стабільність і безпеку функціонування глобальної мережі; Internet Engineering Task Force (IETF), що розробляє стандарти технічного функціонування Інтернету; World Wide Web Consortium (W3C), що розробляє веб-стандарти для забезпечення взаємодії та доступності веб-технологій; ООН, що займається питаннями глобальної політики та прав людини в інформаційному просторі; ЮНЕСКО, що працює над розвитком етичних стандартів для інформаційних і комунікаційних технологій, наприклад, в межах заходів щорічної з 2019 року ініціативи Міжнародного дня загального доступу до інформації; Рада Європи, що просуває стандарти прав людини, демократії та верховенства права в кіберпросторі через різні ініціативи та конвенції; International Telecommunication Union (ITU), що займається питаннями інформаційних і комунікаційних технологій, включаючи стандартизацію та регулювання; національні уряди, що розробляють і впроваджують національні стратегії та законодавство щодо інформаційної безпеки, наприклад, Центр глобальної взаємодії Державного департаменту США; транснаціональні компанії, наприклад, Google, Facebook, Amazon, Microsoft, мають значний вплив на інформаційний простір і розробляють власні політики з управління даними та конфіденційності; громадські організації та спільноти, наприклад, East Stratcom Task Force, Global Coalition for Digital Safety, Digital Trust & Safety Partnership (Bondar, 2023).

На основі моделей інформаційної безпеки можна визначити потенційні об’єкти та предметні області управлінського впливу в світовому інформаційному просторі. Можна виділити моделі A, B, C, D та E (Макаренко, 2003). Модель А передбачає створення системи абсолютного захисту країною, що є лідером в інформаційній сфері. Лідерство передбачає розвиненість інформаційних технологій, інвестиційну перевагу в даній сфері, створення інноваційних центів. Реалізація даної моделі може відрізнятися залежно від особливостей країни: при авторитарному типі правління реалізація управління інформаційним простором може здійснюватися шляхом обмеження доступу до національного інформаційного простору, а в країнах демократичного типу - шляхом збільшення кількості даних про користувачів та розвитку систем моніторингу (Білоусов, 2016).

Модель В передбачає розробку наступальних видів озброєння, засобів інформаційного впливу. В такому випадку передбачається управління інформаційним простором з метою реалізації країною власних інтересів та забезпечення переваги на політичній арені. Модель С реалізується через об’єднання декількох країн-лідерів в інформаційній сфері з метою стримування інформаційних загроз та вирішення глобальних проблем. В такому випадку управління світовим інформаційним простором передбачає створення дієвих механізмів правового регулювання, розробку міжнародних нормативно-правових актів та систему санкцій щодо порушення їхніх положень. Об’єктом впливу є інформаційні міжнародні відносини.

Модель D відзначається використанням транспарантності інформаційного простору та формуванням ситуативних альянсів при вирішенні локальних проблем, наприклад, проведення міжнародних антитерористичних операцій, чи стимулювання внутрішньодержавних конфліктів. Модель Е акцентує увагу на протидії злочинності в інформаційному просторі, її впливові на політичні, економічні та суспільні процеси. Відповідно передбачається шляхом міжнародно-правового регулювання інформаційного простору мінімізувати загрозу застосування інформаційної зброї (Забара, 2013). Об’єктом впливу може бути інформаційна зброя. Її визначення, заборона чи моніторинг застосування.

Заборонити розробку та використання інформаційної зброї в умовах інтенсивного розвитку інформаційних технологій неможливо, як і обмежити світовий інформаційний простір.

Управління інформаційним простором можна розглянути в контексті парадигм управління інформаційною безпекою (Панченко, 2020). Перша парадигма ґрунтується на системному підході та передбачає управління інформаційним простором щодо усунення вразливостей та передбачення можливих дестабілізуючих чинників, що сприятиме загальній стійкості системи інформаційної безпеки. Наприклад, введення обмежень США щодо застосування деяких китайських технологій в інформаційній сфері, що відзначилися проблемами в забезпеченні приватності.

Друга парадигма заснована на синергетичному підході, що відповідає особливостям розвитку інформаційного простору. Управління реалізується через створення конструктивних умов саморозвитку, передбачення можливих сценаріїв та убезпечення шляхом спрямовування від небажаних ефектів та наслідків. Передбачається визначення принципів розвитку, аналіз часової динаміки та характерних тенденції. Наприклад, аналіз сценарних прогнозів інформаційного ажіотажу щодо коронавірусу.

Третя парадигма використовує феноменологічний підхід. Інформаційний простір розглядається як інтерсуб'єктивний, насичений життєвим досвідом та особистісними сенсами. Одна й та ж подія може бути представлена з різних точок зору та матиме при цьому різний потенціал реагування суспільства. Управлінський вплив в інформаційному просторі стосується значущих предметних областей, враховує ситуативний характер взаємозв'язків. Ключовим в інформації визначається її суспільна значущість. Умовою ефективного управління є розуміння інтерсуб'єктивного простору, знання механізмів та моделей його конструювання, здатність до виявлення латентних чинників, фонових знань, що впливають на інтерпретацію подій. Наприклад, управління інформаційним простором може реалізовуватися через вплив на соціальні установки, забезпечення прозорості смислових систем, швидкість реагування в інформуванні населення державними

органами про події, що можуть інтерпретуватися неоднозначно та мати значущі соціальні наслідки.

Четверта парадигма передбачає використання когнітивного підходу, що узгоджується з концептуальною моделлю інформаційного суспільства. Управління інформаційним простором ґрунтується на зростаючій значущості знання та наукомістких технологій, використанні кваліфікованої експертизи ситуації. Наприклад, обмеження знань або викривлення інформації з метою маніпулювання свідомістю населення.

Регулювання світового інформаційного простору на міжнародному рівні стикається з низкою складних викликів і проблем, основні з яких включають:

1. Юрисдикційні розбіжності. Країни мають різні закони та норми, що регулюють використання інформації та кіберпростір. Це створює складнощі в ситуаціях, коли потрібно визначити, які закони застосовувати в конкретних випадках, особливо коли дані перетинають межі держав (Lahmann, 2020). Кожна держава має свої власні правила та стандарти, що ускладнює створення єдиного міжнародного правового поля, наприклад, у питаннях захисту персональних даних стандарти ЄС суворіші за стандарти інших країн.

2. Безпека даних та конфіденційність. Забезпечення безпеки даних та приватності в умовах, коли інформація легко переміщується через кордони, є величезною проблемою, зумовленою різними законами про захист даних. Необхідним є визначення правил та стандартів для збору, зберігання та обробки великих обсягів даних. Міжнародні організації та держави мають знаходити баланс між захистом особистих даних і вимогами національної безпеки.

3. Кіберзлочинність. Міжнародне регулювання кіберзлочинності є складним через швидкі зміни в технологіях та методах злочинів (Ievdokymov et al., 2024). Існуючі закони часто застарівають швидше, ніж встигають адаптуватися до нових викликів. Складність міжнародного співробітництва у розслідуванні та переслідуванні кіберзлочинців.

4. Культурні та політичні розбіжності. Різні культурні погляди на цензуру, свободу слова та приватність можуть впливати на міжнародні угоди щодо

регулювання інформаційного простору. Прийнятність в одній культурі, не гарантує того ж в іншій.

5. Розвиток технологій. Швидкий розвиток штучного інтелекту та машинне навчання створює нові виклики для регулювання, включаючи етичні питання та потенційні зловживання. Необхідність встановлення єдиних технічних стандартів для забезпечення взаємодії між різними системами та платформами.

6. Міжнародне співробітництво. Посилення міжнародного співробітництва необхідне для ефективного регулювання інформаційного простору, але політичні та економічні інтереси часто ускладнюють процес узгодження та впровадження загальноприйнятих норм і стандартів.

7. Баланс між свободою слова та цензурою. Проблеми визначення та видалення незаконного контенту, такого як мова ненависті, екстремістські матеріали, фейкові новини. Питання відповідальності соціальних мереж та інших платформ за контент, який розміщують їхні користувачі. Наприклад, сервіс Transparency Report від Google надає інформацію щодо запитів до корпорації від держав, змістом яких є видалення контенту з інформаційного простору або надання доступу до персональних даних джерела інформації чи користувачів сервісів корпорації.

8. Монополізація. Домінування великих технологічних компаній, які контролюють значну частину ринку інформаційних послуг, вимагає розробки антимонопольного регулювання міжнародного рівня.

9. Штучний інтелект. Забезпечення етичного використання штучного інтелекту, включаючи питання прозорості, справедливості та відповідальності. Наприклад, розробка та впровадження Китайською Народною Республікою системи розумних міст.

10. Наявність обхідних шляхів регулювання. Інформаційне поле окремої країни не співпадає з державними кордонами, на які поширюється дія нормативно-правових актів, що знижує ефективність їхньої регулятивної спроможності. Наприклад, 16 грудня 2022 року Комісія з надзвичайних ситуацій Республіки

Молдова призупинила дію ліцензій на мовлення шести проросійських телеканалів, проте вони все ще активні через веб-платформи та соціальні мережі.

11. Асиметричність регулятивного впливу. Держави, що мають більшу технологічну перевагу, можуть використовувати додаткові можливості для активного впливу на світовий інформаційний простір. Наприклад, Китайська Народна Республіка активно намагається впливати на світовий інформаційний простір через трансформацію контенту місцевих медіа без маркування, що джерелом є іноземний уряд, через фільтрацію доступу до новинних каналів за допомогою контролю постачання послуг кабельного телебачення в країнах Африки, через вбудовані функції цензурування повідомлень в телефонах, вироблених китайською корпорацією Xiaomi.

Наявність розробленої системи забезпечення національної та міжнародної інформаційної безпеки є основою інформаційного суверенітету держав, забезпечення її гнучкості має спиратися на структурну відповідність мережевій природі простору її функціонування. Управління світовим інформаційним простором є динамічною і суперечливою сферою, перспективними напрямами подолання існуючих обмежень та вирішення проблемних аспектів можуть бути:

1. Глобальна співпраця та багатосторонні механізми. Розробка нових міжнародних угод для врегулювання кібербезпеки, захисту персональних даних та прав людини в цифровому просторі. Створення форумів та платформ для міжнародного діалогу щодо питань глобального управлінням Інтернетом, залученням держав, приватного сектору та громадянського суспільства. Реалізація мережевого підходу до управляння світовим інформаційним простором, що передбачає формування ієрархічної структури множини управлінських груп, які взаємодіють на основі великої кількості взаємозв’язків. Завдяки цьому групи залежать одна від одної в плані ресурсів та об'єднані спільним інтересом. Мережа є гнучкою структурою на відміну від сформованої системи інститутів (Юськів, 2009).

2. Гармонізація законодавства. Узгодження законодавства різних країн для ефективного регулювання світового інформаційного простору,

наприклад, встановлення єдиних стандартів захисту персональних даних для всіх країн.

3. Посилення кібербезпеки. Розробка та впровадження уніфікованих міжнародних стандартів кібербезпеки для захисту критичної інфраструктури та особистих даних. Створення спільних центрів реагування на кіберзагрози, які об'єднують ресурси та інформацію різних країн для оперативного реагування на глобальні кіберзагрози. Використання штучного інтелекту та великих даних для аналізу кіберзагроз, виявлення аномалій та покращення кібербезпеки.

4. Регулювання контенту. Розробка етичних стандартів для платформ соціальних мереж та інших онлайн-сервісів з метою забезпечення свободи слова та запобігання поширенню дезінформації. Використання технологій штучного інтелекту та алгоритмів для автоматичної модерації контенту, поєднаних з людським контролем для забезпечення точності та справедливості (Kuzmenko et al., 2021).

5. Цифрова інклюзія. Запуск міжнародних програм з підвищення цифрової грамотності, особливо в країнах, що розвиваються, та серед вразливих груп населення. Інвестиції в розбудову інтернет-інфраструктури в регіонах з обмеженим доступом до Інтернету для забезпечення рівних можливостей доступу до інформації.

6. Етичні рамки та відповідальність. Розробка та впровадження етичних кодексів для IT-компаній, що регулюють відповідальність за використання даних та розробку технологій. Залучення громадських організацій та спільнот до контролю за діяльністю великих технологічних компаній для забезпечення прозорості та відповідальності.

Світовий порядок демонструє разом з інформатизацією суспільства зростання значимості інформації як визначального ресурсу економічного розвитку, політичного впливу та культурної експансії. Механізми стабілізації/дестабілізації суспільства все більше визначаються діяльністю інформаційних структур та технологічним рівнем розвитку країни. Інформаційний простір стає повноцінним виміром дипломатичних, економічних, військових, культурних відносин.

Глобалізація цього виміру розширює можливості розвитку всіх сфер суспільного буття та викриває нові загрози та виклики через відсутність адаптованої до особливостей світового інформаційного простору системи регулювання.

Управління світовим інформаційним простором зменшує рівень невизначеності та посилює міжнародну та національну інформаційну безпеку. Воно здатне забезпечити посилення позитивних наслідків, попередження чи компенсацію негативних наслідків глобалізації та реалізується заходами на локальному, національному, регіональному та глобальному рівнях. Можливості управління ґрунтуються: на наявних правових нормах та стандартах, їхній пластичності в межах загальних положень міжнародного права та національного законодавства, на ініціативах громадських організацій, експертних об'єднань, які швидше можуть реагувати на актуальні виклики; на використанні інформаційних технологій як внутрішнього механізму регулювання інформаційного простору; на впроваджені мережевого підходу з ієрархічною структурою множини управлінських груп, які взаємодіють на основі великої кількості взаємозв'язків, що відповідає логіці та темпам глобалізації.

Обмеження управління світовим інформаційним простором стосуються: неадаптованого до сучасних динамічних умов та неуніфікованого нормативно-правового забезпечення; відсутності прозорості та неупередженості в міжнародних політичних відносинах через асиметричність в розподілі ресурсів та глибоку інтегрованість інформаційного простору в різні сфери суспільного буття; іррадіації наслідків управлінських заходів у регулюванні світового інформаційного простору на функціонування інших сфер суспільного буття та швидкості розвитку світової інформаційної інфраструктури. Така регуляторна та управлінська обмеженість в міжнародно-правовій сфері визначає необхідність розвитку альтернативних систем інформаційної безпеки як протидії зростаючому масштабуванню загроз.

Проєкт Концепції інформаційної безпеки України (2015) передбачав визначення підґрунтя розвитку потенціалу України в інформаційній сфері, забезпечення її інформаційного суверенітету, захисту та розвитку національного інформаційного простору. Його зміст охоплював також сегмент кібербезпеки, що

забезпечувало цілісність концептуальних засад. Інформаційний захист України передбачав в ст. 4 ч. 2 захист національного інформаційного простору, однак регуляторні основи його забезпечення як прояву управління національним інформаційним простором визначались через можливість запровадження відповідних правових норм. Власне оцінка Концепції відповідно до міжнародних стандартів та зобов'язань ОБСЄ виявила потенційні обмеження свободи слова і думки при здійсненні управління інформаційним простором (Найман-меткалф, 2015).

Розглянемо передбачені заходи для реалізації завдань Стратегії інформаційної безпеки України, враховуючи перспективи масштабування загроз, зважаючи на загальні тенденції цифровізації, інформатизації та інтеграції, яким слідує Україна, а також проаналізовані можливості та обмеження управління інформаційним простором. Згідно з передбаченим Стратегією інформаційної безпеки Планом заходів на період до 2025 року (Розпорядження Кабінету Міністрів України від 30 березня 2023 року № 272-р "Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року", 2023), основними стратегічними завданнями є:

1. Створити систему раннього виявлення, прогнозування та запобігання гібридним загрозам. Така система дозволить здійснювати моніторинг національного та іноземного простору з метою оперативної протидії дезінформації та зловмисним інформаційним впливам, забезпечить можливість превентивного реагування держави та суспільства в цілому на потенційні інформаційні загрози. Реалізація даного завдання передбачає здійснення заходів збору та аналізу інформаційних даних шляхом медіа-моніторингу, моніторингу спеціальними методами іноземних та вітчизняних медіа та Інтернету, системного моніторингу іноземного інформаційного простору, постійного аналізу інформаційного простору, збору та аналітичного опрацювання розвідувальної інформації, систематичного узагальнюючого моніторингу національного та іноземного інформаційного простору, офіційного моніторингу телерадіопростору. Однак реалізація всіх даних заходів передбачається більшою мірою різними

структурними підрозділами, а індикаторами виконання – підготовка відповідних звітних матеріалів. Необхідність створення системи виявлення, прогнозування та запобігання таким чином реалізовується фрагментарно з відсутністю інтеграційної складової в її функціонуванні.

2. Запобігати та протидіяти поширенню дезінформації та деструктивної пропаганди стосовно європейської та євроатлантичної інтеграції України, що передбачає міжнародну співпрацю, популяризацію України в Європі, виявлення зовнішніх інформаційних загроз та своєчасну протидію їхньому впливу, визначення санкцій до фізичних та юридичних осіб за поширення дезінформації, поширення контрінформації щодо наративів та міфів, створених державою-агресором. Передбачені заходи в межах даного завдання частково передбачають виявлення та протидію зовнішнім загрозам, дезінформації, спеціальним операціям в інформаційній сфері, що відповідає необхідності побудови системи інформаційної безпеки, яка б забезпечила узгодженість та оперативність дій.

3. Сприяти підвищенню обороноздатності в інформаційному просторі шляхом створення відповідних структурних підрозділів, їхнього ресурсного забезпечення, проведення навчальних тренінгових програм для підвищення ефективності прогнозування, запобігання та раннього виявлення інформаційних загроз, розробки та проведення тренінгових програм для представників медіа щодо особливостей висвітлення військової тематики в умовах війни, щоб убезпечити від поширення не перевіреної, сфабрикованої та стратегічно важливої інформації.

4. Визначити регулятивні механізми щодо виявлення та обмеження доступу до потенційно небезпечного чи забороненого законом контенту, посилення відповідальності щодо поширення дезінформації та сприянню інформаційним операціям держави-агресора. Дане комплексне завдання передбачає розробку алгоритмів щодо виявлення інформаційних загроз.

5. Підготувати та провести інформаційно-психологічні операції з метою протидії, попередженню чи нівелюванню зловмисних впливів Російської Федерації проти української державності в національному та світовому інформаційному просторі. Зокрема передбачається протидія розповсюдженню відповідної

інформаційної продукції, виготовлення та поширення матеріалів, розробка та підтримання проєктів з метою захисту національного інформаційного простору.

6. Задля ефективної реалізації державної політики в інформаційній сфері сприяти узгодженій діяльності державних органів, органів місцевого самоврядування та інститутів громадянського суспільства. Забезпечити наукове супроводження реалізації Стратегії інформаційної безпеки, зокрема щодо виявлення та реагування на інформаційні впливи держави-агресора. Дане завдання передбачає проведення заходів з налагодження співпраці з метою захисту вітчизняного інформаційного простору та наукового супроводження реалізації Стратегії інформаційної безпеки України, створення єдиної інформаційної платформи

7. Забезпечити розвиток української культури та національної ідентичності шляхом розвитку та забезпечення всебічного функціонування української мови, сприяння популяризації та розвитку українського кінематографа, мистецтва видавництв, медіа простору.

8. Створити умови для консолідації українського суспільства. Заходи спрямовано на сприяння посиленню готовності до захисту Вітчизни в у мовах війни шляхом проведення інформаційних кампаній військово-патріотичної тематики, популяризації військової історії України тощо.

9. Сприяти підвищенню рівня довіри до державних інституцій та правоохоронних органів. Передбачено проведення прес-конференції та публікацій в межах загальної інформаційної кампанії.

10. У внутрішній політиці посилити соціогуманітарну складову, зокрема розглянути питання створення системи соціогуманітарних технологій, що на основі використання сучасних інформаційних технологій дозволить модернізувати діяльність суспільних інститутів.

11. Підвищити рівень медіаграмотності та медіакультури. Розробка та реалізація тренінгових та навчальних програм для закладів середньої освіти, військовослужбовців Збройних Сил, медіафахівців, працівників державних

органів. Проведення просвітницьких, інформаційно-комунікаційних кампаній з медіаграмотності та важливості критичного мислення.

12. Посилити правове регулювання національного інформаційного простору з метою захисту персональних даних, забезпечення доступу до публічної інформації, дотримання принципу безбар'єрності.

13. Визначення системи взаємодії з питань кризового реагування, післякризової комунікації та попередження кризових ситуацій.

14. Сприяти інформаційній реінтеграції громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України, що передбачає поширення наративів про безапеляційного відновлення цілісності території України, протидію інформації, відновлення доступу до національного інформаційного простору, поширення об'єктивної інформації щодо ситуації на окупованих, деокупованих та прилеглих районах, зміцнення почуття спільності між громадянами України тощо.

В глобальних та національних загрозах визначено дезінформацію як одну з провідних загроз, реагування на яку має бути оперативним. «Водночас ефективна система реагування на такі виклики в Україні досі не створена, не забезпечено функціонування розвиненої національної інформаційної інфраструктури, що обмежує можливість належним чином протидіяти інформаційній агресії з метою захисту національної безпеки та реалізації національних інтересів України» (Указ Президента України №685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"», 2021). Створення такої системи є одним із стратегічно важливих завдань інформаційної безпеки, однак за своїм функціональними можливостями дозволить реалізувати й інші стратегічні завдання, деякі в повному обсязі, а деякі частково:

- здійснювати збір, аналіз, систематизацію даних національного та світового інформаційного простору;
- проводити постійний моніторинг інформаційної ситуації та підвищити інформаційну обізнаність;

- виявляти загрози національній безпеці України та вчасно на них реагувати з метою попередження деструктивного впливу, його мінімізації чи нейтралізації;

- оперативно реагувати на дезінформаційну політику держави-агресора та розповсюджувати спростовуючу інформацію, поширювати зміцнюючі репутацію України на міжнародній арені наративи;

- здійснювати оперативне інформування населення про суспільно важливі події, не даючи можливості використовувати державою-агресором паузи, неоднозначності для викривлення інформації, маніпулювання свідомістю;

- забезпечити повноту добування та аналізу розвідувальної інформації;

- сприяти обміну даними щодо інформаційних загроз, кібератак, загальній співпраці з іноземними партнерами в сфері протидії дезінформації ;

- реалізовувати інформаційні кампанії з протидії зовнішнім інформаційно-психологічним впливам;

- впровадити алгоритми реагування на гібридні загрози.

Стратегічні завдання Доктрини інформаційної безпеки України співпадають в ключових напрямах забезпечення інформаційної безпеки в цілому, актуальність забезпечення відповідних стратегічних завдань зберігається через швидкість розвитку інформаційних технологій та складнощів нормативно-правової та технологічної адаптації до темпів розвитку інформаційної сфери (Указ Президента України № 47/2017 від 25 лютого 2017 року «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України"», 2021). Однак визначене як один з пріоритетів державної політики в інформаційній сфері створення інтегрованої системи оцінки та оперативного реагування на інформаційні загрози так і не було реалізовано, як і в актуальній Стратегії інформаційної безпеки передбачається фрагментарне забезпечення створення такої системи. В умовах цифровізації інформаційного простору та транспарантності його геополітичних кордонів її створення матиме велику доцільність та практичне навантаження. Вона посилить співробітницво з іноземними партнерами та може стати основою проактивної позиції України в сфері глобальної інформаційної безпеки, забезпечить високу оперативність

кризового реагування та військових інформаційних операцій, поглибить аналіз інформаційних загроз та ефективність реагування на інформаційні загрози, що дозволить наростити потенціал інформаційного захисту та кіберзахисту. Проблемні аспекти створення даної системи інформаційної безпеки стосуються як теоретичної, так і практичної сторони, оскільки відсутнє концептуальне бачення функціонування такої системи, яке є підґрунтям її розробки в множині необхідних методів та технологій, а також труднощі з технічним забезпеченням та залежністю від міжнародної технологічної підтримки партнерів. В забезпеченні інформаційної безпеки також відсутні індикатори її ефективності, оскільки достатність інформаційної безпеки визначається специфікою глобальних та національних загроз та викликів, а ефективність відображає її актуальні функціональні спроможності. Відсутність розроблених індикаторів інформаційної безпеки не дозволяють її об'єктивізувати та оцінити актуальний стан забезпеченості.

В. Фурашев (2013) визначив базисні індикатори інформаційної безпеки та їхні властивості. Використання даних індикаторів передбачає оцінку повноти інформації відповідно до її достатності для прийняття рішення, розуміння ситуації та повноти реалізації завдань збору інформації. Вчасність інформації визначається як важливість доступу до даних саме в потрібний для прийняття рішень час, як актуальність інформації. Вірогідність інформації є показником її достовірності, конфіденційність – захищеності від несанкціонованого доступу. Цілісність інформації визначається через відсутність викривлення, зміни даних, доступність – через можливість отримання даних. Санкціонованість поширення інформації оцінюється через правомірність та узгодженість дій при розповсюджені інформації. Дані базисні індикатори змістовно відповідають властивостям інформації, однак їхнє визначення є лише результатом теоретичного узагальнення без кількісного чи якісного вимірювання та розробки відповідних методів, індексів, показників. Об'єктивація даних індикаторів є важливим завданням для визначення стану системи інформаційної безпеки України, однак надзвичайно складним для реалізації (Фурашев, 2013, с. 149). Пропонується використовувати реалізаційні індикатори як: наявність та достатність нормативно-правового забезпечення,

ефективність інституційного, економічного та технологічного забезпечення інформаційної безпеки України для протидії реальним та можливим загрозам, а також загальна спроможність протидії інформаційно-психологічним впливам. Такі індикатори є досить загальними, вони можуть бути об'єктивовані через реалізацію відповідних заходів передбачених Стратегією інформаційної безпеки України як забезпечення досягнення стратегічних завдань. Однак така оцінка не буде цілісною, а проблемно орієнтованою.

А. Геворкян (2021) розробив інтегральний індекс оцінки інформаційно-комунікаційного розвитку за регіонами як основи для розробки стратегії забезпечення інформаційної системи України. Інтегральний індекс визначається як лінійна комбінація групових індикаторів, які визначають доступ до інформаційно-комунікаційних технологій, їхнє використання, послуги в інформаційній сфері та е-державні послуги. Звісно така індикація не є достатньою для оцінки забезпеченості інформаційної безпеки, однак дозволяє визначити найбільш вразливі регіони, наприклад, Чегнігівська, Житомирська, Херсонська області (Геворкян, 2021).

Більшість розробок в даній сфері відносяться до власне індикаторів компрометації, тобто інформаційних загроз, наприклад, інфологічна модель факторів, що впливають на інформаційну безпеку, дає можливість оцінити рівень захищеності інформаційно-телекомунікаційних систем від кіберзагроз (Писарчук & Кошара, 2024). Здатність ідентифікації загроз може бути власне індикатором ефективності забезпечення інформаційної безпеки, однак запропонована модель визначає ефективність інформаційної безпеки через призму аналізу кіберзагроз. Розробка індикаторів прицільно інформаційної безпеки є актуальною та визначається як одне з стратегічних завдань Стратегії кібербезпеки України, зокрема до стратегічних завдань також належить необхідність розробки системи інформаційно-аналітичного забезпечення кібербезпеки та постійного моніторингу національного інформаційного простору (Указ Президента України №447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"», 2021).

За відсутності індексів ефективності інформаційної безпеки для її оцінки було використано Національний індекс кібербезпеки (National Cyber Security Index by e-Governance Academy, 2023). Кібербезпека краще об'єктивізується. Сучасний інформаційний простір є цифровізованим, ця тенденція поширюється на все більші сфери суспільного буття. Кіберпростір як сегмент інформаційного простору розширюється. Кібербезпека зазвичай пов'язується з комп'ютерними технологіями, цифровими мережами, інформаційна безпека стосується інформаційних технологій як комунікативних, так і комп'ютерних (Панченко, 2013). З цифровізацією світового інформаційного простору ці поняття все більше зближуються. Національний індекс кібербезпеки відображає готовність країни запобігати кіберзагрозам та керувати кіберінцедентами, його можна розглядати як наближення, оцінку інформаційної безпеки. Він ґрунтується на актуальній оцінці показників та дозволяє аналізувати динаміку в контексті світового рейтингу, який формують 176 країн (рис. 2.2). Кожна точка на даному графіку відповідає перегляду світового рейтингу показників національного індексу кібербезпеки. З 2019 по 2023 рік рейтинг України коливався від 24 до 29 рангового місця. Однак на початок 2024 року цей показник стрімко піднявся до 4 місця, на кінець 2024 року фіксується 15 місце. Такий рейтинг є пластичним і відображає інтенсивність розвитку кібербезпеки у світі. Гібридна війна та довготривала інформаційна експансія Російської Федерації, окупація територій України, розповсюдження дезінформації в світовому інформаційному просторі, кібератаки на об'єкти критичної інфраструктури звісно дали поштовх розвитку кіберзахисту, особливо після повномасштабного вторгнення 2022 року.

За актуальними показниками достатності можливостей кібербезпеки Україна має 81 зі 100%, який може бути конкретизовано за ключовими сферами щодо повноти забезпечення (рис. 2.3). Кожна з даних сфер має індикатори вимірювання, за якими можна визначити достатньо забезпечені та найбільш проблемні.

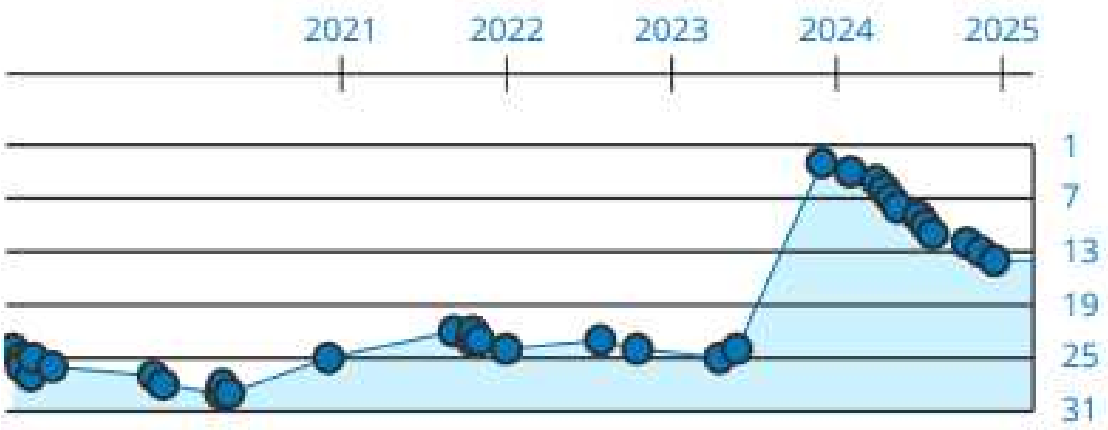

Рис. 2.2. Місце України в світовому рейтингу кібербезпеки з 2019 по 2025 рік

Джерело: National Cyber Security Index by e-Governance Academy, 2025.

Індикатори також поділяються на стратегічні, профілактичні та реактивні. Найвищі показники відзначаються щодо політики кібербезпеки, що визначається за наявністю розробленої національної стратегії кібербезпеки, плану дій, компетентного органу відповідального за керівництво кібербезпекою та реалізацію політики кібербезпеки. Висока достатність також відзначається щодо розвиненості систем, захисту персональних даних, боротьби з кіберзлочинністю, забезпечення військового кіберзахисту та досліджень у сфері кібербезпеки, наприклад, проєкти лабораторії кібербезпеки Національного авіаційного університету. Найнижчі показники достатності відзначаються за стратегічними та реактивними індикаторами. Є необхідність посилення координації та забезпечення управління кіберпростором з метою підвищення оперативності реагування та попередження негативних наслідків кіберінцидентів. Важливою є також проблема достатності в освітньому секторі та міжнародному співробітництві.

В освітньому секторі є необхідність посилення фахової підготовки працівників, а також введення навчальних програм щодо основ інформаційної безпеки в початковій та середній освіті. Це співвідноситься з визначеними загрозами як глобальними, так і національними щодо недостатнього рівня інформаційної культури. Зважаючи на швидкість розвитку цифрових технологій та

їхнє проникнення в різні сфери соціальних відносин та суспільного буття, вивчення основ інформаційної безпеки має бути забезпечене до активного використання цифрового простору. Також важливим є інформування населення щодо розповсюджених загроз та заходів безпеки. В правовому забезпеченні відсутні загальні стандарти інформаційної безпеки для державного сектору та нормативно-правове забезпечення регулювання використання волонтерів у кібербезпеці.

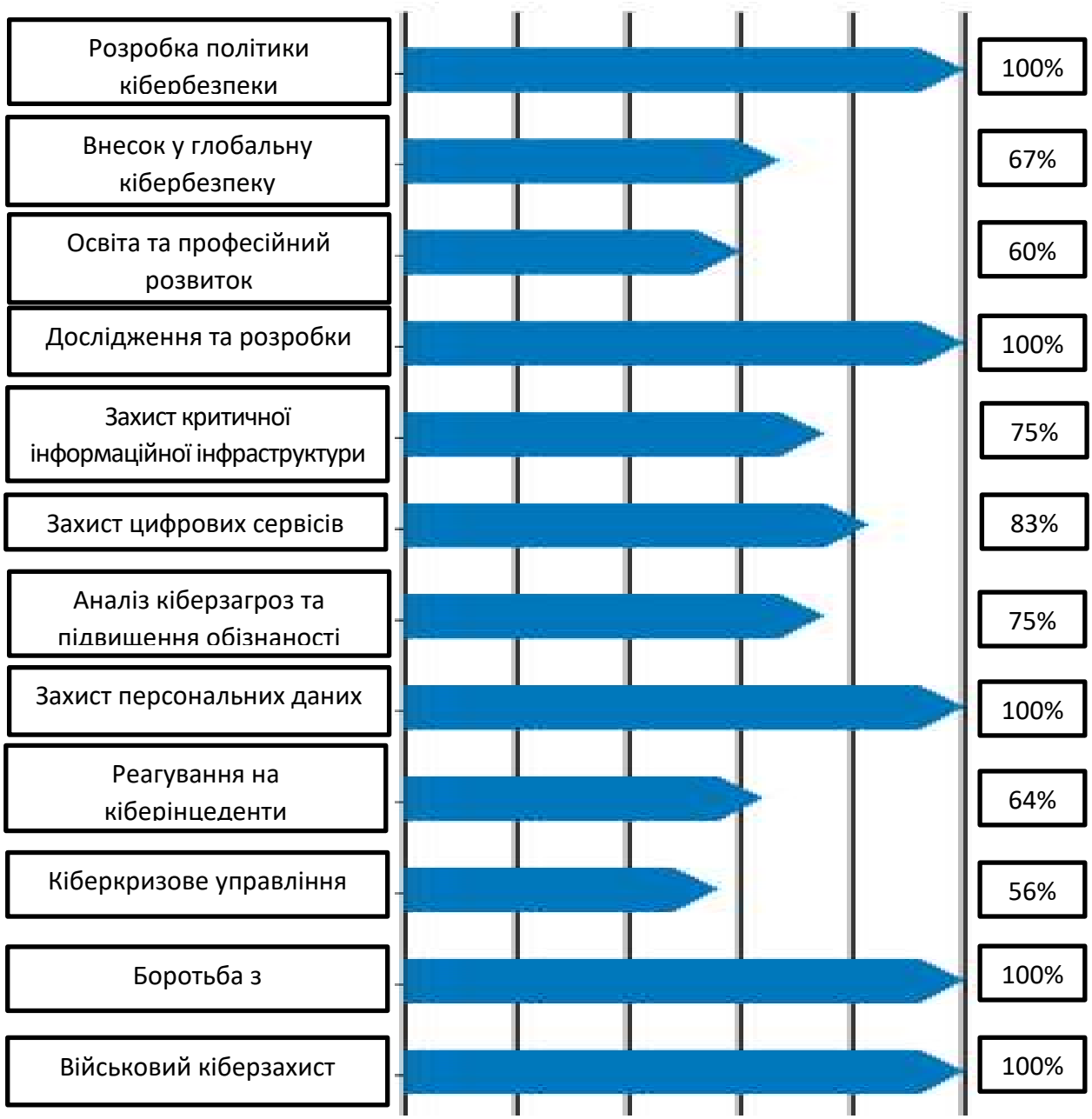

Рис. 2.3. Забезпеченість кіберзахисту України на кінець 2023 року.

Джерело: сформовано автором на основі даних National Cyber Security Index by e-Governance Academy, 2024.

У міжнародному співробітництві ініціація проєктів з кібербезки, участь в діяльності міжнародних організацій, в міжнародній координації кібербезпеки сприяли б розвитку даного сектору національної безпеки. Індикатори внеску у глобальну кібербезпеку є стратегічними, оскільки є важливими для визначення довготривалої перспективи розвитку національної кібербезпеки. Чим більше держава інтегрована в глобальну систему безпеки, тим кращими є механізми та технології її кіберзахисту. Міжнародна співпраця сприяє трансферу технологій, підвищує ефективність навчання за рахунок обміну досвідом та оперативність реагування на загрози. Основою проактивної позиції України в забезпеченні глобальної кібербезпеки є досвід кіберпротистояння, гібридної війни, який можна використати для посилення спроможностей як національної кібербезпеки, так і міжнародної.

Оцінка достатності кібербезпеки України за індикаторами NCSI дозволяє визначити області посилення спроможностей забезпечення інформаційної безпеки, співвідносні з попередньо проаналізованими її викликами та загрозами, а саме створення інтегральної системи моніторингу, реагування на інформаційні впливи та координації дій, підвищення обізнаності населення щодо інформаційної безпеки, посилення міжнародної співпраці та важливість реалізації проактивної діяльності України в даній сфері.

Отже, розробка інтегральної системи інформаційної безпеки України стосується також сегменту кібербезпеки. Її розробка передбачає активне використання науково-аналітичних робіт, що відповідає особливостям інформаційного простору та основним тенденціям глобалізації. Однак в структурі інституційного забезпечення інформаційної безпеки навантаження на науко-дослідні інституції передбачено в мінімальному обсязі та поза реалізацією відповідних даному стратегічному завданню заходів. Цифровізація світового та національного простору збільшує об’єми інформації, швидкість її поширення, масштабність та інтенсивність впливу. Система інформаційної безпеки при цьому має бути озброєною відповідними методами, які будуть спроможні ефективно функціонувати в таких умовах. Для розробки таких систем можуть бути

застосовані сучасні наукові розробки, наразі науково-аналітичне супроводження передбачається як доцільне для виконання лише завдання забезпечення ефективної взаємодії між державними органами, органами місцевого самоврядування та інститутами громадянського суспільства при реалізації інформаційної політики в актуальному Плані заходів. Потенціал використання наукового підходу, наприклад, моделювання та проектування інформаційних процесів, впровадження прогнозування та оцінки ризиків, є значно ширшим та становить основу ефективної реалізації стратегічних завдань щодо протидії дезінформації, моніторингу, розробки системи інформаційної безпеки та забезпечення ефективної реалізації інформаційних операцій.

Реалізацією Стратегії інформаційної безпеки передбачено можливість створення відповідного структурного підрозділу як підвищення спроможностей складових сил оборони в протидії загрозам в інформаційному просторі. Передбачається необхідність відповідного ресурсного забезпечення та фахової підготовки. Такий структурний підрозділ міг би стати основою вирішення проблеми координації діяльності в національному та світовому просторі різних органів державної влади, що залучені до реалізації інформаційної політики в Україні. Створення єдиного інформаційного потоку в цифровому просторі і в протидії дезінформації, і в антикризовому реагуванні, і в кризовій комунікації, і в поширені наративів консолідації українського суспільства є важливим для ефективності інформаційних дій. Основою для розробки такої системи інформаційної безпеки має бути простір її функціонування, вона має бути конгруентною йому. Тільки з врахуванням особливостей, тенденцій розвитку та механізмів функціонування національного та світового інформаційного простору розроблена система інформаційної безпеки буде ефективною, оперативною та цілісною. Створення інтегральної системи інформаційної безпеки дозволить подолати обмеження управління інформаційним простором шляхом реалізації феноменологічного підходу.

Висновки до Розділу 2

Глобальні виклики та загрози інформаційній безпеці України складають зовнішній простір її реалізації, який ґрунтується на внутрішніх можливостях. Обмеженість або слабкі сторони таких можливостей визначають національні загрози та виклики. Глобальними викликами для інформаційної безпеки України можна вважати складний комплексний характер інформаційних впливів та стрімкий розвиток інформаційних технологій, а загрозою глобального та національного масштабу – інформаційні операції Російської Федерації. Внутрішньою національною загрозою інформаційній безпеці України є відсутність системи виявлення та ефективного реагування на інформаційні впливи, що формує плідне підґрунтя для перетворення зовнішніх загроз інформаційній безпеці України у внутрішні небезпеки як негативні явища щодо реалізації національних інтересів та функціонування національного інформаційного простору.

Нормативно-правове забезпечення інформаційної безпеки України включає нормативно-правові акти, що визначають конститутивні засади інформаційної безпеки, її інституційне забезпечення та стратегічні завдання. Однак відсутні прямі доктринальні акти, які б визначали систему ідей, принципів та механізмів державної політики в інформаційній сфері, напрями розвитку інформаційної безпеки, що стали б концептуальним підґрунтям нормотворчої та правозастосовної діяльності, визначення стратегічних цілей та їхньої реалізації, що забезпечило б цілісність функціонування інформаційної безпеки України.

Актуальна інституційна забезпеченість Стратегії інформаційної безпеки України вказує на масштабність, мультиканальність та узгодженість її реалізації, однак при цьому забезпечення інформаційної безпеки України характеризується фрагментарністю, відсутністю функціональної цілісності та нерівномірністю захищеності. Потенційним напрямом підвищення спроможності інформаційної безпеки України є управління інформаційним простором. Серед виокремлених можливостей його реалізації є використання інформаційних технологій як внутрішнього регулятора інформаційного простору та впровадження мережевого

підходу як зовнішнього регулятора при забезпеченні міжнародної інформаційної безпеки.

Потенційними спроможностями посилення інформаційної безпеки України є створення інтегральної системи моніторингу та реагування на інформаційні впливи як ініціативного проєкту в межах реалізації проактивної діяльності України у сфері забезпечення міжнародної інформаційної безпеки.

Створення інтегральної системи інформаційної безпеки забезпечить ефективність виявлення та оперативного реагування на інформаційні впливи та дозволить подолати обмеження управління інформаційним простором шляхом реалізації феноменологічної підходу. В умовах цифровізації інформаційного простору та транспарантності його геополітичних кордонів система інформаційної безпеки має бути конгруентною його особливостям та використовувати технології відповідні його природі. Синергетичні ефекти, характерні для інформаційного простору, сприятимуть розвитку систем штучного інтелекту, а використання штучного інтелекту як асоційованого суб'єкта інформаційної безпеки підвищить її ефективність.

РОЗДІЛ 3
ІНТЕГРАЛЬНА ПРОЄКТИВНА СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

3.1. Достатність інформаційної безпеки України: внутрішні та зовнішні чинники

Глобалізаційні процеси з кожним роком посилюються. Глобалізація стирає географічні кордони, охоплює все більше сфер суспільного буття та поглиблює розростання мережі інтеграційних зв'язків. Розвиток інформаційних технологій здійснює найбільший каталізуючий вплив на глобалізацію соціальної сфери, індикатори якої свідчать про формування світового інформаційного простору, а показники індексу соціальної глобалізації за 2023 рік свідчать про його розширення. Впливовість інформації за умов транспарантності геополітичних кордонів та взаємозалежності країн глобалізованого світу надає інформаційній безпеці виняткової значущості в забезпеченні національної та міжнародної безпеки.

Оскільки світовий інформаційний простір є індикатором глобалізації та здійснює системоутворюючий вплив на основні сфери суспільного буття, то передбачається, що існує зв'язок між глобалізацією економічної, соціальної, політичної сфер та розвиненістю системи інформаційної безпеки. Для перевірки даної гіпотези було здійснено кореляційний аналіз з використанням індексів соціальної, політичної, економічної глобалізації за даними KOF на кінець 2023 року (KOF Index of Globalization, 2023) та національного індексу кібербезпеки, показник цифрового розвитку, тенденції розвитку кібербезпеки за даними NCSI (National Cyber Security Index by e-Governance Academy, 2023) в першій та другій половині 2023 року. Таким чином досліджувані зв'язки розглядалися в динаміці 2023 року.

Перша та друга половини 2023 року мали відмінності за насиченістю подіями значущими для національної та міжнародної безпеки. Перша половина 2023 року відзначається приєднанням Фінляндії до НАТО, що зміцнило міжнародну безпеку в європейському регіоні, активним постачанням зброї Україні. Отже, цей період характеризується консолідацією західних сил. Друга половина 2023 року мала значно вищій конфліктний потенціал: загострення відносин між КНР та Тайванем, посилення протистояння США та КНР щодо Тайванської протоки, вихід РФ з Чорноморської зернової ініціативи, обстріл портової інфраструктури Одеської області України, руйнування Каховської дамби та підвищення ризику аварійної ситуації на Запорізькій АЕС. Отже, цей період відзначається підвищенням напруженості в міжнародних відносинах. Міжнародна кризова група визначила війну в Україні як найбільшу сухопутну війну за останні 60 років, що створює загрозу конфронтації між західними країнами, які надають Україні військову та економічну допомогу, та Російською Федерацією, найбільшою ядерною державою світу (CrisisWatch, 2023). Передбачалося, що відмінність в міжнародній ситуації першої та другої половини 2023 року може проявитися в статистичних показниках результатів кореляційного аналізу, що дозволить виявити контекстуальність достаності інформаційної безпеки. Оскільки чим більш нестабільною є міжнародна ситуація, тим більш вразливими стають взаємозалежні країни в умовах глобалізації. Якщо інформаційний простір дійсно сприяє інтеграції різних сфер суспільного буття, то кореляційний аналіз виявить зв’язок інтенсивності глобалізації та індикаторів інформаційної безпеки.

Для об’єктивації в дослідженні зв’язків глобалізації з інформаційною безпекою було обрано індекс кібербезпеки, оскільки кібербезпека є компонентом інформаційної безпеки і може відображати загальну тенденцію. Кібербезпека легше об’єктивується, що полегшує її вимірювання через статистику кібератак, об’єми передачі даних, кількість центрів обробки даних тощо. Відповідно цифровізація даного сегменту інформаційного простору дозволяє збирати більш об’єктивні дані та мати до них доступ. Попередньо проведений аналіз гістограм розподілу частот індексів економічної, соціальної та політичної глобалізації виявив

відмінність розподілів від нормального, тому для перевірки наявності статистично значущих зв'язків було використано коефіцієнт кореляції Спірмена. Дані першої половини 2023 року містять показники індексів глобалізації економічної, соціальної та політичної сфер, індекс кібербезпеки, показник цифрового розвитку та тенденції розвитку кібербезпеки для 147 країн (табл. 3.1.).

Таблиця 3.1

Зв'язок глобалізації економічної, соціальної та політичної сфер з цифровим розвитком та забезпеченням кібербезпеки в першій половині 2023 року

Показники		Економічна глобалізація	Соціальна глобалізація	Політична глобалізація
Індекс кібербезпеки	Коефіцієнт кореляції Спірмена	0,464	0,457	0,549
	Статистична значущість	<0,001	<0,001	<0,001
Цифровий розвиток	Коефіцієнт кореляції Спірмена	0,493	0,535	0,296
	Статистична значущість	<0,001	<0,001	<0,001

Джерело: сформовано автором.

На основі встановлених статистично значущих зв'язків можна стверджувати, що чим більш інтенсивнішою та масштабнішою є глобалізація в соціальній (ρ=0,457) та економічній сферах (ρ=0,464), тим розвиненішою є система кібербезпеки країни. При цьому чим вищою є цифровізація країни, тим вищою є економічна (ρ=0,493) та соціальна глобалізація (ρ=0,535). Це підтверджує визначену попередньо актуальну тенденцію цифровізації глобального економічного простору та можливих негативних наслідків для інформаційної безпеки країн в умовах взаємозалежності економік та підвищенню ризику зовнішнього втручання в систему їхнього функціонування. Соціальна ж глобалізація та цифровізація мають навіть сильніший зв'язок за рахунок меншої дії стримуючих механізмів на глобалізацію.

В політичній сфері виявлено найбільший за силою зв'язок (ρ=0,549) між глобалізацією та розвиненістю системи кібербезпеки, однак значно менший за силою зв'язок з цифровим розвитком (ρ=0,296). Такі зв'язки вказують, що цифровізація не є визначальним чинником посилення кібербезпеки при зростаючій

політичній глобалізації. При цьому чим більшою є вираженість політичної глобалізації, тим більш вираженою є тенденція посилення кібербезпеки, статистично значущий зв'язок з тенденцією розвитку кібербезпеки виявлено лише з політичною глобалізацією (ρ=0,457 при $p<0,001$). Це може бути зумовлено діяльністю міжнародних організацій, спільними правовими та технологічними ресурсами, а може бути наслідком розмивання геополітичних кордонів та необхідності захисту національного суверенітету в умовах нових важелів впливу на політичній арені. І. Р. Боднар (2014) зазначає, що визначення ризиків в інформаційній безпеці передбачає необхідність врахування засад політичної безпеки, її концептуальних принципів та стандартів. Дане положення емпірично підтверджується виявленим кореляційним зв'язком тенденцій розвитку кібербезпеки та політичної глобалізації.

Дані другої половини 2023 року містять показники індексів глобалізації економічної, соціальної та політичної сфер, індекс кібербезпеки, показник цифрового розвитку та тенденції розвитку кібербезпеки для 151 країни (табл. 3.2.).

Таблиця 3.2

Зв'язок глобалізації економічної, соціальної та політичної сфер з цифровим розвитком та забезпеченням кібербезпеки в другій половині 2023 року

Показники		Економічна глобалізація	Соціальна глобалізація	Політична глобалізація
Індекс кібербезпеки	Коефіцієнт кореляції Спірмена	0,602	0,640	0,752
	Статистична значущість	<0,001	<0,001	<0,001
Цифровий розвиток	Коефіцієнт кореляції Спірмена	0,758	0,883	0,471
	Статистична значущість	<0,001	<0,001	<0,001

Джерело: сформовано автором.

Результати кореляційного аналізу підтверджують встановлені на даних першої половини 2023 року тенденції, відмінність полягає лише в посиленні попередньо виявлених зв'язків. Саме з глобалізацією політичної сфери найбільше

пов’язаний національний індекс кібербезпеки (ρ=0,752), але інтенсивність цього зв’язку стала більшою, як і з глобалізацією в економічній (ρ=0,602) та соціальній (ρ=0,640) сфері. Національний індекс кібербезпеки вимірюється на основі можливостей кібербезпеки, які впроваджуються центральними урядами, а отже його показник дійсно залежить від міжнародної ситуації, політичного становища, інтересів, прогнозованих загроз. Тенденція розвитку кібербезпеки (ρ=0,558 при p<0,001) також посилюється, що підкреслює, що саме політична глобалізаціє впливає на розвиток кібербезпеки. Посилення кореляційних зв’язків підтверджує контекстуальність достаності інформаційної безпеки. Посилення нестабільності міжнародної ситуації позначилось на посиленні інформаційної безпеки взаємозалежних країн, оскільки виявлені статистично значущі кореляції свідчать про прямий зв’язок.

Порівняння гістограм національного індексу кібербезпеки з кривою щільності розподілу в першій та другій половині 2023 року дозволяє візуалізувати дві підгрупи країн: з нижчим та вищим рівнем забезпечення кібербезпеки (рис. 3.1). При цьому групи більш диференційовані в першій половині 2023 року, а в другій за рахунок приросту в розвитку кібербезпеки відмінність між ними стає менш виразною, що відповідає загальній тенденції до підвищення заходів безпеки урядами держав в інформаційній сфері особливо при нестабільності міжнародної ситуації.

Дослідження зв’язку між глобалізацією в економічній, соціальній та політичній сферах та забезпеченням кібербезпеки підтвердили значущості світового інформаційного простору для національної та міжнародної безпеки. Інформаційний простір сприяє інтеграції різних сфер суспільного буття, оскільки виявлено зв’язки інтенсивності глобалізації та індикаторів інформаційної безпеки для всіх трьох основних сфер суспільного буття. Результати кореляційного аналізу свідчать, що інтенсивність глобалізаційних процесів передбачає необхідність розвитку інформаційної безпеки.

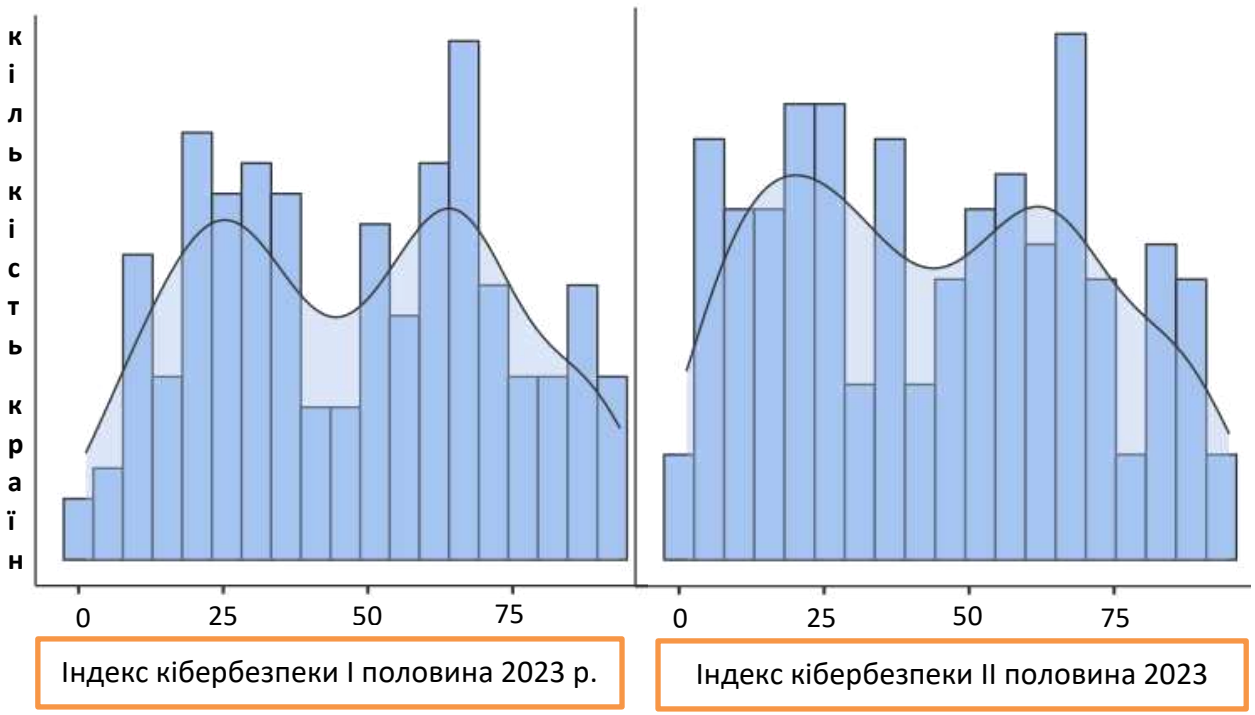

Рис. 3.1. Порівняння розподілів національного індексу кібербезпеки в I та II половині 2023 року

Джерело: сформовано автором.

Порівняння коефіцієнтів кореляції між індексами економічної, соціальної та політичної глобалізації та забезпеченням кібербезпеки з доповненням гістограми розподілу національного індексу кібербезпеки підтвердило, що події, що мають значення для міжнародної та національної безпеки впливають на активізацію захисту інформаційного простору. Оскільки чим інтенсивнішою є глобалізація, особливо в політичній сфері, тим більш масштабними можуть бути загрози та їхні наслідки. Саме політичні чинники є визначальними для приросту інформаційної безпеки.

Зважаючи на проаналізовані чинники глобалізації, тенденції світового розвитку та динаміку глобалізаційних процесів, можемо стверджувати, що мають бути, окрім зовнішніх чинників інформаційної безпеки, які реалізуються у вигляді викликів чи загроз, ще й внутрішні умови, які посилюють чи стримують

глобалізаційні процеси, розвиток інформаційної безпеки та її відповідність викликам майбутнього. Визначальний вплив політичної глобалізації на достатність кібербезпеки та тенденції її розвитку, проблеми управління світовим інформаційним простором через політичні, культурні, юрисдикційні розбіжності приводять до розуміння національних культурних особливостей як глибинних ціннісних засновків функціонування суспільства, національної та міжнародної політики.

Виявлені прямі зв'язки політичної глобалізації з кібербезпекою та тенденцією її розвитку, посилення кібербезпеки як реагування на ризики світової дестабілізації свідчать про те, що інформаційна безпека має вирішальне значення в сучасному цифровому світі, залежність від технологій та впливовість інформації стають визначальними чинниками соціальної, економічної та політичної стабільності. При цьому особливості національної культури та відповідної їй міжнародної політики впливають на різні елементи інформаційної безпеки, що передбачає необхідність врахування міжкультурних відмінностей.

На основі врахування індексів національної культури Г. Хофстеде за базою даних з 113 країн від The Culture Factor Group (Country comparison tool, The Culture Factor Group, 2023) виявлено культурні особливості процесів глобалізації. Культура, за визченням Г. Хофстеде, є колективним програмуванням розуму, специфіку якого пояснюють національні відмінності. Для визначення такої специфіки використовуються шість вимірів, кількісна вираженість яких відповідає таким якісним рівням: високий (70-100), середній (40-69) та низький (0-39). Вимірами національної культури є (Country comparison tool, The Culture Factor Group, 2023):

1. Дистанціювання влади. В основі лежить факт, що всі люди в суспільстві не є рівними. Цей вимір виражає ставлення культури до цієї нерівності. Він визначається як ступінь, до якого менш впливові члени інституцій та організацій у країні очікують і приймають, що влада розподілена нерівномірно.

2. Індивідуалізм проти колективізму. В основі – ступінь взаємозалежності, яку підтримує суспільство між своїми членами, це виявляється в особливостях

самоідентифікації людини через «Я» (індивідуалізм) чи через «Ми» (колективізм). В індивідуалістичних суспільствах люди повинні дбати лише про себе та свою родину. У колективістських суспільствах люди належать до груп, які піклуються про них в обмін на лояльність.

3. Мотивація досягнення та успіху. Фундамент складає питання про джерело мотивації людей: чи це бажанням бути найкращим, чи займатися улюбленою справою. Першому відповідає модель конкуренції з увагою в суспільстві до досягнень, героїзму, самовпевненості та матеріальної винагороди за успіх. Другому відповідає модель консенсусу з увагою в суспільстві до співпраці, скромності, турботи про слабких і якості життя.

4. Уникнення невизначеності. В основі – ставлення до неоднозначності майбутнього, що виявляється в доцільності намагань контролювати його та переживанні тривоги. Різні культури навчилися справлятися з цією тривогою по-своєму. Ступінь переживання загрози невизначеності відображається в моделях поведінки та створенні інституцій її уникання.

5. Довгострокова орієнтація проти короткострокової. В основі – зв'язок минулого з поточними та майбутніми діями: чи варто спиратися на минуле, вирішуючи виклики сьогодення та майбутнього. Суспільства, які мають низький бал за цим виміром, вважають за краще підтримувати перевірені часом традиції та норми, вони з підозрою ставляться до суспільних змін. Суспільства, які мають високий бал, дотримуються більш прагматичного підходу, необхідності змін відповідно до викликів майбутнього.

6. Поблажливість проти стриманості. Цей вимір відображає ступінь свободи, яку суспільні норми надають громадянам у виконанні їхніх бажань. Відносно слабкий контроль за індивідуальними бажання та імпульсами з боку суспільства називається поблажливістю, а відносно сильний – стриманістю.

Для визначення культурних особливостей в глобалізації було використано кореляційний аналіз з коефіцієнтом кореляції Спірмена, оскільки розподіл індексів економічної, соціальної та політичної глобалізації відрізняється від нормального. В економічній сфері глобалізація має статистично значущі зв’язки з такими

вимірами національної культури, як дистанціювання влади, індивідуалізм та довгострокова орієнтація (див. табл. 3.3). Найсильніший зв'язок виявлено з дострокoвою орієнтацією. Дані зв'язки визначають тенденцію, що чим більш спрямованою є країна на майбутнє, прагне враховувати актуальні тенденції, прогнозувати виклики та досягати стратегічних цілей, орієнтується на індивідуальну вигоду, тим більшою буде залученість її до економічної інтеграції. При цьому економічна глобалізація має обернений зв'язок з дистанціюванням влади. Чим більш важливим для суспільства є могутність, владність і значущість, ієрархія та статус на міжнародній арені, тим меншою є економічна глобалізація, яка передбачає побудову та розвиток взаємозалежних економік.

Таблиця 3.3

Зв'язок економічної глобалізації з вимірами національної культури за Г. Хофстеде

Показники		Економічна глобалізація
Дистанціювання влади	Коефіцієнт кореляції Спірмена (ρ)	-0,379
	Статистична значущість (p)	<0,001
Індивідуалізм	Коефіцієнт кореляції Спірмена (ρ)	0,619
	Статистична значущість (p)	<0,001
Довгострокова орієнтація	Коефіцієнт кореляції Спірмена (ρ)	0,683
	Статистична значущість (p)	<0,001

Джерело: сформовано автором.

Зміст виявлених зв'язки було уточнено шляхом побудови діаграм розсіювання з лінією регресії. Це дозволило конкретизувати особливості зв'язку економічної глобалізації та дистанціювання (рис. 3.2).

Виявлений зв'язок має пояснювальну здатність тільки тоді, коли економічна глобалізація стає досить сильною, особливості функціонування влади та ставлення до владної ієрархії стримують подальші глобалізаційні процеси. Подальше посилення економічної глобалізації стримується в країнах з високим

дистанціюванням влади (ρ=-0,370 при p<0,05). Відповідно при нижчій вираженості економічної глобалізації такого статистично значущого зв'язку не спостерігається (ρ=-0,134 при p>0,05).

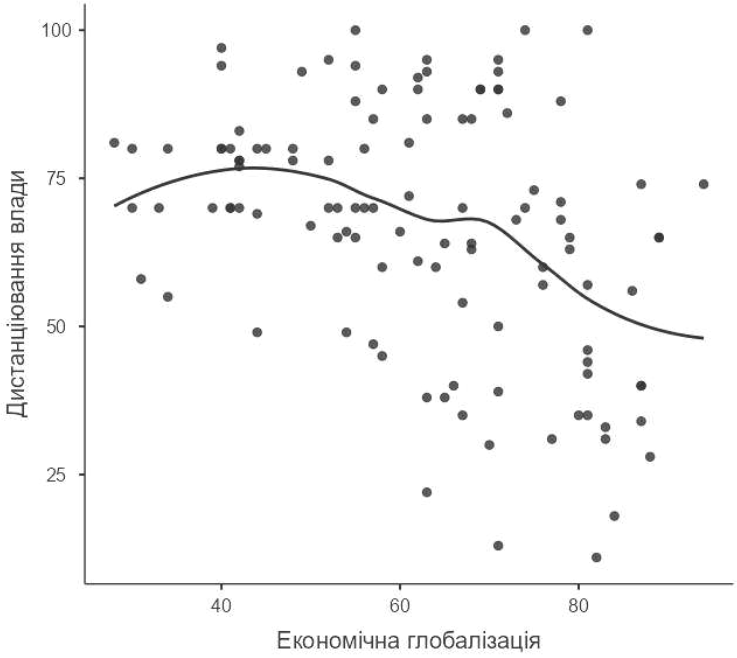

Рис. 3.2. Діаграма розсіюванні: дистанціювання влади та економічна глобалізація

Джерело: сформовано автором.

Аналіз діаграм розсіювання для вимірів, з яким не було виявлено статистично значущого зв'язку дозволив визначити приховані нелінійні тенденції зв'язку, параболічного характеру, між економічною глобалізацією та уникненням невизначеності (рис. 3.3). Залученість до глобальних економічних процесів до певної інтенсивності цієї інтеграції сприяє уникаанню невизначеності (ρ=0,243 при p<0,05), однак при досягненні високих показників глобалізації (більше 70), прагнення уникнення невизначеності стримує її подальший розвиток (ρ=-0,480 при p<0,01). Дана тенденція узгоджується з дистанціюванням влади (ρ=0,393 при p<0,05), чим більшим є прагнення до стабільності, визначеності, структурності, незалежності, тим більшою є цінність владних переваг.

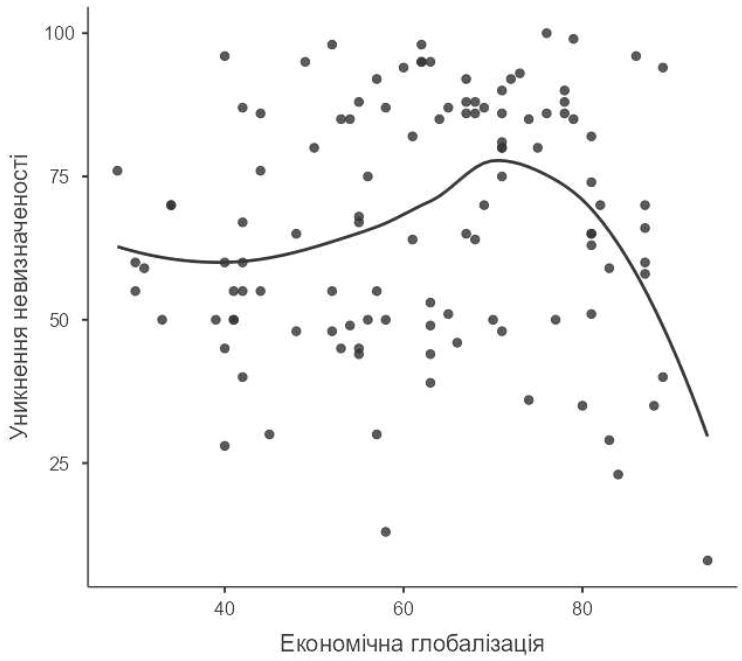

Рис. 3.3. Діаграма розсіюванні: уникання невизначеності та економічна глобалізація.

Джерело: сформовано автором.

Отже, в економічній сфері культурні особливості, які інтенсифікують процеси глобалізації полягають в стратегічному плануванні та оцінці викликів майбутнього, намаганні відповідати актуальним світовим тенденціям, отриманні індивідуальної вигоди та якнайкращого забезпечення власних інтересів. Однак при досягненні високої економічної інтеграції (70 балів) спостерігається активація механізмів стримування, пов'язаних з уникненням економічної взаємозалежності, чутливості національної економіки до поширення економічних криз, вразливості, що визначається особливостями національної культури щодо важливості стабільності, цінності статусу, владних переваг та ієрархічної визначеності у розподілі влади.

В соціальній сфері глобалізація також має статистично значущі зв'язки з такими вимірами національної культури, як дистанціювання влади, індивідуалізм та довгострокова орієнтація (табл. 3.4).

Таблиця 3.4

Зв'язок соціальної глобалізації з вимірами національної культури за Г. Хофстеде

Показники		Соціальна глобалізація
Дистанціювання влади	Коефіцієнт кореляції Спірмена (ρ)	-0,511
	Статистична значущість (p)	<0,001
Індивідуалізм	Коефіцієнт кореляції Спірмена (ρ)	0,747
	Статистична значущість (p)	<0,001
Довгострокова орієнтація	Коефіцієнт кореляції Спірмена (ρ)	0,714
	Статистична значущість (p)	<0,001

Джерело: сформовано автором.

Найсильніший зв'язок виявлено з індивідуалізмом: чим менш згуртованим є суспільство, чим більшої ваги набувають свої власні інтереси, чим більшою є індивідуальна відповідальність та свобода дій, тим інтенсивніші процеси соціальної глобалізації в такому суспільстві. При цьому чим більш прагматичним є суспільство країни, чим більш адаптивним, намагаючись використовувати актуальні можливості, тим більшою буде інтеграція в соціальній сфері. При цьому соціальна глобалізація має обернений зв'язок з дистанціюванням влади. Чим більш прийнятною для суспільства є поляризація влади, контролю, значущість ієрархії та статусу, тим меншою є соціальна глобалізація, яка передбачає розмивання геополітичних кордонів, інтеграцію суспільств та впливовість світової громадської думки.

Зміст виявлених зв'язки було уточнено шляхом побудови діаграм розсіювання з лінією регресії. Це дозволило підтвердити виявлену попередньо при дослідженні економічної глобалізації тенденцію нелінійного зв'язку з дистанціюванням влади та залежності його тенденції від інтенсивності глобалізації (рис. 3.4). При розвитку глобалізаційних процесів в соціальні сфері стримування їхньої інтенсивності спостерігається при досягненні високо рівня інтеграції (більше 75 балів) (ρ=-0,634 при $p<0,01$), тоді чим більш жорсткою є структура влади, чим

більш значущим є контроль, статус, могутність, тим більш стримуються глобалізаційні процеси спрямовані на формування світового громадянського суспільства.

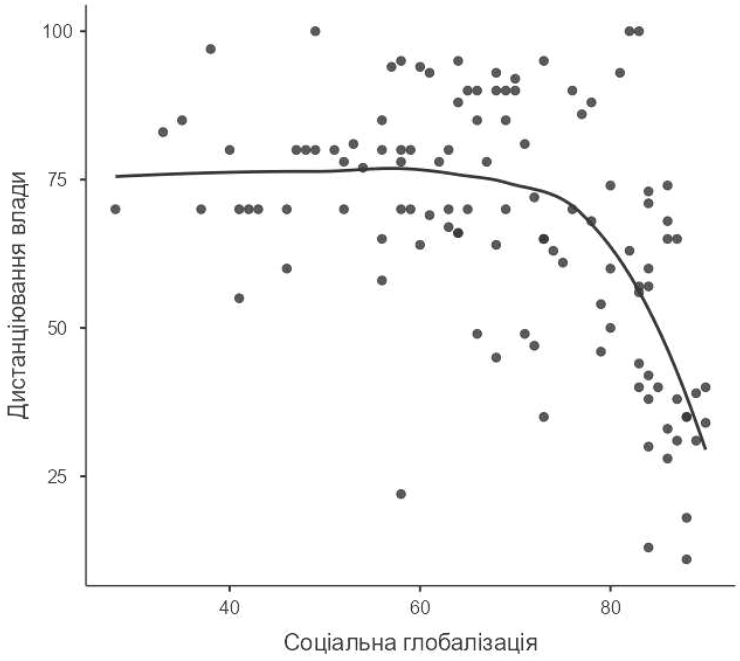

Рис. 3.4. Діаграма розсіюванні: дистанціювання влади та соціальна глобалізація

Джерело: сформовано автором.

Аналіз діаграм розсіювання для вимірів, з яким не було виявлено статистично значущого зв’язку дозволив визначити приховані нелінійні тенденції, зокрема було підтверджено наявність зв’язку параболічного характеру між соціальною глобалізацією та уникненням невизначеності (рис. 3.5).

Даний зв’язок нелінійний, немонотонний, який вказує на зміну напряму зв’язку між уникненням невизначеності та інтенсивністю соціальної глобалізації. До досягнення високої соціальної інтеграції залученість до світової соціальної спільноти сприяє зменшенню невизначеності ($\rho=0,367$ при $p<0,01$), однак надалі мультинаціональність глобалізованого соціального простору в умовах слабко регульованого інформаційного простору створює потенційно складні ситуації, наприклад, відсутності цивілізаційної спорідненості населення країни та мігрантів,

нерівноправності доступу до різних галузей суспільного виробництва, поширення радикальних настроїв (ρ=-0,581 при p<0,01).

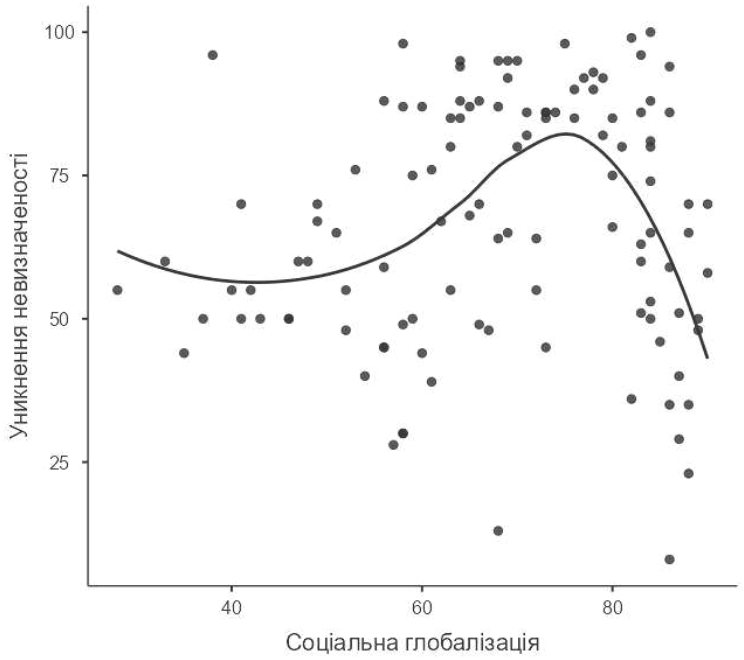

Рис. 3.5 Діаграма розсіюванні: уникання невизначеності та соціальна глобалізація
Джерело: сформовано автором.

На основі аналізу діаграми розсіювання показників соціальної глобалізації та виміру поблажливості виявлено також тенденцію залежності зв'язку від інтенсивності інтеграційних процесів в соціальній сфері (рис. 3.6). Поблажливість сприяє культурному обміну, міграції, новому соціальному досвіду та відкритості до нових ідей.

Між виміром поблажливості та інтенсивністю процесів соціальної глобалізації зв'язок статистично значущій з'являється тоді, коли останні досягають високого рівня (ρ=0,699 при p<0,01). Сприятливою для подальшої соціальної інтеграції є характерна для суспільства свобода самовиявлення, задоволення власних потреб та самореалізації, толерантність до інакшості та відсутність жорстких соціальних норм.

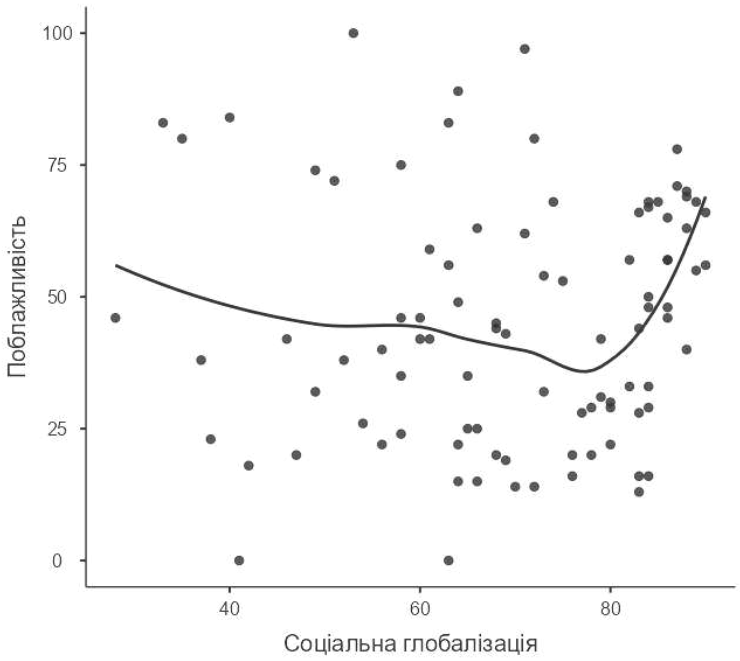

Рис. 3.6. Діаграма розсіюванні: поблажливість та соціальна глобалізація

Джерело: сформовано автором.

Таким чином, глобалізація в соціальній сфері має такі ж культурні спонуки, які полягають у відповідності актуальним тенденціям, стратегічному плануванню, реалізації власних інтересів, використанню можливостей світу соціальних зв'язків без кордонів. Однак при досягненні високого рівня соціальної інтеграції в країнах з характерним дистанціюванням влади та униканням невизначеності починають діяти механізми стримування як реалізація попередження втрати контролю та дестабілізації суспільства, загрози зовнішніх втручань у зміну суспільних настроїв через світовий інформаційний простір. Однак при цьому подальша соціальна інтеграція забезпечується в країнах, суспільство яких є толерантним, вільним від упереджень, необхідності жорсткої відповідності визначеним нормам соціальної поведінки, традиційним формам спілкування.

В політичній сфері глобалізація також має статистично значущі зв'язки з такими вимірами національної культури, як дистанціювання влади, індивідуалізм та довгострокова орієнтація (табл. 3.5).

Таблиця 3.5

Зв'язок політичної глобалізації з вимірами національної культури за Г. Хофстеде

Показники		Соціальна глобалізація
Дистанціювання влади	Коефіцієнт кореляції Спірмена (ρ)	-0,371
	Статистична значущість (p)	<0,001
Індивідуалізм	Коефіцієнт кореляції Спірмена (ρ)	0,424
	Статистична значущість (p)	<0,001
Довгострокова орієнтація	Коефіцієнт кореляції Спірмена (ρ)	0,581
	Статистична значущість (p)	<0,001

Джерело: сформовано автором.

При цьому найсильніший зв'язок спостерігається з довгостроковою орієнтацією. Чим більше суспільство країни орієнтоване на задоволення власних інтересів, керується індивідуальною відповідальністю, має далекоглядне уявлення про майбутнє, оцінює можливі ризики та можливості їх самостійного подолання, тим більшої інтенсивності набувають інтеграційні процеси в політичній сфері спрямовані на спільне вирішення глобальних проблем. Дані зв'язки були також характерними і для економічної, і для соціальної глобалізації, що визначає дію даних вимірів національної культури наскрізними, характерними фасилітаторами глобалізації в цілому. При цьому виявлений обернений зв'язок з дистанціюванням влади було уточнено на основі аналізу діаграми розсіювання (див. рис. 3.7). Попередньо встановлена для економічної та соціальної глобалізації тенденція була підтверджена і для політичної глобалізації, а значить вплив дистанціювання влади також є наскрізним для глобалізації як чинник стримуючого впливу. Його особливістю є наявність порогу інтенсивності глобалізаційних процесів. До досягнення даного значення інтеграційні процеси розвиваються без значимого зв'язку, а після нього починається стримування зростаючої інтеграції в країнах з високим дистанціюванням влади.

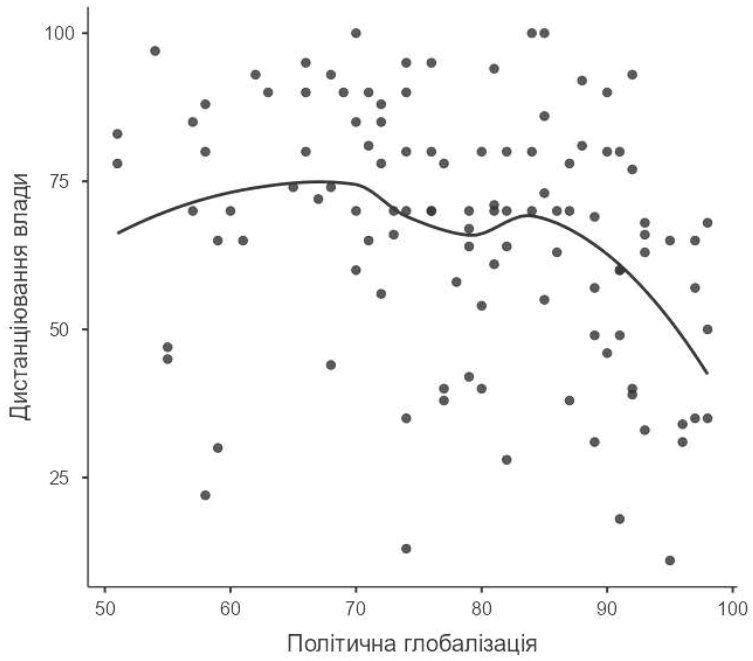

Рис. 3.7. Діаграма розсіюванні: дистанціювання влади та політична глобалізація

Джерело: сформовано автором.

У політичній сфері дистанціювання влади стримує подальшу інтенсивність процесів глобалізації (ρ=-0,448 при $p<0,01$). Якщо для суспільства характерна прийнятність устрою, що ґрунтується на нерівності, владних перевагах, статусі, вагомості та значимості, то в такому випадку висока політична інтегрованість, що в ідеалі передбачає рівноправність, вступає в протиріччя зі звичним для такої культури розумінням державності. В економічній сфері цей вимір протидіє поглибленню залежності національної економіки, в соціальній сфері стримує розмивання національних кордонів та віртуалізації суспільно-політичних відносин, в політичній – ерозію суверенітету, протидіє зміні політичної конфігурації світу з підвищенням значущості мережевих структур та кризою інституту глобального лідерства.

Розвиток інформаційних технологій актуалізує питання безпеки на рівні індивідуальному, суспільному, державному та глобальному, що визначає необхідність превентивних технологічних, інституційних, правових, етичних та освітніх заходів (Admass et al., 2024). Інформаційні впливи можуть мати вражаючі деструктивні наслідки. Найпоширенішими типами інформаційних загроз у 2022

році було визначено соціальну інженерію та дезінформацію (Admass et al., 2024). Інформаційна безпека в контексті розвитку інформаційний технологій та глобалізації характеризується необхідністю оперативного реагування на появу нових загроз і тенденційних викликів, однак цифрова стійкість та специфіка заходів забезпечення інформаційної безпеки відрізняється залежно від культурних особливостей країни. Міжнародний валютний фонд в річному звіті за 2024 рік визначив цифровізацію та розвиток технологій штучного інтелекту одними з ключових чинників невизначеності майбутнього.

За допомогою регресійного аналізу було перевірено, які виміри національної культури визначають розвиненість інформаційної безпеки та готовності до штучного інтелекту. Індекс готовності до штучного інтелекту враховує цифрову інфраструктуру країни, політику щодо людського капіталу та ринку праці, інновації та економічну інтеграцію, регулювання та етику (AI Preparedness Index (AIPI) International Monetary Fund , 2023). Ці чотири виміри визначаються як важливі для плавного впровадження штучного інтелекту. Кожен вимір обчислюється шляхом усереднення набору індикаторів, наприклад:

- для цифрової інфраструктури такими є розвиненість онлайн-послуг державного сектора, використання мобільного телефону для онлайн-транзакцій (% населення), вартість доступу до мережі Інтернет та кількість користувачів на 100 жителів та ін.;

- для політики щодо людського капіталу та ринку праці такими є державні витрати на освіту (середнє за 10 років, % ВВП); цифрові навички серед активного населення, гнучкість визначення заробітної плати та ін.;

- для інновацій та економічної інтеграції такими є готовність передових технологій (кількість наукових публікації, кількість патентів), внутрішній кредит приватному сектору (% ВВП), фінансова відкритість та ін.;

- для регулювання та етики такими є адаптованість законодавчої бази до цифрових бізнес-моделей, ефективність уряду, підзвітність ООН та ін.

Регресійна модель готовності до штучного інтелекту має високу пояснювальну здатність. Ґрунтуючись на показниках вимірів національної культури, вона дозволяє пояснити 78,7% варіативності даних (табл. 3.6).

Таблиця 3.6

Показники якості регресійної моделі готовності до штучного інтелекту

R	R^2	RSME	F	P
0,887	0,787	0,0566	88,6	<0,001

Джерело: сформовано автором.

Отримана модель є статистично значущою. Помилка прогнозу складає 0,0566, що відповідає 5% та в поєднанні з оцінкою точності передбачення готовності до штучного інтелекту дозволяє зробити висновок, що процеси глобалізації, застосування інформаційних технології та розвиток регуляторних механізмів залежать від культурних особливостей країн. Залишки моделі мають нормальний розподіл (тест Колмогорова-Смірнова, p=0,951). Відсутність автокореляції (тест Дарбіна-Утсона, p=0,072), гомоскедастичність залишків (тест Бройша-Пейгана, p=0,249), відсутність мультиколінеарності (VIF<3) свідчить про стабільність регресійних коефіцієнтів та достовірність моделі.

За спаданням визначальної здатності виміри національної культури можна впорядкувати так: індивідуалізм, довгострокова орієнтація та дистанціювання влади (табл. 3.7).

Таблиця 3.7

Коефіцієнти регресійної моделі готовності до штучного інтелекту

Виміри культури	B	t	p	β
Константа	0,41	10,21	<0,001	
Індивідуалізм	0,003	6,93	<0,001	0,550
Довгострокова орієнтація	0,002	5,16	<0,001	0,326
Дистанціювання влади	-0,001	-3,02	<0,01	-0,223

Джерело: сформовано автором.

Готовність до штучного інтелекту як відповідь на потенційні виклики майбутнього визначається не лише зовнішніми чинниками, вони діють через внутрішні культурно специфічні особливості кожної країни, що позначається на міжнародних відносинах та регулюванні інтеграційних процесів. Через це загальні світові тенденції мають не однаковий відгук, наявні внутрішні механізми стримування та інтенсифікації уточнюють також внутрішні виклики для забезпечення інформаційної безпеки.

Індивідуалізм, що має найбільше визначальне значення, відображає вираженість інтеграції на груповому та суспільному рівні, жорсткість чи пластичність соціальної структури суспільства, значимості групових чи індивідуальних інтересів, внутрішній чи зовнішній локус контролю та особливості розуміння соціальної відповідальності. На основі побудованої моделі можемо стверджувати, що чим більшою є вираженість індивідуалізму в національній культурі, тим менше стримуючих внутрішніх чинників для світових інтеграційних процесів та розвитку цифровізації, тим більш підготовленою буде країна до розвитку інформаційних технологій. Більша пластичність суспільства, зацікавленість у власних інтересах та фокусування суспільства на індивідуальній відповідальності кожного сприяють розвитку технологій, зростанню можливостей, адаптивності до нових викликів.

Довгострокова орієнтація відображає важливість стратегічного бачення майбутнього, оцінку короткострокових чи довгострокових перспектив, а відповідно і вирішення нагальних чи стратегічно важливих проблем, орієнтованість на постановку швидкодосяжних цілей чи бачення перспективи, планування далекосяжного майбутнього. Побудована модель свідчить, що країни з вираженою довгостроковою орієнтацією, будучи завбачливими, далекоглядними, оцінюючи ситуацію в перспективі, є більш підготовленими до розвитку інформаційних технологій та глобалізації світу. Глобальні виклики інформаційній безпеці визначають в стратегічній площині та викликають відповідну адаптаційну діяльність, спрямовані на розвиток відповідних секторів, наприклад, економічного, правового чи технологічного.

Дистанціювання влади як важливість влади в суспільстві, ієрархічності соціальної структури на основі владних переваг, їхнього досягнення та втримання. Культури з високим дистанціюванням влади часто мають розкол в суспільстві щодо соціальних винагород та доступу до ресурсів. Володіння владою є бажаним, підтверджує винятковість, впливовість, значимість. Влада є самоціллю. Регресійна модель вказує на стримуюче значення високого дистанціювання влади щодо готовності до одного з найбільших викликів майбутнього. Якщо проаналізувати показники готовності до штучного інтелекту, то фінансова прозорість, сприяння розвитку цифрових навичок та освіченості населення, контроль міжнародного права в інформаційному секторі, – такі зміни зменшують визначальність влади, сприяють суспільним змінам та рівноправності в доступі до можливостей розвитку. Високе дистанціювання влади стримує глобалізацію, як і створює внутрішньої природи бар'єри для готовності до одного з глобальних викликів інформаційної безпеки.

Отже, побудована пояснювальна модель готовності до штучного інтелекту є моделлю готовності до одного з глобальних викликів інформаційної безпеки. Актуальні світові тенденції, що впливають на інформаційний простір, а саме стрімкий розвиток технологій та глобалізація різних сфер суспільного буття, надають штучному інтелекту атрибутів суб'єктності в інформаційному просторі через можливості моніторингу, виявлення інформаційних впливів та протидії їм, прогнозування та попередження. Виявляється, що готовність до даного глобального виклику інформаційної безпеки має культурну специфіку, яка створює внутрішні сприятливі умови чи перепони, тому й управління інформаційним простором має культурно зумовлені обмеження, які при глобалізації можуть ще й загострюватися.

Якщо регресійна модель готовності до штучного інтелекту вказує на готовність до глобальних викликів інформаційній безпеці при подальшій цифровізації та глобалізації, то регресійна модель кіберзахисту вказує на актуальні можливості реагування на загрози інформаційній безпеці.

Пояснювальна здатність регресійної моделі кібербезпеки складає 51% варіативності даних (табл. 3.8). Отримана модель є статистично значущою. Помилка прогнозу складає 16,4, що відповідає 16%.

Таблиця 3.8

Показники якості регресійної моделі індексу національної кібербезпеки

R	R^2	RSME	F	P
0,714	0,510	16,4	46,4	<0,001

Джерело: сформовано автором.

Дана модель демонструє, що національні культурні відмінності не можуть бути достатнім підґрунтям для прогнозування забезпечення кібербезпеки, а її актуальний рівень розвитку залежить в великій мірі також від позакультурних чинників. Залишки моделі мають нормальний розподіл (тест Колмогорова-Смірнова, p=0,768). Відсутні автокореляції (тест Дарбіна-Утсона, p=0,414), та мультиколінеарності (VIF<2). Перевірка на гомоскедастичність залишків (тест Бройша-Пейгана, p=0,007) з діаграмами розсіювання встановила, що індивідуалізм має більшу визначальну здатність для значень, що перевищують 50, тобто в індивідуалізованих культурах регресійна модель менше помиляється, ніж при колективістських культурах. Побудова зваженої регресії дозволила покращити пояснювальну здатність моделі з 47,2% до 51%.

За спаданням визначальної здатності виміри національної культури можна впорядкувати так: індивідуалізм та поблажливість (табл. 3.9).

Таблиця 3.9

Коефіцієнти регресійної моделі індексу національної кібербезпеки

Виміри культури	B	t	p	β
Константа	47,271	10,46	<0,001	
Індивідуалізм	0,627	9,58	<0,001	0,665
Поблажливість	-0,316	-4,18	<0,001	-0,320

Джерело: сформовано автором.

За стандартизованими регресійними коефіцієнтами можемо встановити тенденцію, що країни з індивідуалістськими культурами мають вищі показники кіберзахисту, можливо завдяки індивідуалізації відповідальності та зацікавленості у використанні актуальних можливостей для реалізації власних інтересів. Поблажливість відображає жорсткість регуляторних механізмів поведінки в суспільстві, необхідності слідувати встановленим правилам та нормам. За побудованою моделлю чим більш нормативно підпорядкованою є поведінка людей в суспільстві, тим сприятливіше це впливає на кіберзахист. Чим більше свободи мають громадяни країни у задоволенні власних бажань, тим більше проблемних аспектів в забезпеченні кібербезпеки має така країна. В даному контексті більшої визначеності набувають результати досліджень ризикованої поведінки, що стосується порушень вимог інформаційної безпеки на робочому місці. Якщо ці норми, зважаючи на культурні особливості суспільства, не сприймаються як суворі та обов'язкові, а існує примат задоволення власних потреб, то такі норми порушуються, що зменшує спроможності системи інформаційної безпеки. Відповідно найкращою з точки зору культурних особливостей країни як сприятливих внутрішніх чинників інформаційного захисту є суспільство з високим індивідуалізмом та діючими на підставі особистої відповідальності соціальними нормами та правилами.

На підставі побудованих регресійних моделей як моделі готовності до викликів та моделі спроможності щодо загроз глобалізованого інформаційного простору можна визначити національні культурні особливості як внутрішні умови слідування зовнішнім світовим тенденціям та як внутрішні умови ефективності забезпечення інформаційної безпеки держави. В контексті даних моделей особливості України за культурними вимірами Г. Хофстеде можна розглядати як внутрішні передумови для забезпечення інформаційної безпеки, її ефективності щодо спроможності протидії загрозам та готовності функціонування при актуалізації викликів (рис. 3.8).

Даний профіль дозволяє визначити глибинні рушійні сили української культури. Для побудови використано дані на 16 жовтня 2023 року (Country

comparison tool, The Culture Factor Group, 2023). Використання культурологічного підходу в міжнародних відносинах дозволяє визначити сутнісні ціннісні позиції, які є достатньо стабільними, щоб стати суттєвою перешкодою для реалізації суперечливих їм заходів. Вони сприяють викривленням в сприйманні однієї й тієї ж інформації залежно від ціннісних культурних особливостей. Відповідно до мети наукового дослідження дані особливості України можуть бути проаналізовані як сприяючі чи перешкоджаючі реалізації стратегічних завдань Стратегії інформаційної безпеки України.

Рис. 3.8. Профіль України за культурними вимірами Г. Хофстеде

Джерело: сформовано автором на основі даних Country comparison tool, The Culture Factor Group, 2023.

Високий показник дистанціювання влади свідчить про соціальний розрив між більш впливовими та менш впливовими людьми в суспільстві, про значущість владних атрибутів та соціальних статусів, про домінування управлінського підходу «зверху вниз» та важливість чіткого розмежування повноважень. При цьому суспільство України перехідне, відносно індивідуалістичне, оскільки все більшої значимості набувають досягнення при побудові кар'єри, призначені на посаду, перехід від значимості повноважень до компетентностей. Вектор цінностей задає спрямування не на приналежність, а на забезпечення власних інтересів. Це може пояснюватися переходом цінностей пострадянської ідеології старших поколінь до європейської орієнтованості молоді.

Низька вираженість мотивації досягнення та успіху узгоджується з високим дистанціюванням влади. Применшення власних досягнень більшістю населення, схильність миритися із соціальною несправедливістю в розподілі винагород – це підтримує важливість та переваги владних повноважень, які виправдовують поведінку щодо отримання максимальних благ як доречну та схвальну для представників цього ж соціального класу. Висока вираженість уникнення невизначеності свідчить про прагнення стабільності, схильності до планування, інструктажів, чітко визначених правил, однак дані правила при високому дистанціюванні влади можуть вважатися обов'язковими для більшості та виключенням для владних осіб. Низька вираженість поблажливості, свідчить про загальну стриманість суспільства, обмеженість в реалізації власних потреб, орієнтованості на соціальні норми.

В контексті статистично значущої визначальної здатності кожного з даних культурних вимірів можна припустити, що українське суспільство має внутрішні сприятливі можливості для посилення інформаційного захисту від наявних загроз, оскільки вираженою є тенденція до дотримання соціальних норм та правил в площині особистої відповідальності. Розробка та впровадження стандартів інформаційної безпеки як обов'язкових не тільки в державних установах, а й в приватному секторі разом з заходами підвищення обізнаності населення та медіаграмотності дозволить значно посилити стійкість даного сектору безпеки.

Відсутність таких стандартів та низька інформованість населення визначені як слабкі місця в достатності інформаційної безпеки за оцінкою NCSI. Однак в заходах реалізації стратегії інформаційної безпеки передбачено лише інформування населення, але актуального розвитку індивідуалізму не достатньо, щоб дані освітні та навчальні заходи перейшли в площину внутрішніх регуляторів поведінки, а от реалізація їх як певних норм та стандартів обов'язкового дотримання додасть зовнішній соціальний контроль. Таке поєднання потенційно буде працювати на посилення національної інформаційної безпеки. Що стосується готовності до викликів інформаційній безпеці України, то введення таких норм є необхідністю сьогодення та відповідає тенденції масштабування загроз в майбутньому, адже одним із критеріїв готовності до викликів майбутнього є наявність міжнародних стандартів та механізмів забезпечення їхнього дотримання. В межах регресійної моделі готовності до штучного інтелекту найбільше значення для інформаційної безпеки України має дистанціювання влади (92) при середній вираженості індивідуалізму (55) та довгострокової орієнтації (51), його значення є стримуючим. Особливості таких культур визначаються необов'язковістю дотримання соціальних та правових норм залежно від статусу та владних повноважень в суспільстві. Доступ до державних ресурсів в культурах з високим дистанціюванням влади часто асоціюється з високим рівнем корупції та недієвістю правових та соціальних механізмів стримування. Виходить, що розробка стандартів інформаційної безпеки України та інтеграція міжнародних стримується та ускладнюється через можливість зовнішнього контролю та необхідності забезпечення прозорості в системах регулювання, що суперечить високому дистанціюванню влади.

Визначені зв'язки культурних вимірів України та інтеграційних процесів в економічній, соціальній та політичній сферах дозволяють зробити висновок про сприятливі внутрішні умови для посилення процесів глобалізації. Загальні показники глобалізації України становлять: для економічної сфери 64, для соціальної – 67, для політичної – 87 (KOF Index of Globalization, 2023). Отримані нелінійні залежності свідчать про актуалізацію стримуючого впливу

дистанціювання влади при перетині порогового значення, яке наразі досягнуто лише для політичної глобалізації. Хоча його пояснювальна здатність складає лише 18%, однак в поєднанні з результатами регресійної моделі готовності до штучного інтелекту дистанціювання влади можна вважати значущою внутрішньою завадою для стратегічного розвитку України, що вимагає поглибленого аналізу отриманих зв'язків.

Отже, Україна наразі має плідне підґрунтя для посилення достатності інформаційної безпеки, однак реалізація відповідних заходів, що мають в перспективі зростаюче значення за рахунок посилення регуляторної складової площини міжнародних відносин, стримується високим дистанціюванням влади. Враховуючи такі виявлені тенденції, що асоціюються з корупцією, було доповнено побудовані регресійні моделі індексом сприйняття корупції Transparency International (Corruption Perceptions Index, 2023). Даний індекс сприйняття корупції є найпоширенішим показником корупції в усьому світі. В його основі 13 джерел даних від 12 незалежних установ, що спеціалізуються на аналізі управління та бізнес-кліматі. Таким чином даний індекс дає цілісну комплексну оцінку державного сектору. Даний індекс є показником експертного сприйняття корупції в державному секторі від 0 до 100, де 0 – країна сприймається як дуже корумпована, а 100 – країна сприймається як дуже чиста щодо зловживання владою з метою отримання вигоди. Оскільки корупція включає незаконну діяльність, що приховується, а її розкриття стає приводом для розслідування, судових розглядів та скандалів, тому даний індекс визначається як сприйняття корупції. Дослідники з академічних кіл, громадянського суспільства та урядів мають об'єктивні засновки для вимірюванні корупції в окремих секторах підтверджені дослідом та відповідними зв'язками між індикаторами (Методологія визначення індексу сприйняття корупції, 2022).

Індекс сприйняття корупції було включено в регресійні моделі готовності до штучного інтелекту та індексу національного кіберзахисту, діагностичні показники функціонування кожної з моделей залишилися відповідними попереднім, що дозволяє їх вважати надійними та достовірними. В результаті регресійна модель

готовності до штучного інтелекту отримала приріст пояснювальної здатності з 78,7% до 86,7%. Ієрархічна структура чинників готовності до вимог глобалізованого інформаційного простору змінилася (табл. 3.10). Індекс сприйняття корупції поглинув в моделі дистанціювання влади, оскільки між даними показниками існує достатньо сильний зв'язок (ρ=-0,591 при $p<0,001$). При цьому найбільшу визначальну здатність має індекс сприйняття корупції, потім довгострокова орієнтація, а найменшу – індивідуалізм.

Таблиця 3.10

Коефіцієнти регресійної моделі готовності до штучного інтелекту з врахуванням індексу сприйняття корупції

Виміри культури	B	t	p	β
Константа	0,2	11,55	<0,001	
Індекс сприйняття корупції	0,0048	10,94	<0,001	0,628
Довгострокова орієнтація	0,0017	4,73	<0,001	0,245
Індивідуалізм	0,0008	2,13	<0,05	0,135

Джерело: сформовано автором.

Корупція як негативне суспільне явище узгоджується з культурними вимірами як глибинними ціннісними засновками функціонування суспільства. Дистанціювання влади надає можливості використання влади та суспільного становища для реалізації власних інтересів, отримання особистої вигоди та порушення закону. Готовність ефективно діяти в умовах нового світового порядку пов'язана з глобальною цифровізацією та подальшим зростанням значущості інформації, в таких умовах регуляторні механізми світового інформаційного простору покликані забезпечити достатній рівень інформаційної безпеки будуть перешкоджати реалізації злочинних намірів, функціонуванню корупційних схем.

В регресійній моделі достатності національного кіберзахисту також при додаванні індексу сприйняття корупції підвищується пояснювальна здатність моделі від 51% до 61%. Найбільша визначальна здатність так само, як і в попередній версії моделі, належить індивідуалізму, далі поблажливості, а

найменша – індексу сприйняття корупції (табл. 3.11). Визначені моделі дозволяють оцінити внутрішні умови України щодо сприяння чи перешкоджання готовності до викликів та реагування на загрози в сфері кібербезпеки та інформаційної безпеки в цілому, оскільки кіберпростір є сегментом інформаційного простору, його частка активно зростає у зв'язку з розвитком інформаційних технологій.

Таблиця 3.11

Коефіцієнти регресійної моделі індексу національного кіберзахисту з врахуванням індексу сприйняття корупції

Виміри культури	B	t	p	β
Константа	40,857	8,84	<0,001	
Індивідуалізм	0,454	4,89	<0,001	0,473
Поблажливість	-0,333	-5,00	<0,001	-0,346
Індекс сприйняття корупції	0,333	3,18	<0,01	0,277

Джерело: сформовано автором.

В умовах сьогодення корупція не є визначальною особливістю суспільства, що є значущою для забезпечення достатності інформаційної безпеки, однак вона є діючою перепоною ефективному функціонуванню системи інформаційної безпеки як з точки зору її реформування, так і особливостей реалізації заходів стратегічної значущості як готовності до викликів майбутнього. Індекс сприйняття корупції України складає 36, що дозволяє визначити її, як таку, що сприймається корумпованою. В світовому рейтингу з 180 країн Україна посідає 104 місце на 2023 рік, при тому що світова медіана складає 87, а регіональна – 49. Динаміку даного рангового показника можна прослідкувати з 2012 року, який тоді складав 144 (див. рис. 3.9). За даним графіком Україна демонструє поступове наближення до регіональних тенденцій, однак цей шлях ще досить довгий. Зважаючи на актуальний показник оцінки корупції ідеї «прозорого» світу для України є утопією. Національні культурні відмінності мають більш глибоку ціннісну природу, їхня зміна є складною та довготривалою, що передбачає розвиток нових ціннісних

орієнтирів. Подолання корупції як стримуючого чинника готовності до викликів та спроможності ефективного реагування на загрози інформаційній безпеці України є необхідним. В пояснювальній моделі саме готовності до технологій штучного інтелекту, що визначають майбутні виклики та можливості інформаційної безпеки адаптуватися до нових умов цифровізованого світу, індекс сприйняття корупції має визначальне значення як несприятливий внутрішній чинник.

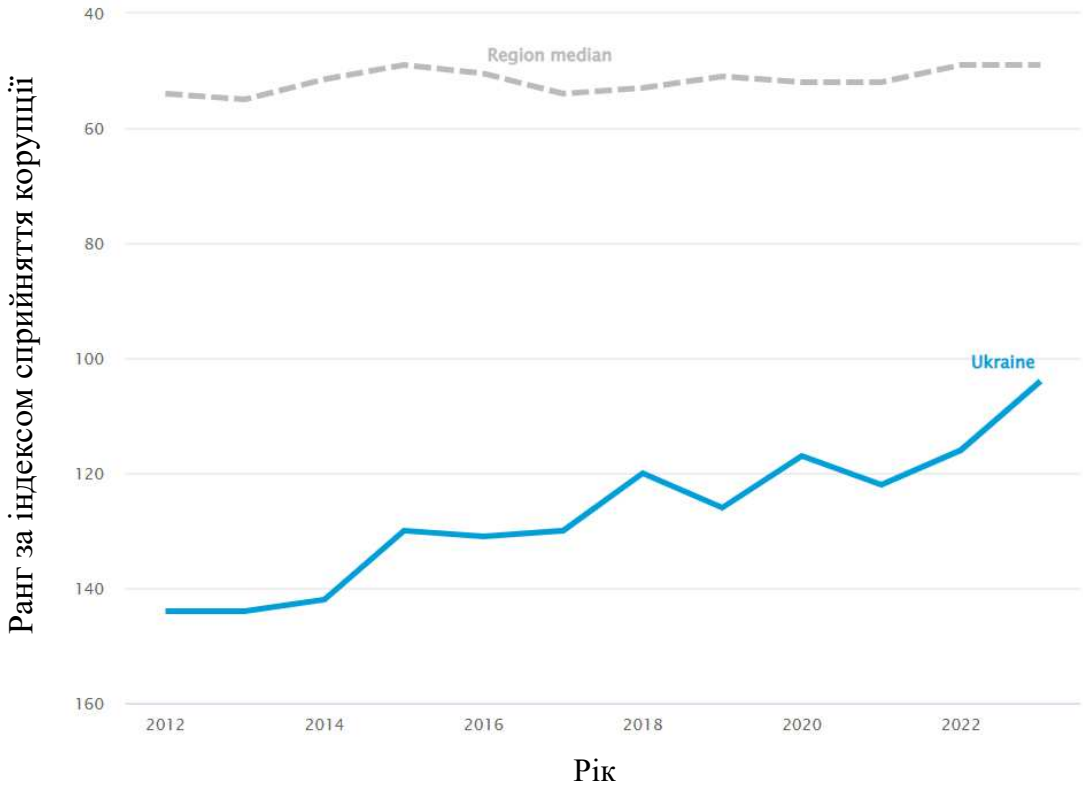

Рис. 3.9. Порядкове місце України в світовому рейтингу індексу сприйняття корупції з 2012 по 2023 рр

Джерело: Corruption Perceptions Index, 2023.

Національні культурні особливості визначають внутрішні чинники забезпечення інформаційної безпеки, доцільність їхнього аналізу узгоджується з обмеженістю управління світовим інформаційним простором саме в аспекті проблеми культурної відповідності міжнародних стандартів. Зважаючи на виявлені національні культурні особливості як внутрішні чинники ефективності забезпечення інформаційної безпеки, з якими узгоджується вплив зовнішніх

чинників глобалізації, запропонована інтегральна проєктивна система інформаційної безпеки може стати оптимальним в актуальних умовах рішенням для посилення спроможностей інформаційної безпеки України, а також в перспективі – платформою міжнародної співпраці. Реалізована в парадигмі управління на основі феноменологічного підходу вона буде здійснювати моніторинг інформаційного простору з використанням технологій моделювання, виявляти латентні чинники, взаємозв'язки, ідентифіковувати загрози, обробляти та узгоджувати великі об'єми інформації з використанням технологій штучного інтелекту. При цьому визначаючи значущість відповідних зв'язків, явищ, проявів як самодостатніх, вона буде реагувати без намагання визначення природи, походження, виконуючи функцію щита. В умовах глобалізації інформаційного простору забезпечення швидкості та своєчасності реагування набуває першопочаткового значення, адже загроза є загрозою сама в собі.

3.2. Концептуальна модель інтегральної проєктивної системи інформаційної безпеки України

Розробка системи інформаційної безпеки відповідно до основних глобальних та національних загроз з врахуванням стратегічних завдань, передбачених заходів як реальних можливостей, та слабких сторін профілю кібербезпеки України за даними NCSI ґрунтується на методологічних положеннях феноменологічного підходу та теорії соціотехнічних систем. Вона передбачає визначення проєктивного інформаційного простору як основи її функціонування.

В умовах посилення глобалізаційних процесів та їх геополітичного масштабування дослідження просторових та просторово часових проблем набувають актуальності. Інформаційний простір, не являючись чітко фізично визначеним, все таки має фізичну протяжність та може бути описаний стосовно часу виникнення інформаційного впливу, швидкості поширення інформації, тривалості інформаційної інтервенції. Можливість збирати великі об'єми даних, дозволяє в результаті аналітичної обробки визначати їхні просторові та часові

маркери. Таким чином інформаційний простір, що являється абстрактною конструкцією, набуває більшої структурної визначеності та об'єктивується. Це дозволяє будувати складні інформаційні та геоінформаційні моделі. При цьому моделі можуть бути статичними та динамічними.

Статичні моделі мають прив'язку до конкретної точки, відстежуваного в інформаційному просторі елементу та його активності. Моделі просторових даних з точковою прив'язкою характеризуються трьома взаємопов'язаними особливостями: стаціонарністю, варіограмами та ізотропією (Ciminelli et al., 2019). Однак статичні моделі не обмежуються лише аспектом моніторингу визначених точок, вони визначають просторово-часові зміни в географії інформаційних процесів, враховуючи зникнення таких точок та появу нових. Якщо розглядати інформаційних простір як реалізацію випадкового набору точок, що розвивається в просторі і часі, то проєктивний інформаційний простір є відображенням точок, значимих для інформаційної безпеки України. Така значимість визначається наявністю визначених атрибутів, як вибору, впливовості, наприклад. Врахування географії інформаційних процесів в точковій представленості дозволяє виявити механізми, що стоять за надходженням нових точок та видаленням точок, що регулюють просторові аспекти додавання і видалення точок, пояснює явища просторового стрибка (González et al., 2016). Такими фізичними точками, наприклад, є центри обробки даних. Масовий збір особистої інформації з боку приватного та державного секторів, розростання соціальних мереж, активне використання хмарних сховищ, цифровізація більшості сфер соціального буття визначають центри обробки даних потенційними мішенями для порушення інформаційної безпеки. Центри обробки даних є осередками фізичного забезпечення IT-систем, обладнання, мережевої інфраструктури та пов'язаних з ними технологій, які забезпечують можливість здійснення більшості IT-процесів, процедур і функцій підтримки (Zhang et al., 2021).

Моделі можуть бути і геодинамічними, які реагують на інформаційні зрушення та сплески активності локаційно та предметно. В побудові таких моделей використовуються дані з багатьох джерел та різних просторових масштабів.

Об’єднання або асиміляція на основі синтезу часто неузгоджених джерел даних дозволяє отримати модель інформаційного простору не фрагментарну, а більш цілісну (Gelfand & Schliep, 2016). Наприклад, поширення дезінформації щодо успішного просування ворога та захоплення певних ділянок фронту може відслідковуватися за маркерами повідомлення на основі об’єднання даних з соціальних мереж, телебачення, пошукових запитів, Інтернет-контенту, повідомлень інформаційних каналів та груп месенджерів. Вони ж можуть поєднуватися з супутниковими даними, наприклад, щодо розміщення позицій ворога, кліматичними даними, щодо локального підвищення температур, точковими даними від місцевих джерел та даними розвідки, центрів обробки даних.

В цілому стаціонарна просторова модель є ідеалізацією, оскільки динамічний аспект все ж таки в ній присутній через структуру зв’язків. Високий ступінь гнучкості коваріаційної структури в умовах глобалізованого інформаційного простору в поєднанні з обмеженістю інформації про коваріаційну структуру при аналізі лише стаціонарних моделей зменшує ефективність заходів інформаційної безпеки (Fuglstad et al., 2015). Моніторинг лише критичних для інформаційної безпеки точок без врахування коваріаційної структури як в глобальному аспекті, так і в локальному з врахуванням її просторової мінливості не дозволить виявити закономірності, розкрити механізми, які можуть мати не лише пояснювальну цінність, а й превентивну щодо впливів на інформаційну безпеку держави.

Інформаційна безпека в реаліях сьогодення активно розглядається як сфера воєнного протистояння та політичного впливу. Створення проєктивного інформаційного простору як геоінформаційної моделі дозволяє розробити та впровадити цілісну систему інформаційної безпеки України. Нові технології сприяють переходу від кінетичного ландшафту до аморфної віртуальної арени протистояння. Воєнні дії згортаються в кіберпростір, однак такі воєнні дії все одно є просторово детермінованими щодо очікуваного результату, оскільки кінцевий об’єкт впливу має зазвичай реальну фізичну та геополітичну представленість. Дані змінюються в часі або в просторі, або і в просторі, і в часі. Поєднання даних з різних джерел дозволить виявляти, які процеси генерували наявні дані та що впливає на

їхню вираженість, інтенсифікує інформаційні процеси та спостережувані ефекти їхньої дії (Fotheringham & Sachdeva, 2022).

Такий підхід глобального моделювання дозволить об’єднати топологічні, географічні та комунікаційні структурні дані про інформаційний простір. Система інформаційної безпеки України, що ґрунтується на відображенні структури інформаційного простору, а саме значимих для інформаційної безпеки структурних елементів як точок, передбачає моделювання інформаційного простору на основі принципу дуальності як структури у формі один-до-одного. В аналогії з можливостями проєктивної геометрії нашим завданням є не перетворення простору зі збереженням пропорцій, не його трансформація, а можливість дати структуру, як відображення точок та ліній незалежно від перспективи. Інформаційний простір як багатомірне утворення в межах проективної геометрії можна представити як набір прямих (гіперплощин), що відображає інваріантне структурне, цей проєктивний простір буде дуальним. Таким чином, маючи інформаційний простір як багатовимірний, ми визначаємо його структуру в єдиній площині інформаційної безпеки України. Відповідно визначення точок такого проєктивного простору залежить від завдань інформаційної безпеки.

Система інформаційної безпеки України, що ґрунтується на проєктивному інформаційному просторі в своїй розробці може спиратися на використання вже існуючих технологій в їх поєднанні та комплексному використанні. За допомогою даних технологій залежно від завдань та заходів інформаційної безпеки може здійснюватися розгортання структури проєктивного інформаційного простору. За аналогією до проєктивної геометрії ми таким чином отримуємо змінювані площини, що дає можливість вивчати об’єкти інформаційного простору з різних точок зору. Аспектами такої зміни можуть бути завдання інформаційної безпеки та особливості аналізованих даних. Джерелами інформації в такому випадку можуть бути відкриті дані: ЗМІ та громадські медіа, Інтернет, соціальні мережі, державні дані, комерційні дані, наукові дані тощо. В цілому потенційно вся інформація, що насичує світовий інформаційний простір. При загальній доступності інформації та оперативності її отримання великий обсяг даних та швидкість поширення

інформації ускладнюють ідентифікацію першоджерел, прогнозування, комплексного аналізу, уникнення викривлення тощо. Дані ефекти зумовлені цифровізацією інформаційного простору, а значить мають застосовуватися інструменти відповідні природі досліджуваних явищ. Відповідні технології наявні та стрімко розвиваються, що зумовило появу приватних організацій, які швидше впроваджують інновації та мають комерційний інтерес у підтриманні технологічно ефективних методів діяльності.

Система інформаційної безпеки має бути конгруентною особливостям світового інформаційного простору, а значить технологічно озброєною та готовою до реагування на зловмисні дії противника, їхнього попередження та цільового впливу (рис. 3.10).

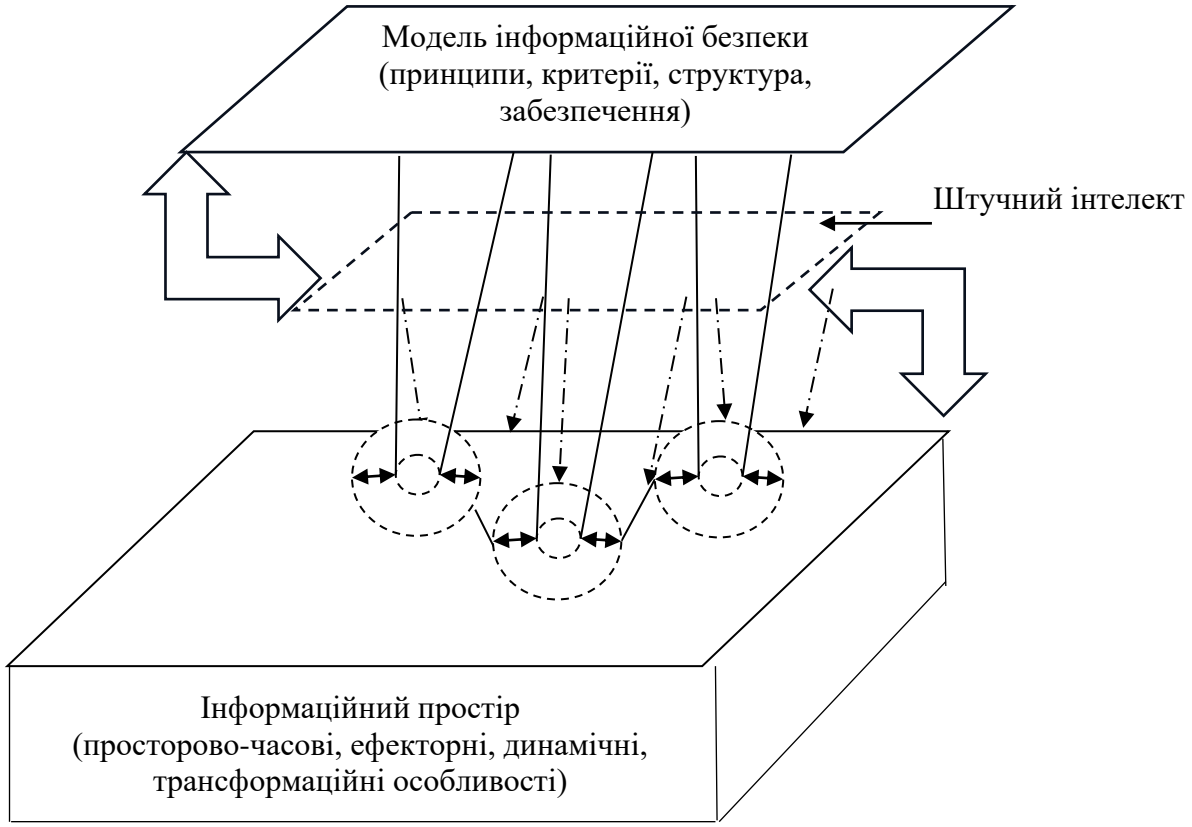

Рис. 3.10. Штучний інтелект в інтеграції інформаційної безпеки та інформаційного простору

Джерело: розроблено автором (Дубовський, 2024с).

Використання технології штучного інтелекту сприятиме інтеграції інформаційного простору та інформаційної безпеки. Особливості інформаційного простору впливають на вдосконалення систем штучного інтелекту, які в свою чергу трансформують інфраструктуру інформаційного простору. Будучи технологією глобалізаційного та цифрового походження, відповідаючи зростаючому масштабуванню загроз, узгоджуючись з тенденціями технологічної сингулярності, системи штучного інтелекту є органічними інфраструктурі світового інформаційного простору, їхнє використання дозволить подолати неконгруентність моделі інформаційної безпеки особливостям глобалізованого інформаційного простору. Розглянемо потенційні можливості такої проєктивної системи інформаційної безпеки України.

Величезні об’єми даних соціальних мереж можуть бути використані для моделювання просторових кореляцій. Соціальні мережі пояснюють взаємодію між людьми. Окремі особи в мережевому аналізі визначаються як вузли, кожен такий суб’єкт має соціальні зв’язки з іншими. Це дає можливість побудувати мережу взаємодій, які описують соціальні відносини. Мережа дозволяє збирати про кожного суб’єкта велику кількість додаткової інформації, крім того, з ким він пов’язаний. Моделювання дозволяє визначити неспостережуване розташування суб’єктів мережі в соціальному просторі та просторовий процес, який існує в цьому просторі на основі виявлених мережевих зв’язків та вузлових атрибутів. Це дозволяє прогнозувати розташування суб’єктів, доданих до мережі на основі коваріат індивідуального рівня (Ciminelli et al., 2019). Для врахування інформації з соціальних мереж може бути застосовано мережевий аналіз з використанням показників центральності в оцінці вузлів, як точок в структурі проєктивного інформаційного простору, та дослідження потоків поширення повідомлень з застосування технологій штучного інтелекту та машинного навчання. Ці технології можуть контролювати та прогнозувати мережевий трафік і статус вузла в режимі реального часу, забезпечуючи своєчасне виявлення потенційних загроз і реагування на них (Zhang et al., 2024). Інтелектуальні алгоритми також можуть визначати топологію мережі, процеси інтеграції та деінтеграції, появу нових вузлів.

Відповідність між соціальними мережами та інформаційним простором може бути реалізовано як представлення соціального простору зав’язків. Суб’єкти, які моделюються як ближчі в соціальному просторі, з більшою ймовірністю матимуть соціальний зв’язок, що вказує на те, що суб’єкти, які перебувають у безпосередній близькості, мають сильні соціальні відносини. Врахування атрибутів членів мережі може здійснюватися шляхом включення в мережевий аналіз моделей вибору та моделей соціального впливу. У моделях вибору зв’язки між членами мережі моделюються на основі фіксованих атрибутів кожного члена мережі. Моделі соціального впливу використовують зв’язки між членами для моделювання атрибутів, що спостерігаються у кожного члена мережі (Wikle et al., 2023). В межах інтегральної проєктивної системи інформаційної безпеки України в контексті структури зв’язків може інтерпретуватися перший закон географії Тоблера: все пов'язане з усім іншим, але близькі речі більш пов’язані, ніж далекі (Ingebrigtsen et al., 2014). У статистичних термінах це означає, що близькі речі мають тенденцію бути більш пов’язаними, залежними, ніж далекі в соціальному просторі.

Дані соціальних мереж можна розглядати і як просторово-часові маркери на геоінформаційній карті, оскільки деякі дописи в соціальних мережах містять інформацію про геолокацію. Величезна кількість користувачів соціальних мереж переглядають та генерують контент, відзначаючи своє місцезнаходження чи свідомо, чи несвідомо. Сучасні методи статистичного аналізу даних дозволяють таким чином прогнозувати ймовірнісні ефекти від подій, можливість розвитку певних явищ з врахуванням їхньої просторової специфіки та протяжності. Моделювання функціональних відносин у зашумлених даних має потенціал для виявлення справжніх латентних тенденцій у даних соціальних медіа (Helwig et al., 2015). Наприклад, даними для аналізу можуть бути результати семантичного сканування дописів в соціальних мережах на наявність певних слів, хештегів, настрою тексту тощо. При реалізації завдань протидії дезінформації, фактчекінгу воєнних подій, наприклад, виявлення неправдивої інформації може здійснюватися на основі мультимодального злиття даних (Guo et al., 2020), визначення неправдивих чуток на основі процесу поширення (Naumzik & Feuerriegel, 2022).

В розробці інтегральної проєктивної системи інформаційної безпеки України цінним ресурсом, що має враховуватися при моделюванні, є експертна інформація. Для традиційних моделей експертні знання значною мірою приховані, хоча потреба у цьому зростає. Експертна оцінка в суспільстві викликає часто більшу довіру, ніж результати кількісних досліджень. Моделі з врахуванням експертних знань можуть бути більш ефективними в описі людської діяльності в ситуаціях, які не легко піддаються збору даних, ніж статистичні моделі оцінки та прогнозування, які можуть бути неточними. Незважаючи на збільшення доступності даних з різних джерел, існує багато ситуацій, для яких дані є обмеженими чи недоступними. Прикладами таких ситуацій є передбачення невидимих подій, таких як потенційне вторгнення, оцінка чисельності та розташування ворога на важкодоступному ландшафті (Brown et al., 2016)**.** В таких ситуаціях використання додаткових джерел, як оцінок експертів, може значно вдосконалити модель. Звісно є труднощі, які варто враховувати. Вони визначають потенційні помилки, як неврахування деяких аспектів знань експертів та упередження.

Локальні моделі можуть бути використані для вимірювання «контекстуальних» ефектів, заснованих на географічно визначеному місці. Інформаційний простір є ширшим за кіберпростір, його використання часто визначається можливостями маніпулювання соціальною поведінкою, впливу на суспільство, ефекти від якого часом є більш значимими за активне воєнне протистояння. Однак в моделюванні соціальної поведінки використання глобальних моделей засвідчило нестаціонарність та високу невизначеність, що потребує калібрування моделі відповідно до особливостей суспільства (Fotheringham & Sachdeva, 2021). Оптимізація втручання щодо попередження чи протидії ворожим інформаційним впливам, стабілізації суспільства має спиратися на статистично надійні пояснювальні моделі. Наприклад, з такою метою може використовуватися географічно зважена регресійна модель, яка буде спроможною виявляти як просторово неоднорідний характер детермінант соціальних настроїв та переконань, так і географічний масштаб, в якому ефекти цих детермінант є відносно стабільними. Оскільки склад населення різниться залежно від просторової

локації, то результати застосування традиційних глобальних моделей не будуть відображати реальну тенденцію. Якщо процеси, що моделюються, є глобальними, тоді локальна модель повторюватиме глобальну. Якщо процеси змінюються в просторі, локальні моделі відображатимуть тенденції точніше та генеруватимуть корисну інформацію про природу просторово змінних процесів шляхом відображення локальних оцінок параметрів. Якщо процеси просторово змінюються, то модель, відкалібрована в одному місці, не буде точно відтворена в іншому місці (Fotheringham et al., 2021). Однак такі відмінності можуть бути основою для встановлення їхнього джерела та більш змістовного аналізу географії інформаційних процесів. Результати локальної оцінки можуть стати основою побудови карт інформаційних процесів. Просторові процеси можна картографувати та аналізувати майже так само, як і просторові дані на основі просторової неоднорідності та залежності (Fotheringham et al., 2021). Співвідношення отриманої карти та формально визначеної структури інформаційних процесів дозволяє визначити та проаналізувати наявні відмінності та зони впливу, реальних акторів та вектори поширення інформації, які виходять за межі геополітичних кордонів.

Безпека інформаційного простору України в проблемному аспекті її реалізації передбачає моніторинг та превентивне реагування на інформаційні дії, що впливають на суспільні процеси. Виявлення зон потенційних конфліктів чи загострення ситуації може здійснюватися з використанням систем моніторингу, наприклад, як CrisisWatch. Він є глобальним інструментом відстеження конфліктів, раннього попередження та запобігання. Він здійснює відстеження подій щомісяця в понад 70 точках геополітичного простору, які визначаються як конфліктні чи кризові. Визначає статус: покращення, незмінність чи погіршення ситуації, можливість вирішення, попередження про ризик конфлікту. Виявлення таких тенденцій дозволяє підвищує загальну обізнаність та зовнішньополітичну пластичність, а можливість ретроспективного аналізу з 2003 року дозволяє відстежувати закономірності та джерела дестабілізації світового порядку. Глобальний трекер конфліктів дозволяє попередити про конфлікти та кризи за три-

шість місяців з метою введення превентивних заходів та стабілізації ситуації (CrisisWatch, 2023). Якщо подивитись дані щодо ситуації в Україні з вересня 2021 року, то статус був про погіршення та незмінність ситуації, а з листопаду по лютий було сповіщення про ризик конфлікту, тобто попередження про конфлікт на основі аналітики міжнародних подій, які описуються в кожний звітній період, було сформовано та уточнювалось на підтвердження впродовж майже 4 місяців. Аналіз всього періоду збройної агресії Російської Федерації проти України демонструє відсутність сприятливого періоду для вирішення конфлікту включно по сьогоднішній час, за даними цієї моніторингової системи. Такого плану інструменти дозволяють визначати ключові тенденції та приймати рішення, а також відслідковувати його ефекти на основі відображення в світовому інформаційному просторі та сприймання міжнародною спільнотою.

Залежно від просторового контексту детермінанти суспільних процесів можуть зміщуватися чи відрізнятися взагалі, тому техніка локального моделювання створює коваріативні смуги пропускання, кожна з яких дає порівняльну міру просторової межі, до якої процес є відносно стабільним. Більша смуга пропускання вказує на процеси, які є більш стабільними в просторі, а глобальна модель є крайнім випадком локальної моделі з надзвичайно великою смугою пропускання (Fotheringham et al., 2021). Такий підхід попереджає дію можливих парадоксів коваріації, наприклад, Сімпсона з взагалі оберненою тенденцією, коли визначальним фактором його появи є не стільки просторові особливості, як пропущений інформаційно важливий чинник, що асоціюється з відповідною просторою залежністю і визначає локальну специфіку моделі. У структурі інтегральної проєктивної системи інформаційної безпеки такі локальні моделі калібруються для кожного визначеного місця, щоб обчислити специфічні для цього місця параметри. Похибка в оцінках локальних параметрів глобальною моделлю спричиняється запозиченням даних з інших місць, де процеси, які створили аналізовані дані, можуть не збігатися з тими, які оцінюються в місці регресії. Якщо припустити, що якщо процеси змінюються в просторі, ця варіація буде невипадковою і виявлятиме певний ступінь просторової залежності, тому зміщення

в оцінках локальних параметрів буде мати тенденцію до збільшення, коли дані запозичуються з більш віддалених місць (Fotheringham & Sachdeva, 2021)**.**

Реалізація такої системи може бути забезпечена поєднанням методів нейронних мереж зі статистичним аналізом точкових патернів, що забезпечить дослідження просторово-часових точкових процесів на основі аналізу різних типів даних (Mateu & Jalilian, 2022)**.** Гнучкість, здатність до узагальнення та масштабованості алгоритмів машинного навчання забезпечує можливість використання для статистичного аналізу складних і багатовимірних даних з просторовими та часовими атрибутами. Для калібрування моделей можуть використовуватися емулятори. Емулятор є моделлю, яка виступає як сурогат для більш складної чисельної моделі (Wikle & Zammit-Mangion, 2023).

Для виявлення зон ризику можуть використовуватися методи кластерного аналізу. Самі методи передбачають визначення просторової структури на основі схожості, суміжності, що може бути представлена у вигляді дистанції в деякому багатомірному просторі упереджень, що перешкоджає значущому відкриттю та інтерпретації. Виявленні значущих просторових скупчень може стосуватися не лише реального фізичного розташування, а й виявлення інформаційного простору як просування певного наративу чи суміжності розрізнених, здавалося, подій, які формуючи кластер дозволяють виділити об’єднуючу їх причинність. Є методи фізичного сканування, які накладають наперед визначену структуру, використовуючи заздалегідь визначене геометричне вікно при оцінці потенційних кластерів. Наприклад, використовується сітка точок з колами різних радіусів. Якщо кількість інцидентів у межах даного кола перевищує очікувану кількість інцидентів для основної популяції, географічна протяжність кола вважається гарячою точкою. Аналогічно, як кругова, так і еліптична статистика просторового сканування використовує заздалегідь визначені геометричні форми для ідентифікації та тестування потенційних скупчень (Murray et al., 2014). Однак, використання заздалегідь визначених геометричних форм може замаскувати фактичну просторову морфологію гарячих точок. Реальні просторові скупчення не обов'язково відповідають геометрії кола чи еліпса, що використовуються для

мозаїки простору. Привнесені структури можуть перешкоджати визначенню глибинних причин виникнення кластерів, виявленню зв'язку між кластерами та їхнім соціальним, економічним та екологічним середовищем. Кластерний аналіз в інформаційному просторі дозволяє визначити подібність між подіями, які кількісно оцінюються на основі, наприклад, частоти подій, географічного розташування, часу, атрибутів та іхньої комбінації.

Отже, інтегральна проєктивна система інформаційної безпеки України може бути реалізована відповідно до принципу дуальності з використанням проєктивного інформаційного простору та основ проєктивної геометрії. Для її розробки є достатньо великий арсенал існуючих технологій та статистичних інструментів, що забезпечують в поєднанні високу функціональну спроможність та оперативність реагування на загрози, можливість прогнозування та попередження зловмисних інформаційних впливів.

Поява нових способів впливу на інформаційну безпеку вимагає цілісного підходу до управління інформаційною безпекою України, що включає технологічні, організаційні та соціальні компоненти. Цілісний підхід до управління інформаційною безпекою наголошує на важливості врахування «людського» елемента при забезпеченні інформаційної безпеки як на рівні окремої організації, так і держави в цілому (Rocha Flores et al., 2014). Ставлення, переконання, норми, соціокультурні особливості, загальна обізнаність населення визначають не лише індивідуальний рівень забезпечення інформаційної безпеки та попереджають можливість ризикованої поведінки, а й визначають пріоритетні напрямки проблемного управління інформаційною безпекою на рівні організації. Організації та об’єкти критичної інфраструктури, навіть будучи закритими системами, все таки мають зв’язок з зовнішнім середовищем через працівників. Дослідження з інформаційної безпеки показали, що організаційний персонал часто не дотримується процедур політики безпеки, віддаючи перевагу ризику, незважаючи на те, що він обізнаний з відповідними інструкціями (Alraja et al., 2023). Управління інформаційною безпекою, що в такому випадку набуває поведінкового аспекту, називається поведінковим управлінням інформаційною безпекою (Rocha Flores et

al., 2014). Моделювання поведінки персоналу об’єктів критичної інфраструктури, створення дерев прийняття рішень щодо ризикованих дій в Інтернеті, використання методів багатомірного шкалювання для реконструкції когнітивного простору цільових груп чи об’єктів впливу, використання пізнавальних та прогностичних технологій для реалізації завдань поведінкового управління дозволить підвищити ефективність заходів інформаційної безпеки та є перспективним напрямом використання можливостей інтегральної проєктивної системи інформаційної безпеки України.

Оскільки загрози інформаційній безпеці стають все більш інструментально складнішими, об’єми інформації для аналітичної обробки зростають виникає необхідність автоматизувати механізм інформаційного захисту за допомогою штучного інтелекту та технологій машинного навчання. Штучний інтелект дозволяє виявляти потенційні загрози, аналізуючи величезну кількість даних, визначати шаблони зловмисних дій та аномалії, оцінювати вразливості, автоматизувати заходи безпеки, підвищити швидкість реагування тощо (Admass et al., 2024). Таким чином звільнити фахівців з безпеки для зосередження на реалізації завдань стратегічного рівня. Інтегральна проєктивна система інформаційної безпеки України може використовуватися не лише, як система моніторингу, прогнозування, спрямована на виявлення загроз, а й як система реагування, що дозволяє за допомогою використання технологій штучного інтелекту автоматизувати деякі процеси, зокрема заходи безпеки, а також використовуватися для розробки стратегічних завдань та при їхній реалізації.

Зв’язність та неперервність простору, можливість його стискання та розгортання дозволяє здійснювати локальне уточнення глобальних тенденцій. Глобальний підхід до реалізації проєктивної системи інформаційного безпеки буде відповідати особливостям світового інформаційного простору, який не є замкненим, а здатний переходити з простору однієї системи в простір іншої, набуваючи локальної специфіки. На основі даної особливості інформаційного простору реалізація інтегральної проєктивної системи інформаційної безпеки може забезпечуватись за рахунок мережевого підходу її структурного забезпечення.

Використання мережевого підходу дозволяє розглядати, як перспективу використання, можливість розгортання даної системи в контексті міжнародної співпраці з забезпечення глобальної інформаційної безпеки. Як прототип міжнародної платформи обміну інформацією, уніфікованої системи інформаційної безпеки, потенційно культурно вільна, інтегральна проєктивна система інформаційної безпеки спирається на визначені можливості управління інформаційним простором, а саме використання інформаційних технологій як внутрішнього механізму регулювання інформаційного простору. Міжнародна співпраця дозволить залучити більшу кількість інструментів, як інтелектуальних, так і технічних для її вдосконалення. Реалізація інтегральної проєктивної системи інформаційної безпеки в такому випадку матиме достатнє ресурсне забезпечення та буде основою попередження конфліктів, насилля, забезпечення демократичних прав та свобод глобального громадянського суспільства. В контексті міжнародної безпеки інтегральна проєктивна система інформаційної безпеки сприятиме підвищенню глобальної компетентності як розуміння глобальних справ і подій, що сприятиме створенню можливостей для їх вирішення. Глобальна компетентність здатна посилити інноваційний потенціал країни, її економічну та військову потужність, стійкість до потрясінь. Вона може служити основою публічної дипломатії, підтримуючи м’яку силу країни та глобальний вплив, зміцнити національні інституції, боротися з дезінформацією та зменшити інформаційну вразливість (George, 2024). Отже, інтегральна проєктивна система інформаційної безпеки може стати основою проактивної діяльності України в міжнародному співробітництві та компенсувати слабкі місця в достатності інформаційної безпеки за оцінкою NCSI. Вона може використовуватися потенційно також при реалізації поведінкового управління в забезпеченні інформаційної безпеки. За рахунок використання технологій штучного інтелекту її спроможності можуть бути розширенні шляхом автоматизації окремих процесів, наприклад, забезпечення інформаційного захисту та відповідного реагування на виявлені загрози.

Висновки до Розділу 3

Достатність інформаційної безпеки є контекстуальним параметром, при цьому визначальними для приросту інформаційної безпеки є політичні чинники, оскільки саме вони впливають на тенденцію її розвитку. Національні культурні особливості є внутрішніми чинниками слідування зовнішнім світовим тенденціям, внутрішніми умовами ефективності забезпечення інформаційної безпеки держави. Наскрізними для економічної, політичної та соціальної сфер внутрішніми чинниками, сприятливими для інтеграційних впливів чинників глобалізації, є індивідуалізм та довгострокова орієнтація, стримуючими – дистанціювання влади. Однак його стримуюча дія активується при досягненні певного порогу інтеграції як реакція на загрозу втрати контролю, дестабілізації суспільства. Для економічної та соціальної сфери таким стримуючим чинником є уникнення невизначеності, що узгоджується з можливими негативними ефектами взаємозалежних економік та ризиків мультинаціональної дезадаптивності суспільств. Компенсаторним чинником для соціальної сфери в таким умовах виступає поблажливість, дія якого активується також порогово при посиленні інтеграційних процесів, що забезпечує толерантність до інакшості.

Модель національного індексу кібербезпеки визначає сприяючі внутрішні чинники достатності інформаційній безпеці, а саме високий індивідуалізм та діючі на підставі особистої відповідальності соціальні норми та правила. Модель готовності до штучного інтелекту визначає внутрішні чинники готовності держави до провідного світового виклику для інформаційної безпеки в умовах глобалізації та цифровізації інформаційного простору. Виявлено, що сприятливими національними культурними особливостями є довгострокова орієнтація та індивідуалізм, стримуючий вплив має дистанціювання влади. При цьому рівень корупції є стримуючим чинником для забезпечення достатності інформаційної безпеки, а для готовності до глобальних викликів майбутнього він є ще й визначальним.

Виявлені закономірності дозволяють проаналізувати достатність інформаційної безпеки України через призму національних культурних особливостей як внутрішніх чинників її детермінації. Вираженість індивідуалізму та довгострокової орієнтації є сприятливими як для розвитку інтеграційних процесів глобалізації, так і для готовності до штучного інтелекту як виклику майбутнього для національної та міжнародної інформаційної безпеки. Однак дистанціювання влади України та асоційований з ним рівень корупції мають стримуючий вплив на процеси політичної глобалізації, позначаються на забезпеченні достатності інформаційної безпеки та найбільшою мірою на її готовності до викликів майбутнього. Розуміння внутрішніх чинників детермінації достатності інформаційної безпеки України є важливими для розробки заходів її посилення. Слабкою стороною забезпечення достатності інформаційної безпеки є відсутність загальних стандартів інформаційної безпеки та низька інформованість населення, однак в заходах реалізації Стратегії інформаційної безпеки України передбачено лише інформування населення, але актуального розвитку індивідуалізму недостатньо, щоб дані освітні та навчальні заходи перейшли в площину внутрішніх регуляторів поведінки, а от реалізація їх як певних норм та стандартів обов'язкового дотримання додасть зовнішній соціальний контроль та забезпечить більшу ефективність, зважаючи на актуальний рівень культурного виміру поблажливості. В умовах сьогодення дистанціювання влади та корупція не є визначальною особливістю суспільства для забезпечення достатності інформаційної безпеки, однак вони є діючою перепоною ефективному функціонуванню системи інформаційної безпеки України як з точки зору її реформування, так і особливостей реалізації заходів стратегічної значущості довгострокової орієнтації.

Інтегральна проєктивна система інформаційної безпеки України є оптимальним в актуальних умовах рішенням для посилення спроможностей інформаційної безпеки України. Дана концептуальна модель, відповідно до принципу дуальності та основ проєктивної геометрії, передбачає побудову проєктивного інформаційного простору, що дозволить об'єднати топологічні,

географічні та комунікаційні структурні дані. Інтегральність системи реалізується використанням технологій штучного інтелекту, що трансформує суб'єктність в цифрову площину як перехід від агрегування даних до аналізу, що дає змогу не тільки виявляти загрози, а й здійснювати проактивний пошук. Для розробки інтегральної проєктивної системи інформаційної безпеки України є достатньо великий арсенал технологій та статистичних інструментів, що забезпечують в поєднанні високу функціональну спроможність системи щодо виявлення саме інформаційних загроз. Розробка та впровадження даної системи забезпечить безперервність моніторингу інформаційного простору, оперативність виявлення загроз та відповідного реагування, можливість прогнозування та попередження негативних наслідків інформаційних впливів, узгодженість діяльності різних структурних підрозділів.

Інтегральна проєктивна система інформаційної безпеки України потенційно може стати основою проактивної діяльності України в забезпеченні міжнародної інформаційної безпеки та міжнародного співробітництва в інформаційній сфері: бути прототипом міжнародної платформи обміну інформацією, уніфікованою системою інформаційної безпеки; реалізуватися як культурно вільна система моніторингу та оперативного реагування на загрози; стати основою функціонування мережевого підходу до управління світовим інформаційним простором; сприяти підвищенню глобальної компетентності.

ВИСНОВКИ

Реалізація завдань дослідження інформаційної безпеки України в умовах глобалізації світового інформаційного простору дозволила досягти поставленої мети та сформулювати наступні висновки:

1. Відповідно до даних теоретико-методологічних засад інформаційна безпека розглядається автором роботи як об'єктно-суб'єктний феномен, що визначає умови функціонування суб'єктів в інформаційному просторі, конституйованому глобалізацією. Методологічним підґрунтям дослідження визначено феноменологічний підхід, відповідно до якого конституювання інформаційної безпеки веде до конституювання просторових речевостей та суб'єктів, що відповідає розумінню інформаційного простору як об'єкта інформаційної безпеки та узгоджується з положеннями теорії соціотехнічних систем. У результаті аналізу основоположних концепцій теоретичного осмислення інформаційної безпеки визначено теорію соціотехнічних систем як основу інтеграції техніко-технологічного та соціально-психологічного аспектів забезпечення інформаційної безпеки в умовах глобалізації. Положення теорії соціотехнічних систем визначають інформаційний простір середовищем життєдіяльності соціотехнічних систем, відповідно їхня захищеність та ефективність функціонування залежать від врахування його особливостей. Забезпечення інформаційної безпеки реалізується на індивідуальному, загальному та захисному рівні, одним з механізмів останнього є управління інформаційним простором. Встановлено, що світовий інформаційний простір є інфраструктурним середовищем розгортання системи інформаційної безпеки та масштабується відповідно до інтенсивності процесів глобалізації.

2. Глобальні виклики та загрози інформаційній безпеці України задають зовнішній контур, контекст забезпечення інформаційної безпеки, її відповідність актуальним тенденціям глобалізації, визначають значущість готовності до розвитку інформаційних технологій та необхідність посилення актуальних та потенційних спроможностей. Національні загрози та виклики відображають слабкі сторони та обмеженість інформаційної безпеки України. Глобальними

викликами для інформаційної безпеки України визначено складний характер інформаційних впливів та стрімкий розвиток інформаційних технологій, а загрозою глобального та національного масштабу – інформаційні операції Російської Федерації. Внутрішньою національною загрозою інформаційній безпеці України є відсутність системи оперативного виявлення та ефективного реагування на інформаційні впливи, що формує підґрунтя для перетворення зовнішніх загроз інформаційній безпеці України у внутрішні небезпеки як негативні явища щодо реалізації національних інтересів та функціонування національного інформаційного простору. У нормативно-правовому забезпеченні інформаційної безпеки України відсутні доктринальні акти, які б визначали систему ідей, принципів та механізмів державної політики в інформаційній сфері, напрями розвитку інформаційної безпеки, що стали б концептуальним підґрунтям нормотворчої та правозастосовної діяльності, визначення та реалізації стратегічних цілей як короткострокових, так і довгострокових, що забезпечило б цілісність функціонування інформаційної безпеки України та її стратегічний розвиток. Актуальна інституційна забезпеченість реалізації Стратегії інформаційної безпеки України характеризується масштабністю, мультиканальністю та узгодженістю, однак при цьому забезпеченню інформаційної безпеки України притаманна фрагментарність, дублювання завдань, відсутність функціональної цілісності та нерівномірність захищеності.

3. Потенційним напрямом посилення спроможності інформаційної безпеки України є реалізація управління інформаційним простором як механізму захисного рівня інформаційної безпеки. Його обмеженнями визначено: неадаптованість до сучасних динамічних умов та неуніфікованість нормативно-правового забезпечення; відсутність прозорості та неупередженості в міжнародних політичних відносинах; культурні розбіжності в розробці стандартів інформаційної безпеки; іррадіація наслідків управлінських заходів у регулюванні світового інформаційного простору на функціонування інших сфер; швидкість розвитку інформаційних технологій. Серед виокремлених можливостей управління інформаційним простором перспективним є використання інформаційних

технологій як внутрішнього регулятора інформаційного простору та впровадження мережевого підходу як зовнішнього регулятора в контексті забезпеченні міжнародної інформаційної безпеки. Концептуальною моделлю їхньої реалізації, заснованої на феноменологічній парадигмі управління інформаційною безпекою, є створення інтегральної проєктивної системи інформаційної безпеки України.

4. Достатність інформаційної безпеки є контекстуальним характеристикою, що реагує на зміни в міжнародній безпековій ситуації. Встановлено, що визначальними для приросту інформаційної безпеки є політичні чинники, оскільки саме вони впливають на тенденцію її розвитку. Особливості трансформаційного впливу чинників глобалізації на інформаційну безпеку, тенденції її розвитку, проблеми управління світовим інформаційним простором через політичні, культурні, юрисдикційні розбіжності приводять до розуміння національних культурних особливостей як внутрішніх чинників достатності інформаційної безпеки. Наскрізними для економічної, політичної та соціальної сфер сприятливими для глобалізації культурними вимірами є індивідуалізм та довгострокова орієнтація, стримуючими – дистанціювання влади, його стримуюча дія активується при досягненні певного порогу інтеграції як реакція на загрозу втрати контролю. Для економічної та соціальної сфери таким стримуючим чинником є уникнення невизначеності, що узгоджується з можливими негативними ефектами взаємозалежних економік та ризиків мультинаціональної дезадаптивності суспільств. Компенсаторним чинником для соціальної сфери в таким умовах виступає поблажливість, дія якого активується також порогово при посиленні інтеграційних процесів, що забезпечує толерантність до інакшості. Регресійні моделі національного індексу кібербезпеки та готовності до штучного інтелекту конкретизують детермінаційний вплив даних чинників в забезпеченні інформаційної безпеки. Сприятливими чинниками достатності інформаційної безпеки є високий індивідуалізм та діючі на підставі особистої відповідальності соціальні норми та правила. Готовність до найбільшого виклику майбутнього, а саме до штучного інтелекту, визначають довгострокова орієнтація та індивідуалізм, стримуючий вплив має дистанціювання влади. При цьому рівень

корупції, асоційований з дистанціюванням влади, є значущим стримуючим чинником для забезпечення достатності інформаційної безпеки, а для готовності до глобальних викликів майбутнього цей чинник є визначальним. Виявлені закономірності дозволяють оцінити достатність інформаційної безпеки України через призму сприяючих та стримуючих зовнішніх та внутрішніх чинників, що є важливими для розробки заходів її посилення. Загальними тенденціями розвитку інформаційної безпеки України є інтенсифікація розвитку сектору кібербезпеки; масштабність, мультиканальність та узгодженість забезпечення інформаційної безпеки.

5. Потенційною спроможністю посилення інформаційної безпеки України є розробка інтегральної проєктивної системи, що ґрунтується на принципі дуальності та основах проєктивної геометрії та передбачає побудову проєктивного інформаційного простору. Інтеграційні можливості забезпечення такої відповідності реалізовуються використанням технологій штучного інтелекту. При цьому синергетичні ефекти, характерні для інформаційного простору, сприятимуть розвитку систем штучного інтелекту, а використання штучного інтелекту як асоційованого суб'єкта інформаційної безпеки підвищить її ефективність. Інтегральна проєктивна система інформаційної безпеки України є концептуальною моделлю, яка дозволяє поєднати науково-аналітичні розробки та інформаційні технології не лише в сегменті кібербезпеки, а відповідно до викликів та можливостей цифровізації інформаційного простору в соціально-психологічному вимірі. Розробка та впровадження даної системи забезпечить безперервність моніторингу інформаційного простору, оперативність виявлення загроз та відповідного реагування, можливість прогнозування та попередження негативних наслідків інформаційних впливів, посилить узгодженість діяльності різних структурних підрозділів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications, 2*. https://doi.org/10.1016/j.csa.2023.100031

2. AI Preparedness Index (AIPI) International Monetary Fund. (2023). https://www.imf.org/ external/datamapper/datasets/AIPI

3. Alguliyev, R. M., Imamverdiyev, Y. N. & Mahmudov, R. Sh. (2020). Information security as a national security component. *Information Security Journal: A Global Perspective, 30*(1), 1−18. http://dx.doi.org/10.1080/19393555.2020.1795323

4. Alraja, M. N., Butt, U. J., & Abbod, M. F. (June 2023 p.). Information security policies compliance in a global setting: An employee's perspective. *Computers & Security*, 129. https://doi.org/10.1016/j.cose.2023.103208

5. Asmadi, A., Almutahar H., Sukamto, S., Zulkarnaen, Z., Listiani, E.A. & Sikwan, A. (2023). Digital Information Security Policy in the National Security Strategy. *International Journal of Multidisciplinary Approach Research and Science, 1*(02), 96−103. http://dx.doi.org/10.59653/ijmars.v1i02.61

6. Babenko, V., Perevozova, I., Mandych, O., Kvyatko, T., Maliy, O., & Mykolenko, I. (1 August 2019 p.). World informatization in conditions of international globalization: Factors of influence. *Global Journal of Environmental Science and Management*. doi:10.22034/GJESM.2019.05.SI.19

7. Bloch, M., & Barros, J. (2011). Physical-layer security: from information theory to security engineering. *Cambridge University Press*.

8. Bondar, V. (2023). Artificial intelligence as a tool of public administration in ensuring informational and psychological security. USA experience. *Journal of Scientific Perspectives, 12*(42), 81−87. https://doi.org/10.52058/2708-7530-2023-12(42)-80-87

9. Bortnikova, O., Kashperska, D., Leonov, O., Rubel, K., & Chumak, O. (2024). Information security of the state: motives, necessity, and sufficiency criteria. *Lex*

Humana, 16(1), 1–19. https://seer.ucp.br/seer/index.php/LexHumana/article/view/ 2837/3686

10. Brown, R., Bruza, P., Heard, W., Mengersen, K., & Murray, J. (November 2016 p.). On the (virtual) getting of wisdom: Immersive 3D interfaces for eliciting spatial information from experts. *Spatial Statistics, 18*(Part A), 318–331. https://doi.org/10.1016/j.spasta.2016.07.001

11. Buhaichuk, K., Warawa, W., Batrachenko, T., Cherniavska, B., & Kondel, V. (2023). Cybercrimes in the global security system in modern conditions. *Lex Humana, 15*(2), 26–44. https://seer.ucp.br/seer/index.php/LexHumana/article/view/ 2474

12. Chien, F., Zhang, Y. & Sadiq, M. (2024). Impact of open innovation on globalization: a survey study on China. *Technological and Economic Development of Economy, 30*(1), 196–217. doi:10.3846/tede.2024.19982

13. Chmyr, Y., Nekryach, A., Kochybei, L., Dakal, A., & Strelbytska, L. (2023). Postindustrial Society and Global Informational Space as Infrastructure Medium and Factor for Actualization of the State Informational Security. *National Security Drivers of Ukraine, Contributions to Political Science*, 61–73. https://doi.org/10.1007/978-3-031-33724-6_4

14. Ciminelli, J.T., Love, T., & Wu, T. (March 2019 p.). Social network spatial model. *Spatial Statistics, 29*, 129–144. https://doi.org/10.1016/j.spasta.2018.11.001

15. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981). *Council of Europe*. https://rm.coe.int/1680078b37

16. Convention on Cybercrime (2001). *Council of Europe*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

17. Convention on the Rights of the Child (1989). *United Nations*. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

18. Corruption Perceptions Index (2023). https://prosperitydata360.worldbank.org/ en/dataset/TI+CPI

19. Country comparison tool, The Culture Factor Group (2023). https://www.theculturefactor.com/country-comparison-tool

20. CrisisWatch (2023). https://www.crisisgroup.org/crisiswatch?utm_campaign=cw_menu_link

21. Delegation for Strategic Affairs. (2013). *Strategic Horizons 2040.* Ministére de la Défense, Paris. https://archives.defense.gouv.fr/content/download/161982/1671192/file/Horizons%20strat%C3%A9giques%20-%20Introduction.pdf

22. Dovhan, O. (2014). National information sovereignty is an object of information security. *Information and law, 3*(12), 102–112. http://dx.doi.org/10.37750/2616-6798.2014.3(12).272574

23. Dubovskyi, O. (2024). Features of world information space in the context of criterion analysis of globalization phenomenon. *Acta De Historia & Politica: Saeculum XXI, 08*, 99–107. https://doi.org/10.26693/ahpsxxi2024.08.099

24. Enebeli, J.P. (2024). Information And Communication Technology (Ict), Globalization And Inpeneding Challenges. *Global Journal of Pure and Applied Sciences, 30*(1), 95–100. doi:10.4314/gjpas.v30i1.9

25. ESPAS European Strategy and Policy Analysis System (2024). Global trends to 2040: Choosing Europe's future. An inter-institutional EU project. https://espas.eu/files/espas_files/about/ESPAS-Global-Trends-to-2040-Choosing-Europes-Future-EN.pdf

26. European Convention on Human Rights. (2010). *Council of Europe*. https://www.echr.coe.int/Documents/Convention_ENG.pdf

27. Fotheringham, A., & Sachdeva, M. (April 2021 p.). Modelling spatial processes in quantitative human geography. *Annals of GIS, 28*(2), 1–10. doi:10.1080/19475683.2021.1903996

28. Fotheringham, A. S., & Sachdeva, M. (August 2022 p.). On the importance of thinking locally for statistics and society. *Spatial Statistics*, *50*. https://doi.org/10.1016/j.spasta.2022.100601

29. Fotheringham, A. S., Li, Z., & Wolf, L. J. (11 January 2021 p.). Scale, Context, and Heterogeneity: A Spatial Analytical Perspective on the 2016 U.S. Presidential Election.

Annals of the American Association of Geographers, 1602–1621. https://doi.org/10.1080/24694452.2020.1835459

30. Fuglstad, G.A., Simpson, D., Lindgren, F.K., & Rue, H. (November 2015 p.). Does non-stationary spatial data always require non-stationary random fields? *Spatial Statistics, 14*(Part C), 505–531. https://doi.org/10.1016/j.spasta.2015.10.001

31. Gelfand, A.E., & Schliep, E.M. (November 2016 p.). Spatial statistics and Gaussian processes: A beautiful marriage. *Spatial Statistics*, *18*(Part A), 86–104. https://doi.org/10.1016/j.spasta.2016.03.006

32. George, R. A. (2024). Global Competency as National Security: Exploring the Global Affairs Education-Security Nexus. *Orbis, 68*(4), 646–665. https://doi.org/10.1016/j.orbis.2024.09.009

33. Ghioni, R., Taddeo, M., & Floridi, L. (2023). Open source intelligence and AI: a systematic review of the GELSI literature. *AI & Society*. https://doi.org/10.1007/s00146-023-01628-x

34. Global Strategic Trends: Out to 2055 (2024*).* UK Ministry of Defence. Отримано з https://www.gov.uk/government/publications/global-strategic-trends-out-to-2055

35. Global Trends 2040: a more contested world (2021). National Intelligence Council. Washington D. C.: Office of the Director of National Intelligence. https://www.dni.gov/index.php/gt2040-home/gt2040-media-and-downloads

36. González, J.A., Rodríguez-Cortés, F.J., Cronie, O., & Mateu, J. (November 2016 p.). Spatio-temporal point process statistics: A review. *Spatial Statistics*, *18*(Part B), 505–544. https://doi.org/10.1016/j.spasta.2016.10.002

37. Guo, B., Ding, Y., Yao, L., Liang, Y., & Yu, Z. (11 July 2020 p.). The Future of False Information Detection on Social Media: New Perspectives and Trends. *ACM Computing Surveys, 53*(4), 1–36. https://doi.org/10.1145/3393880

38. Helwig, N. E., Gao, Y., Wang, S., & Ma, P. (November 2015 p.). Analyzing spatiotemporal trends in social media data via smoothing spline analysis of variance. *Spatial Statistics, 14*(Part C), 491–504. https://doi.org/10.1016/j.spasta.2015.09.002

39. High-Level Expert Group on Artificial Intelligence of the European Commission. Ethics guidelines for trustworthy AI. (2019). https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai

40. Hlobenko, S. (2023). Information space of the state and problems of ensuring its protection in Ukraine. *Scientific Herald: Public Administration, 13*(1), 195–210. https://doi.org/10.33269/2618-0065-2023-1(13)-195-210

41. Hovorushchenko, T., Izonin, I., & Kutucu, H. (2024). Advancements in AI-Based Information Technologies: Solutions for Quality and Security. *Systems, 12*(2). https://doi.org/10.3390/systems12020058

42. Idrisov, H. V. (2022). Information Security in the National Security System in the Modern Age. *Fiat Justisia: Jurnal Ilmu Hukum, 16*(4), 321–330. https://doi.org/10.25041/fiatjustisia.v16no4.2665

43. Ievdokymov, V., Frikel, A., Polishchuk, V., Savchuk, S., & Klimova, I. (2024). Cybercrime and Information Protection in the Field of State Security: Current Threats and Measures for their Prevention. *Economic Affairs, suppl. Special Issue, 69*, 61–69. https://doi.org/10.46852/0424-2513.1.2024.8

44. Ingebrigtsen, R., Lindgren, F., & Steinsland, I. (May 2014 p.). Spatial models with explanatory variables in the dependence structure. *Spatial Statistics*, *8*, 20–38. https://doi.org/10.1016/j.spasta.2013.06.002

45. International Covenant on Civil and Political Rights. (1966). *United Nations*. https://www.ohchr.org/en/instruments-mechanisms/instruments/internationalcovenant-civil-and-political-rights

46. Jagodzinski, K. (29 February 2024 p.). Global Soft Power Index 2024 - A World in Flux. *Brand Finance*. https://brandfinance.com/insights/global-soft-power-index-2024-a-world-in-flux#superpower-text

47. Jordan, J. (2023). Competición entre grandes potencias y militarización del espacio exterior: Great Powers Competition and Outer Space Militarization . *Araucaria*, 25(53). https://doi.org/10.12795/araucaria.2023.i53.07

48. Jordan, J. (2024). How to interpret the Russian sabotage campaign in Europe. Global Strategy Report, 15/2024. https://www.researchgate.net/publication/385778394_How_to_interpret_the_Russian_sabotage_campaign_in_Europe

49. Jordan, J. (2022). La disuasión en la zona gris: una exploración teórica. *Revista Española de Ciencia Política, 59*, 65-88. https://doi.org/10.21308/recp.59.03

50. Jordan, J. (05 December 2017 p.). Political and social trends in the future of global security. A meta-study on official perspectives in Europe and North America. *European Journal of Futures Research*, *5*(11). https://doi.org/10.1007/s40309-017-0120-x

51. Knyazev, S. (2021). Information Security of Ukraine in the Context of National Security. *Information Security of the Person, Society and State, 31*, 81–88. doi:10.51369/2707-7276-2021-(1-3)-9

52. KOF Index of Globalization. (2021, 2023). *Swiss Federal Institute of Technology Zurich.* www.kof.ch/globalization/

53. Kollias, Ch. & Tzeremes, P. (2024). Militarization, globalization and liberal democracy: a nexus? *Review of Economics and Political Science*. https://www.emerald.com/insight/content/doi/10.1108/reps-03-2023-0026/full/html

54. Kotliarov, V. O. (2023). Comprehensive approach to understanding information security in the context of national security. *Public management and administration in Ukraine, 38*, 168–172. http://dx.doi.org/10.32782/pma2663-5240-2023.38.30

55. Kuzmenko, O., Cyburt, A., Yarovenko, H., Yesh, V., & Humenna, Y. (2021). Modeling of «information bubbles» in the global information space. *Journal of International Studies, 14*(4). https://doi.org/10.14254/2071-8330.2021/14-4/18

56. Lahmann, H. (2020). Protecting the global information space in times of armed conflict. *International Review of the Red Cross, 102*(915), 1227–1248. doi:10.1017/S1816383121000400

57. Liang, Y., Poor, H. V., & Shamai, S. (2009). Information theoretic security. *Foundations and Trends in Communications and Information Theory, 5*(4-5), 355–580.

58. Lohse, M. (2020). Sharing national security information in Finland. *Information & Communications Technology Law, 29*(3), 279–290. http://dx.doi.org/10.1080/13600834.2020.1759277

59. Lukyanova, V. & Lautar, A. (2013). Information security in the context of the development of information systems. *Bulletin of the Khmelnytskyi National University. Series «Economic Sciences», 2*(3), 97–101.

60. Lykhova, S., Servatiuk, L., Shamsutdinov, O., Sysoieva, V. & Hurina, D. (без дати). International and national standards on societal information security. *Revista Científica General José María Córdova, 20*(38), 247–264. http://doi.org/10.21830/19006586.898

61. Mateu, J., & Jalilian, A. H. (August 2022 p.). Spatial point processes and neural networks: A convenient couple. *Spatial Statistics, 50*. https://doi.org/10.1016/ j.spasta.2022.100644

62. Murray, A. T., Grubesic, T. H., & Wei, R. (November 2014 p.). Spatially significant cluster detection. *Spatial Statistics*, 103–116. https://doi.org/10.1016/j.spasta.2014.03.001

63. *National Cyber Security Index by e-Governance Academy.* (2023). https://ncsi.ega.ee/data-collection

64. Naumzik, C., & Feuerriegel, S. (2022). Detecting False Rumors from Retweet Dynamics on Social Media. *WWW '22: Proceedings of the ACM Web Conference 2022*, 2798–2809. https://doi.org/10.1145/3485447.3512000

65. Nye, J. (21 February 2017 p.). Soft power: the origins and political progress of a concept. *Humanities and Social Sciences Communications: Palgrave Communications, 3*. doi:10.1057/palcomms.2017.8

66. Oleksenko, R. (2015). The philosophy of sustainable development in the era of globalization. *Hileia, 100*, 175–179. http://nbuv.gov.ua/UJRN/gileya_2015_100_47

67. Orlova, N.S. (2019). Information security in Ukraine's national security system. *States and Regions. Series: Public Administration, 4*, 166–170. http://dx.doi.org/10.32840/ 1813-3401-2019-4-27

68. Phillips, P. J. & Pohl, G. (2023). The Information Game, National Security, and Bitcoin. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.4648742

69. Pipchenko, N. & Darnytskyi, A. (2024). Public diplomacy of Ukraine under martial law. *Actual Problems of Internatonal Relations*, *1*(160), 25–31. https://doi.org/10.17721/apmv.2024.160.1.25-31

70. Pipchenko, N., Makarenko, I., Ryzhkov, M. & Zaitseva, M. (2021). The Policy of European and Euro-Atlantic Integration as a Key Factor for Ukraine's Transformation. *European Spatial Research and Policy*, *28*(1), 265–285. https://doi.org/10.18778/1231-1952.28.1.14.

71. Pynnöniemi, K. & Parppei, K. (29 Jul 2024 p.). Understanding Russia's war against Ukraine: Political, eschatological and cataclysmic dimensions. *Journal of Strategic Studies*. https://doi.org/10.1080/01402390.2024.2379395

72. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. (27 April 2016 p.). *Official Journal of the European Union, 119*, 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

73. Resolution on Information Security. (1 December 2021 p.). *United Nations, Resolution No. A/RES/75/282*. https://www.un.org/en/ga/75/resolutions.shtml

74. Riehle, K.P. (2022). Information Power and Russia's National Security Objectives. *The Journal of Intelligence, Conflict, and Warfare, 4*(3), 62–83. http://dx.doi.org/10.21810/jicw.v4i3.3791

75. Rocha Flores, W., Antonsen, E., & Ekstedt, M. (June 2014 p.). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security, 43*, 90–110. https://doi.org/10.1016/j.cose.2014.03.004

76. Schlette, D., Böhm, F., Caselli, M., & Pernul, G. (2021). Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security, 20*, 21–38. https://doi.org/10.1007/s10207-020-00490-y

77. Shahbazyan, M. (2017). Information Security in the System of Ensuring National Security. *WISDOM, 9*(2), 92–97. http://dx.doi.org/10.24234/wisdom.v9i2.193

78. Skopik, F., Bonitz, A., Grantz, V., & Göhler, G. (2022). From scattered data to actionable knowledge: flexible cyber security reporting in the military domain. *International Journal of Information Security*, *21*, 1323–1347. https://doi.org/10.1007/s10207-022-00613-7

79. Spandonidis, B. (2015). Linking Information Security Awareness to Information Security Management Strategy. A Study in an IT Company. *Linnéuniversitetet, Institutionen för informatik (IK)*.http://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-45894

80. Talabis, M., & Martin, J. (2013). Information Security Risk. Assessments. *Information Security Risk Assessment Toolkit*, 1–26. https://doi.org/10.1016/B978-1-59-749735-0.00001-4

81. Tykhomyrova, Ye. (2004). Public relations in a globalized world. *Our culture and science*.

82. Umarova, N. (2023). Information Security in the Context of Ensuring National Security of Uzbekistan. *International relations and international law, 104*(4). http://dx.doi.org/10.26577/irilj.2023.v104.i4.05

83. Upreti, R., Lind, P.G., Elmokashfi, A., & Yazidi, A. (2024). Trustworthy machine learning in the context of security and privacy. *International Journal of Information Security, 23*, 2287–2314. https://doi.org/10.1007/s10207-024-00813-3

84. Vetrov, K. & Voznyuk, Y. (2019). Information Terrorism as a Modern Threat to Information Security of European States. *International relations, public communications, and regional studies, 1*(5), 34–42.

85. Voronkova, V.G. (2010). The philosophy of globalization: socio-anthropological, socio-economic and socio-cultural dimensions. *RVV ZDIA*.

86. White, G. (2009). Strategic, tactical, and Operational management security model. *Journal of Computer Information Systems, 49*(3), 71–75. https://doi.org/10.1080/08874417.2009.11645326

87. Wikle, C. K., & Zammit-Mangion A. (March 2023 p.). Statistical Deep Learning for Spatial and Spatiotemporal Data. *Annual Review of Statistics and Its Application*, *10*. https://doi.org/10.1146/annurev-statistics-033021-112628

88. Wu, J., Gao, D., Haverly, A., Mittal, S., & Chen, J. (2024). AI Ethics: A Bibliometric Analysis, Critical Issues, and Key Gaps. *International Journal of Business Analytics; Montclair, 11*(1), 1–19. https://doi.org/:10.4018/IJBAN.338367

89. Yeganegi, K., Arbabi, Z. & Hussein, A.I. (2020). The role of information technology in national security. *Journal of Physics: Conference Series, 1530*. doi:10.1088/1742-6596/1530/1/012112

90. Zacharis, A., Katos, V., & Patsakis, C. (2024). Integrating AI-driven threat intelligence and forecasting in the cyber security exercise content generation lifecycle. *International Journal of Information Security*. https://doi.org/ 10.1007/s10207-024-00860-w

91. Zhang, C., Li, S., Zhao, C., & Xia, C. (15 August 2024 p.). Robustness of space information networks based on coverage centrality. *Physics Letters A*, *516*. https://doi.org/10.1016/j.physleta.2024.129636

92. Zhang, Q., Meng, Z., Hong, X., Zhan, Y., Liu, J., Dong, J., Bai, T., Niu, J., & Deen, M.J. (October 2021 p.). A survey on data center cooling systems: Technology, power consumption modeling and control strategy optimization. *Journal of Systems Architecture, 119*. https://doi.org/10.1016/j.sysarc.2021.102253

93. Zharovska, I. (2020). National and information security. *Visnik Nacional'nogo universitetu «Lvivska politehnika». Seria: Uridicni nauki, 7*(27), 56–61. http://dx.doi.org/10.23939/law2020.27.056

94. Авер'янова, Н., & Воропаєва, Т. (2020). Інформаційна безпека України: соціально-філософські аспекти. *Молодий вчений, 10*(86), 297–303. https://doi.org/10.32839/2304-5809/2020-10-86-61

95. Алещенко, В. І. (2022). Інформаційно-психологічна складова безпеки особистості в умовах війни. *Вісник Національного університету оборони України, 66*(2), 5–17. https://doi.org/10.33099/2617-6858-2022-66-2-5-17

96. Андрєєва, О., & Бовкунович, Т. (2021). Трансформація ролі держави в умовах глобалізації. *InterConf*, (51), 269–277. https://ojs.ukrlogos.in.ua/index.php/interconf/ article/ view/11611

97. Арабаджиєв, Д. Ю., & Сергієнко, Т. І. (2020). Політична маніпуляція та інформаційно-психологічна безпека в політичних відносинах. *Політикус: наук. журнал, 2*, 36–44.

98. Архипова, Є. О. (2011). Соціально-філософське осмислення поняття «інформаційна безпека». *Вісник Нац. технічного ун-ту України «Київський політехнічний інститут». Філософія. Психологія. Педагогіка, 3*, 7–11.

99. Безуглий, Д. (2018). Інформаційна безпека України: огляд останніх тенденцій. *Фізико-математична освіта,* (2), 13–17. doi:10.31110/2413-1571-2018-016-2-002

100. Бєлоусова, Н. Б., & Євдомаха, М. С. (2019). «М'яка сила» та екологічна стратегія ЄС. *International relations, part «Political sciences»*, (20). http://journals.iir.edu.ua/index.php/pol_n/article/view/3926

101. Бєльська, Т. В., & Крюков, О. І. (2019). Інформаційні війни та інформаційна безпека: загрози та виклики для демократії. *Вісник Національного університету цивільного захисту України. Серія: Державне управління*, 3–11. http://nbuv.gov.ua/UJRN/VNUCZUDU_2019_2_3

102. Біленчук, П. Д., & Малій, М. І. (2022). Правове забезпечення інформаційної безпеки. *Забезпечення публічної безпеки і порядку в умовах воєнного стану: матеріали Всеукраїнської науково-практичної конференції* (м. Кропивницький, 1 липня 2022 року), 35–38. Кропивницький: Донецький державний університет внутрішніх справ.

103. Біловус, Л. І. (2020). Електронний контент для дітей: теоретико-соціологічний аспект. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Соціальні комунікації», 17*.

104. Білоусов, О. (2016). Міжнародна інформаційна безпека як спільна задача світового співтовариства. *Молодий вчений,* (11), 142–146. http://nbuv.gov.ua/UJRN/molv_2016_11_35

105. Боднар, І. Р. (2014). Державна політика та інформаційна безпека України: післякризові виклики. *Вісник Львівської комерційної академії. Серія економічна,* (46), 28–32. http://nbuv.gov.ua/UJRN/Vlca_ekon_2014_46_7

106. Бойко, Д., Городиський, І. (2023). Регулювання ШІ в Україні: головні тенденції та виклики. *Центр Дністрянкого*. https://dc.org.ua/news/regulyuvannya-shi-v-ukrayini-golovni-tendenciyi-ta-vyklyky

107. Бойченко, О. (2009). Міжнародна інформаційна безпека: проблеми і перспективи. *Форум права,* (3), 74–79. http://nbuv.gov.ua/UJRN/FP_index

108. Бондаренко, Р. (2021). Інформаційна безпека держави. *Інвестиції: практика та досвід,* (5), 95–101. http://nbuv.gov.ua/UJRN/ipd_2021_5_17

109. Борисова, Л. Т. (2013). Інформаційна безпека як визначальний компонент національної безпеки України. *Право і Безпека,* (1), 39–42. http://nbuv.gov.ua/UJRN/Pib_2013_1_9

110. Борисова,, Л. В., Біленчук, П. Д., Собина, В. О., & Неклонський, І. М. (2018). *Правові засади інформаційної безпеки України*.

111. Валюшко, І. О. (2018). Інформаційна безпека України в контексті російськоукраїнського конфлікту. *Дисертація*.

112. Вєдєнєєв, Д. В., & Копієвська, О. Р. (2021). Гібридні загрози як об’єкт освітніх практик у культурно-мистецькій сфері україни. *Вісник Національної академії керівних кадрів культури і мистецтв, 2*, 3–11.

113. Виговська, О., & Бєлоусова, Н. (2017). Інформаційна складова національної безпеки України.

114. Вінник, О. М. (2022). Правові проблеми індивідуальних кіберзахисту та кібербезпеки. *Забезпечення публічної безпеки і порядку в умовах воєнного стану: матеріали Всеукраїнської науково-практичної конференції* (м. Кропивницький, 1 липня 2022 року), 65–68. Кропивницький: Донецький державний університет внутрішніх справ.

115. Гбур, З. В. (27 01 2022 р.). Використання штучного інтелекту в інформаційній безпеці України. *Державне управління: удосконалення та розвиток*. doi:10.32702/2307-2156-2022.1.2

116. Геворкян, А. (2021) Інтегральне оцінювання рівня розвитку інформаційно-комунікаційних технологій регіонів в контексті зміцнення інформаційної безпеки

України. *Державне управління: удосконалення та розвиток*, 11. doi: 10.32702/2307-2156-2021.11.36

117. Гребініченко, О.Ю. (2008). Міжнародні рейтинги України як фактор впливу на національну безпеку держави. *Дисертація*. Отримано з https://mydisser.com/dfiles/88268785.doc

118. Гур'єв, В. І., Мехед, Д. Б., Ткач, Ю. М. & Фірсова, І. В. (2018). *Інформаційна безпека держави: «Управління інформаційною безпекою», «Кібербезпека»*.

119. Гусарєв, С. Д. (2004). Діяльний підхід у дослідженнях юридичної діяльності. *Науковий вісник НАВСУ, 4*, 30–39.

120. Гусерль, Е. (2020). Ідеї чистої феноменології і феноменологічної філософії: Книга перша. Загальний вступ до чистої феноменології. *Харків: Фоліо*.

121. Двостороння безпекова угода між Україною та Сполученими Штатами Америки, № 840_001-24 від 13.06.2024. https://zakon.rada.gov.ua/laws/show/840_001-24#Text

122. Дзьобань, О. &. (2015). Інформаційна безпека: нові виміри загроз, пов'язаних із інформаційно-комунікаційною діяльністю. *Гуманітарний вісник Запорізької державної інженерної академії,* (61), 24–34. http://nbuv.gov.ua/UJRN/znpgvzdia_2015_61_4

123. Дзьобань, О. (2006). Інформаційна безпека в умовах глобалізаційних тенденцій: до проблеми осмислення сутності. *Гуманітарний вісник Запорізької державної інженерної академії* (24), 101–108. doi:http://nbuv.gov.ua/UJRN/znpgvzdia_2006_24_12

124. Дмитрук, С. (2019). Трансформація поглядів на безпекове середовище в умовах глобалізації. *Вісник Національної академії Державної прикордонної служби України,* (2). doi:10.32453/governance.vi2.115

125. Довгань, О. Д., & Ткачук, Т. Ю. (2018). Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. *Інформація і право, 2*(25), 73–85.

126. Довгань, О. Д. (2015). Інформаційна безпека – гарант безпеки національних інформаційних ресурсів. *Evropský politický a právní diskurz, 2*(2), 130–134. http://nbuv.gov.ua/UJRN/evrpol_2015_2_2_21

127. Дубняк, К. (2015). Інформаційний простір: структура та функціональні параметри. *Держава та регіони. Серія: Соціальні комунікації, 4*, 21–25.

128. Дубов, Д. (2010). Сучасні тренди кібербезпекової політики: висновки для України. Аналітична записка. http://www.niss.gov.ua/articles/294

129. Дубовський, О. Г. (2024a) Особливості світового інформаційного простору в контексті критеріального аналізу феномена глобалізації. *Acta de historia & politica: saeculum XXI, 8*, 99–107

130. Дубовський, О. Г. (2024b) Управління світовим інформаційним простором: можливості та обмеження. *Міжнародні відносини, суспільні комунікації та регіональні студії*, *1*(18), 16–27

131. Дубовський, О. Г. (2024c) Інформаційна безпека: суб'єктність та штучний інтелект. *Journal of Innovations and Sustainability*, *8*(2). https://doi.org/10.51599/is.2024.08.02.09

132. Євдоченко, Л. О. (2011). Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації. *Автореферат дисертації*.

133. Забара, І. (2013). Міжнародна інформаційна безпека: сучасні концепції в міжнародному праві. *Теорія і практика правознавства,* (2). http://nbuv.gov.ua/UJRN/tipp_2013_2_77

134. Закон України «Про інформацію». (1992). *Верховна Рада України*. https://zakon.rada.gov.ua/laws/show/2657-12#Text

135. Закон України «Про національку безпеку України». (2024). *Верховна Рада України*. https://zakon.rada.gov.ua/laws/show/2469-19#Text

136. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» № 3475-IV від 23.02.2006 (редакція від 28.06.2024) URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

137. Закон України «Про державну таємницю» № 3855-XII від 21.01.1994 (редакція від 30.10.2024) https://zakon.rada.gov.ua/laws/show/3855-12#Text

138. Закон України «Про доступ до публічної інформації» № 2939-VI від 13.01.2011 (редакція від 08.10.2023) https://zakon.rada.gov.ua/laws/show/2939-17#Text
139. Закон України «Про електронні комунікації» № 1089-IX від 16.12.2020 (редакція від 05.01.2025) https://zakon.rada.gov.ua/laws/show/1089-20#Text
140. Закон України «Про заборону пропаганди російського нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну» № 2265-IX від 22.05.2022 (редакція від 23.09.2024). https://zakon.rada.gov.ua/laws/show/2265-20#Text
141. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 05.07.1994 (редакція від 28.06.2024). https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#n67
142. Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010 (редакція від 18.01.2025). https://zakon.rada.gov.ua/laws/show/2297-17#Text
143. Закон України «Про захист суспільної моралі» № 1296-IV від 20.11.2003 (редакція від 31.03.2023). https://zakon.rada.gov.ua/laws/show/1296-15#Text
144. Закон України «Про Збройні Сили України» № 1934-XII від 06.12.1991 (редакція від 05.01.2025). https://zakon.rada.gov.ua/laws/show/1934-12#Text
145. Закон України «Про інформацію» № 2657-XII від 02.10.1992 (редакція від 15.11.2024). https://zakon.rada.gov.ua/laws/show/2657-12#Text
146. Закон України «Про Концепцію Національної програми інформатизації» № 75/98-ВР від 04.02.1998 (редакція від 01.01.2022). https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text
147. Закон України «Про медіа» № 2849-IX від 13.12.2022 (редакція від 01.01.2025). https://zakon.rada.gov.ua/laws/show/2849-20#Text
148. Закон України «Про національну безпеку України» № 2469-VIII від 21.06.2018 (редакція від 09.08.2024). https://zakon.rada.gov.ua/laws/show/2469-19#Text
149. Закон України «Про Національну поліцію» № 580-VIII від 02.07.2015 (редакція від 16.08.2024). https://zakon.rada.gov.ua/laws/show/580-19#Text

150. Закон України «Про Національну програму інформатизації» № 2807-IX від 01.12.2022. https://zakon.rada.gov.ua/laws/show/2807-20#Text

151. Закон України «Про оборону України» № 1932-XII від 06.12.1991 (редакція від 05.01.2025). https://zakon.rada.gov.ua/laws/show/1932-12#Text

152. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 (редакція від 28.06.2024). https://zakon.rada.gov.ua/laws/show/2163-19#Text

153. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» № 537-V від 09.01.2007. https://zakon.rada.gov.ua/laws/show/537-16#Text

154. Закон України «Про правовий режим воєнного стану» № 389-VIII від 12.05.2015 (редакція від 08.02.2025). https://zakon.rada.gov.ua/laws/show/389-19#Text

155. Закон України «Про Раду національної безпеки і оборони України» № 183/98-ВР від 05.03.1998 (редакція від 29.07.2023). https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text

156. Закон України «Про Службу безпеки України» № 2229-XII від 25.03.1992 (редакція від 09.01.2025). https://zakon.rada.gov.ua/laws/show/2229-12#Text

157. Закон України «Про Службу зовнішньої розвідки України» № 3160-IV від 01.12.2005 (редакція від 23.04.2021) URL: https://zakon.rada.gov.ua/laws/show/3160-15#Text

158. Закон України «Про центральні органи виконавчої влади» № 3166-VI від 17.03.2011 (редакція від 15.11.2024). https://zakon.rada.gov.ua/laws/show/3166-VI#Text

159. Закон України 2807-IX «Про Національну програму інформатизації». (2022). https://zakon.rada.gov.ua/laws/show/2807-20#Text

160. Запорожець, О., & Бєлоусова, Н. (2022). Вербальні інтернет-меми під час повномасштабної війни РФ проти України. *Journal of International Relations of KNU*, 56 (2).

161. Зозуля, О. С. (2017). Державне управління забезпеченням інформаційної безпеки України в умовах інформаційнопсихологічного протиборства. *Дисертація*.

162. Ільницька, У. (2016). Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Humanitarian vision, 1*(2), 27–32. http://nbuv.gov.ua/UJRN/ hv_2016_2_1_7

163. Капля, О. М. (2023). Правове регулювання інформаційної безпеки громадянина під час дії воєнного стану. *Експерт: парадигми юридичних наук і державного управління, 6*(24), 16–20. https://doi.org/10.32689/2617-9660-2022-6(24)-16-20

164. Квіткін, П., Дятлова, І., & Петрова, Л. (2021). Інформаційна безпека особистості: теоретико-методологічний аналіз. *Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія, 4*(51). https://doi.org/10.21564/2663-5704.51.241998

165. Килимник, І. (2023). Інформаційне суспільство та інформаційна безпека. Нові виклики та шляхи подолання інформаційних загроз. *Науковий вісник Ужгородського національного університету. Серія: Право*, *76*(2), 53–57. https://doi.org/10.24144/2307-3322.2022.76.2.8

166. Ковальов, К. (2023). Інформаційна безпека: міжнародно-правовий аспект. *Інформація і право, 4*(47), 159–167. https://doi.org/10.37750/2616-6798.2023.4(47).291624

167. Колектив авторів. (2024). Трансформація інформаційної війни в епоху штучного інтелекту. (Б. Попков, & С. Пєтков, Ред.) *Інформаційний спротив українського громадянського суспільства в умовах гібридної війни: генеза національної стійкості крізь призму наукових досліджень: монографія*, 14–26.

168. Коляда, І.Г. (2021). Інформаційно-освітній простір сучасного суспільства: соціально-філософський аналіз.

169. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

170. Кормич, Б.А. (2004). Організаційно-правові основи політики інформаційної безпеки України. *Харків: НУВС, 427*.

171. Кохановська, О. (2013). Основні теорії у сфері інформаційних правовідносин: концепція інформаційних прав як приватноправового інституту і теорія інформаційного права як галузі права у сучасній правовій доктрині України. *Приватне право, 1*, 186–200.

172. Кочубей, Л. (2015). Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі. *Наукові записки Інституту політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України,* (3), 220–237. http://nbuv.gov.ua/UJRN/Nzipiend_2015_3_10

173. Крулевський, А. В. (2024). Тенденції та перспективи цифровізації публічного управління в Україні. *Науковий вісник Одеського національного економічного університету: менеджмент та бізнес-адміністрування*, 99–106. doi:10.32680/2409-9260-2024-5-6-318-319-99-106

174. Кустовська, О.В. (2005). Методологія системного підходу та наукових досліджень: Курс лекцій. *Тернопіль: Економічна думка*.

175. Литовченко, І. В. (2012). Структурно-функціоналістська парадигма в дослідженнях соціальних інститутів. *Вісник Національного авіаційного університету. Філософія. Культурологія, 2*, 48–51.

176. Ліпкан, В. А., Максименко, Ю. Є., & Желіховський, В. М. (2006). Желіховський Інформаційна безпека України в умовах євроінтеграції. Київ: КНТ.

177. Макаренко, Є. А. (2003). *Міжнародна інформаційна політика: структура, тенденції, перспективи* [Дис. д-ра. політич. наук, Київський національний університет імені Тараса Шевченка]

178. Максимов, С. І. (2009). Феноменологічний підхід до розуміння правової реальності. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія: Філософія, філософія права, політологія, соціологія*, 51–57.

179. Мельник, Д. О. (2021). Актуальні загрози національній безпеці України в інформаційній сфері: питання визначення та протидії. *Інформаційна безпека людини, суспільства, держави,* 1–3 (31–33), 16–27.

180. Методологія визначення індексу сприйняття корупції (2022). *Transparency International*. https://images.transparencycdn.org/images/CPI_2022_Methodology.zip

181. Мітенко, О. (2019). Інформаційна безпека як складова національної безпеки України. *Інформаційна безпека людини, суспільства, держави,* (1), 27–36. http://nbuv.gov.ua/UJRN/iblsd_2019_1_6

182. Морозов, О. М., & Морозова, Т. Р. (2019). Остратегії наступу та захисту в інформаційно-психологічній боротьбі. *Актуальні проблеми управління інформаційною безпекою держави*, 96–98

183. Найман-меткалф, К. (2015) Правовий аналіз ОБСЄ проекту концепції інформаційної безпеки. *Інформація і право,* 2 (14). https://doi.org/10.37750/2616-6798.2015.2(14).272716

184. Нашинець-Наумова, А. Ю. (2017). Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика».

185. Нестеряк, Ю., & Лашкіна, М. (2020). Інформаційна політика та інформаційна безпека держави як психосоціальне явище: проблеми та перспективи. *Public management*.

186. Нестеряк, Ю. В. (2014). Державна інформаційна політика: теоретикометодологічні засади: монографія.

187. Новицька, Н. Б., Петрик, В. М., & Кудико, В. М. (2023). Дезінформування як засіб ведення інформаційної війни російської федерації проти україни. *Ірпінський юридичний часопис, 1*(8), 118-130. https://doi.org/10.33244/2617-4154-1(8)-2022-118-130

188. Панченко, В.М. (2013). Співвідношення понять: інформаційна та кібернетична безпека. *Інформаційна безпека людини, суспільства, держави*(2), сс. 20-23. Отримано з http://nbuv.gov.ua/UJRN/iblsd_2013_2_5

189. Панченко, О. А. (2020). Державне управління інформаційною безпекою в турбулентному суспільстві. *World Science, 3*(5(57)), 4–9. https://doi.org/10.31435/ rsglobal_ws/31052020/7082

190. Пархоменко-Куцевіл, О. (2023). Проблеми забезпечення національної безпеки в умовах воєнного часу. *Науковий вісник Вінницької академії безперервної освіти. Серія «Екологія. Публічне управління та адміністрування», 3*. https://doi.org/10.32782/2786-5681-2023-3.19

191. Петрик, В.М., Бедь, В.В., Присяжнюк, М.М. & ін. (2018). *Інформаційно-психологічне протиборство : підручник. Видання друге перекладене, доповнене та перероблене.* Київ: ПАТ «ВІПОЛ».

192. Піпченко, Н. О. (2019). Цифрові виклики для політико-економічної системи ЄС. Науково-практична конференція «Діджиталізація сучасної системи міжнародних економічних відносин», 2 (20).

193. Писарчук, О. О., & Кошара, А. В. (2024). Аналіз індикаторів загроз інформаційній безпеці в інформаційно-телекомунікаційних системах за результатами застосування siem-систем. *Інфокомунікаційні та комп'ютерні технології*, *1*(07), 79 https://doi.org/10.31435/ rsglobal_ws/31052020/708284. https://doi.org/10.36994/2788-5518-2024-01-07-11

194. Постанова Кабінету Міністрів України № 75-2025-п від 24.01.2025 «Деякі питання оперативно-технічного управління електронними комунікаційними мережами в умовах надзвичайної ситуації, надзвичайного або воєнного стану». https://zakon.rada.gov.ua/laws/show/75-2025-%D0%BF#Text

195. Проєкт Концепції інформаційної безпеки України. (2015). https://www.osce.org/files/f/documents/0/2/175056.pdf

196. Радченко, О. В. & Чмир, Я. І. (2022). Гібридна війна як ключова загроза національному суверенітету України. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування,* (3), 100–108. http://dx.doi.org/10.32851/tnv-pub.2021.3.14

197. Резнікова, О. О. (2022). *Національна стійкість в умовах мінливого безпекового середовища. Монографія.* Київ: НІСД.

https://niss.gov.ua/publikatsiyi/monohrafiyi/natsionalna-stiykist-v-umovakh-minlyvoho-bezpekovoho-seredovyshcha

198. Розпорядження Кабінету Міністрів України № 1351-2024-р від 31.12.2024 «Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025-2027 роках». https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text

199. Розпорядження Кабінету Міністрів України № 1163-2023-р від 19.12.2023 «Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України». https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text

200. Розпорядження Кабінету Міністрів України № 366 від 14.04.2021 «Про схвалення Національної стратегії із створення безбар'єрного простору в Україні на період до 2030 року». https://zakon.rada.gov.ua/laws/show/366-2021-%D1%80#Text

201. Розпорядження Кабінету Міністрів України № 687-2019-р від 24.07.2019 «Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року» (редакція від 21.07.2023). https://zakon.rada.gov.ua/laws/show/687-2019-%D1%80#Text

202. Розпорядження Кабінету Міністрів України від 30 березня 2023 року № 272-р «Про затвердження плану заходів з реалізації Стратегії інфомаційної безпеки на період до 2025 року» (2023). *Офіційний вістник України*. https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#Text

203. Сагайдак, О. В. (2010). Інформаційна безпека України в умовах глобалізаційних викликів. *Вісник Луганського національного університету імені Тараса Шевченка. Соціологічні науки, 2*(12), 115–125. doi:http://nbuv.gov.ua/UJRN/vluc_2010_12_2(2)__17

204. Селезньова, О. М. (2016). Теоретико-методологічне трактування окремих засадничих категорій інформаційного права. *ІТ право: проблеми і перспективи розвитку в Україні*, 136–143.

205. Ситник, Г. П., Олуйко, В. М., & Вавринчук, М. П. (2007). *Національна безпека України: теорія і практика.*

206. Ситник, Г.П. (2012). *Державне управління у сфері національної безпеки. Концептуальні та організаційно-правові засади: підручник/ГП Ситник.*

207. Слюсарчук, І. (2015). Антиукраїнська інформаційна війна Російської Федерації. *Інформаційна безпека людини, суспільства, держави*, 18–26. Отримано з http://nbuv.gov.ua/UJRN/iblsd_2015_3_4

208. Солдатенко, О. (2018). Інформаційний простір у мережі Інтернет: правове регулювання та контроль. *Підприємництво, господарство і право, 138*.

209. Солодка, О.М. (2020). Інформаційний простір держави як сфера реалізації інформаційного суверенітету. *Інформація і право, 4*(35), 39–46.

210. Сопілко, І. (2021). Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник. Повітряне і космічне право,* (2), 110–115. Отримано з http://nbuv.gov.ua/UJRN/Npnau_2021_2_16

211. Соснін, О. Г. & Грушова, Г. В (2014). Міжнародна інформаційна безпека як актуальна проблема сучасності. *Держава і право. Юридичні і політичні науки,* (66), 290–297. http://nbuv.gov.ua/UJRN/dip_2014_66_36

212. Степанов, В. (2016). Інформаційна безпека як складова державної інформаційної політики. *Державне будівництво,* (2). http://nbuv.gov.ua/UJRN/DeBu_2016_2_4

213. Тихомиров, Д.О. (2020). Наукові методологічні підходи під час дослідження державної політики у сфері безпеки. *Підприємництво, господарство і право, 3*, 230–234.

214. Тихомиров, О. (2014a). Інформаційна безпека: соціотехнічна парадигма. *Інформаційна безпека людини, суспільства, держави,* (1), 13–20. http://nbuv.gov.ua/UJRN/iblsd_2014_1_4

215. Тихомиров, О. О. (2014b). Забезпечення інформаційної безпеки як функція сучасної держави: монографія. *ЦНННПВ НАСБУ*.

216. Ткаченко, В. В. & Паливода, В. В. (2022). Загрози інформаційній безпеці України як проблематика національної безпеки. *Juridical scientific and electronic journal,* (10), 496–498. https://doi.org/10.32782/2524-0374/2022-10/123

217. Ткачук, Т. Ю. (2019). Забезпечення інформаційної безпеки в умовах євроінтеграції України. *Дисертація*.

218. Указ Президента України № 121/2021 «Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України"» (2021). https://zakon.rada.gov.ua/laws/show/121/2021#Text

219. Указ Президента України № 187/2021 від 07.05.2021 «Питання Центру протидії дезінформації». https://zakon.rada.gov.ua/laws/show/187/2021#Text

220. Указ Президента України № 392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України"», редакція від 07.01.2025. https://zakon.rada.gov.ua/ laws/show/392/2020#n12

221. Указ Президента України № 47/2017 від 25 лютого 2017 року «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України"» (редакція від 30.12.2021). https://www.president.gov.ua/documents/472017-21374

222. Указ Президента України №447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» (2021). https://zakon.rada.gov.ua/laws/show/n0055525-21#Text

223. Указ Президента України №447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"», (2021). https://zakon.rada.gov.ua/laws/show/447/2021#n101

224. Указ Президента України №685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"». (2021). *Офіційний вістник України*. https://zakon.rada.gov.ua/laws/show/685/2021#n14

225. Федченко, О. (June 2022 р.). Аналіз факторів та сучасних загроз інформаційній безпеці держави у контексті забезпечення національної безпеки України. *Journal of Scientific Papers Social development & Security, 12*(3), 128–134. doi:10.33445/sds.2022.12.3.11

226. Фурашев, В. (2013) Інформаційна безпека: індикатори. *Інформація і право*, *1*(7) https://doi.org/10.37750/2616-6798.2013.1(7).272262

227. Цимбалюк, В. С. (2010). Інформаційне право – право інформаційного суспільства.

228. Чмир, Я. (2020). Інформаційне суспільство та глобальний інформаційний простір: безпекові аспекти. *Сучасні аспекти модернізації науки в Україні: стан, проблеми, тенденції розвитку*, 95–97.

229. Чмир, Я. (2022). Сучасні проблеми інфомраційної безпеки України та перспективи їх вирішення. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління, 62*, 149–154. http://dx.doi.org/10.32689/2523-4625-2022-2(62)-23

230. Шатун, В. &. (2016). Інформаційна безпека – невід'ємна складова національної безпеки України. *Наукові праці Чорноморського державного університету імені Петра Могили комплексу "Києво-Могилянська академія". Серія: Державне управління., 267*(255), 174–180. http://nbuv.gov.ua/UJRN/ Npchdu_2016_267_255_29

231. Шемчук, В. В. (2019). Інформаційна безпека та інформаційна оборона в контексті розвитку вітчизняної доктрини й законодавчої справи. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Юридичні науки., 30(69)*(4), 31–37. https://doi.org/10.32838/1606-3716/2019.4/06

232. Шемчук, В. В. (2019). Механізм забезпечення інформаційної безпеки держави: теоретично-методологічні основи. *Філософські та методологічні проблеми права, 1*(17). https://doi.org/10.33270/01191702.51

233. Юдкова, К. В. (2014). Правова інформатика: міжнародний досвід як підґрунтя інтеграційних процесів. *Правова інформатика, 4*(44), 34–39.

234. Юськів, Б. (2009). Глобалізація і трудова міграція в Європі.

235. Яруліна, Н. (2019). Теоретичні підходи до визначення понять «інформаційний простір», «інформаційне середовище», «інформаційно-комунікативне середовище». *Актуальні проблеми державного управління, 2*, 26–31

ДОДАТОК А

Список опублікованих праць за темою дисертації

Статті у наукових фахових виданнях України

4. Дубовський, О. Г. (2024). Особливості світового інформаційного простору в контексті критеріального аналізу феномена глобалізації. *Acta de historia & politica: saeculum XXI, VIII*, 99–107.

5. Дубовський, О. Г. (2024). Управління світовим інформаційним простором: можливості та обмеження. *Міжнародні відносини, суспільні комунікації та регіональні студії*, 1(18), 16–27.

6. Дубовський, О. Г. (2024). Інформаційна безпека: суб'єктність та штучний інтелект. *Journal of Innovations and Sustainability*, 8(2). https://doi.org/10.51599/is.2024.08.02.09

Праці, які засвідчують апробацію матеріалів дисертації

3. Дубовський, О. Г., & Степанишин Р. Д. (2023). Розвиток технологій штучного інтелекту та його вплив на міжнародну інформаційну безпеку. *Матеріали Всеукраїнської науково-практичної конференції молодих вчених, ад'юнктів, слухачів, курсантів і студентів «Молодіжна військова наука у Київському національному університеті імені Тараса Шевченка»*. ВІКНУ, с. 436–437 (Особистий внесок автора: 0,12 авт. аркш.).

4. Дубовський, О. Г. (2021). Психологічна війна: юридичні та етичні аспекти. *Матеріали XVII міжнародної науково-практичної конференції «Військова освіта і наука: сьогодення та майбутнє».* ВІКНУ, Т. 2, с. 18–19.

ДОДАТОК Б

Апробація результатів дослідження

1.Першій науково-практичній міжнародній конференції з питань кібердипломатії (м. Київ, 15-16 травня 2024 року; участь в обговоренні);

2.Всеукраїнській науково-практичній конференції молодих вчених, ад'юнктів, слухачів, курсантів і студентів «Молодіжна військова наука у Київському національному університеті імені Тараса Шевченка» (м. Київ, 27 квітня 2023 року; виступ і публікація тез);

3.XVII міжнародній науково-практичній конференції «Військова освіта і наука: сьогодення та майбутнє» (м. Київ, 26 листопада 2021 року; виступ і публікація тез).