Journal of Innovations and Sustainability
ISSN 2367-8151
2024, Vol. 8, No. 2
https://is-journal.com

ІНФОРМАЦІЙНА БЕЗПЕКА: СУБ'ЄКТНІСТЬ І ШТУЧНИЙ ІНТЕЛЕКТ

Олександр Дубовський
Військовий інститут Київського національного університету імені Тараса Шевченка, Україна
ORCID: https://orcid.org/0009-0001-5587-7980

Дубовський, О. (2024). Інформаційна безпека: суб'єктність і штучний інтелект. *Journal of Innovations and Sustainability*, 8(2), 09. https://doi.org/10.51599/is.2024.08.02.09.

Мета. Метою дослідження є визначення особливостей використання штучного інтелекту для посилення конгруентності систем інформаційної безпеки тенденціям світового інформаційного простору.
Результати. Визначено особливості світового інформаційного простору, які є джерелом актуалізації чинників масштабування загроз інформаційній безпеці та проблемності реалізації принципів розбудови системи інформаційної безпеки, відповідності критеріям ефективного управління. Використання штучного інтелекту трансформує суб'єктність у цифрову площину, що знаменує фундаментальний перехід від простого агрегування даних до інтелектуального аналізу, що дає змогу не тільки виявляти загрози, а й здійснювати проактивний пошук. Використання надійного та етичного штучного інтелекту посилює інформаційну безпеку, збільшує довіру суспільства та зменшує невизначеність. 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 компонента, розробка «спільних когнітивних систем» є оптимальним балансом між аналітиками та алгоритмами.
Наукова новизна. Уперше проаналізовано концептуальні основи розбудови системи інформаційної безпеки та чинники масштабування загроз через призму особливостей світового інформаційного простору; поглиблено функціональні можливості штучного інтелекту в ролі асоційованого суб'єкта інформаційної безпеки, інтеграційної складової ефективності систем інформаційної безпеки в глобалізованому інформаційному просторі; розширено концептуальне бачення моделі інформаційної безпеки та обґрунтовано доцільність розробки концепції інтегральної проєктивної системи інформаційної безпеки на основі принципу дуальності.
Практична цінність. Проведений аналіз можливостей штучного інтелекту для забезпечення інформаційної безпеки є основою для розробки концепції інтегральної проєктивної системи інформаційної безпеки на основі принципу дуальності, який полягає у відповідності ключових вузлів в архітектоніці світового інформаційного простору точкам у спроєктованому інформаційному просторі системи безпеки. Кожній такій точці відповідає певний аналітичний механізм. Інтегральність системи забезпечується зв'язками між цими механізмами. Таким чином, ми відходимо від фрагментарного реагування на загрози до пластичної системи безпеки на основі використання штучного інтелекту.
Ключові слова: глобалізація, світовий інформаційний простір, інформаційна безпека, штучний інтелект.

Journal of Innovations and Sustainability
ISSN 2367-8151
2024, Vol. 8, No. 2
https://is-journal.com

INFORMATION SECURITY: SUBJECTIVITY AND ARTIFICIAL INTELLIGENCE

Oleksandr Dubovskyi
Military Institute of Taras Shevchenko National University of Kyiv, Ukraine
ORCID: https://orcid.org/0009-0001-5587-7980

Purpose. The purpose of the study is to determine the features of the use of artificial intelligence in order to strengthen the congruence of information security systems with the trends of the world information space.
Results. The peculiarities of the global information space are identified, which are the source of actualisation of the factors of scaling threats to information security and the difficulty of implementing the principles of building the information security system, compliance with the criteria of effective management. The use of artificial intelligence transforms subjectivity into a digital plane, which marks a fundamental transition from simple data aggregation to intelligent analysis, which allows not only detecting threats, but also conducting proactive searches. The use of reliable and ethical artificial intelligence strengthens information security, increases public trust and reduces uncertainty. As a technology of action and countermeasures, artificial intelligence allows increasing objectivity, speed of formation and completeness of situational awareness. The effectiveness of the use of artificial intelligence models depends on the preservation of the human component, the development of "joint cognitive systems" is the optimal balance between analysts and algorithms.
Scientific novelty. For the first time, the conceptual foundations of the development of the information security system and the factors of scaling the threat due to the primacy of the features of the global information space were analysed; the functional capabilities of artificial intelligence as an associated subject of information security, an integrative component of the effectiveness of the information security system in the globalised information space are deepened; the conceptual vision of the information security model is expanded and the feasibility of developing the concept of an integrated projective information security system based on the principle of duality is substantiated.
Practical value. The conducted analysis of the capabilities of artificial intelligence to ensure information security is the basis for developing the concept of an integrated projective system of information security based on the principle of duality, which consists in matching key nodes in the architecture of the world information space with points in the designed information space of the security system. Each such point corresponds to a certain analytical mechanism. The integrity of the system is ensured by connections between these mechanisms. Thus, we are moving away from a fragmented response to threats to a plastic security system based on the use of artificial intelligence.
Key words: globalization, global information space, information security, artificial intelligence.

Постановка проблеми. Глобалізаційні процеси з кожним роком посилюються, про що свідчать дані KOF Швейцарського економічного інституту, який розробив систему якісного та кількісного вимірювання глобалізації [1]. Глобалізація стирає географічні кордони, охоплює все більше сфер суспільного буття та поглиблює розростання мережі інтеграційних зв'язків. Будучи першопочатково відповіддю на появу глобальних проблем, вона перетворилася на сучасну світову тенденцію всеохоплюючого масштабу, що зумовило необхідність зміни засобів і підходів до вирішення вже й локальних проблем. Наслідком глобалізації є формування світового інформаційного

простору, який значно посилив вагомість інформації як політичної та економічної одиниці впливу, що актуалізувало четвертий вимір суспільного розвитку, підтверджуючи його рівність із загальновідомими, такими як дипломатичний, економічний та військовий рівні [2]. 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. 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.

Аналіз останніх досліджень і публікацій. Із цієї проблематики можна відзначити дослідження етичних проблем використання штучного інтелекту – J. Wu [3], факторів формування державної системи інформаційної безпеки – С. Глобенко [4], моделей кібербезпеки – K. Buhaichuk [5], глобального інформаційного простору як інфраструктурного середовища та чинника актуалізації інформаційної безпеки держави – Y. Chmyr [6], штучного інтелекту як інструмента державного управляння інформаційною безпекою – В. Бондар [7], критеріїв достатності інформаційної безпеки – O. Bortnikova [2], загроз в інформаційному просторі для національної безпеки та стратегій протидії – V. Ievdokymov [8], штучного інтелекту як інструмента інформаційної безпеки – T. Hovorushchenko [9], R. Upreti [10], A. Zacharis [11], особливостей світовового інформаційного простору – O. Dubovskyi [12], феномена глобалізації та її концептуальних засад – B. Yuskiv [13], правових проблем захисту інформаційного простору в умовах збройних конфліктів – H. Lahmann [14], технологічного забезпечення виявлення інформаційних загроз – D. Schlette та ін. [15], проблем формування ситуаційної обізнаності у військовій сфері – F. Skopik та ін. [16].

На основі аналізу цих наукових робіт можна зробити висновок, що забезпечення інформаційної безпеки є проблемною областю з високим ступенем невизначеності: висока варіативність і різнорідність впливаючих факторів [4], масштабування загроз та різнорівневість їхніх наслідків від національної безпеки до поширення тривожних і депресивних станів у суспільстві [5], зростаюча технологічна складність загроз [8], швидкість появи нових технологій і проблема розробки систем виявлення загроз [15], інституційна суперечливість [6], зростаюча кількість інформації та її джерел [16], проблеми правового регулювання [14]. 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 і мати правове підґрунтя [3], бути безпечними, якісними [8], захищеними технологічно та соціально [7]. У 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, чому й присвячена ця робота.

Мета, матеріали та методи дослідження. Метою дослідження є визначення особливостей використання штучного інтелекту для посилення конгруентності систем інформаційної безпеки тенденціям світового інформаційного простору. Для реалізації цієї мети передбачено вирішення таких завдань: визначити особливості світового інформаційного простору, окреслити концептуальні засновки розбудови системи інформаційної безпеки, розглянути чинники масштабування загроз інформаційній безпеці, проаналізувати можливості використання моделей штучного інтелекту для забезпечення інформаційної безпеки.

Методологічну основу дослідження складає феноменологічний підхід, оскільки світовий інформаційний простір є індикатором глобалізації, а його особливості, виділені на основі критеріального аналізу, відображають її просторово-часові та наслідкові прояви, їхню масштабність та характер змін. Застосовано такі загальнонаукові методи: порівняння та узагальнення – для визначення на основі огляду вітчизняних і зарубіжних наукових публікацій проблемних аспектів забезпечення інформаційної безпеки, контекстуальних особливостей і технологічного забезпечення; синтез – для інтеграції концептуальних основ розбудови системи інформаційної безпеки, особливостей світового інформаційного простору, чинників і наслідків масштабування загроз; аналіз – для визначення можливостей застосування штучного інтелекту в системах інформаційної безпеки.

Програмне забезпечення дослідження складає IBM SPSS Statistics 23.0, проведено кореляційний аналіз з метою виявлення зв’язків між інтенсивністю глобалізації економічної, політичної, соціальної сфер і розвитком кібербезпеки.

Використано результати регресійного аналізу K. Buhaichuk [5]. Визначені таким чином чинники та наслідки масштабування інформаційних загроз проаналізовано через призму особливостей світового інформаційного простору в контексті відповідності критеріям достатності державного регулювання заходів інформаційної безпеки.

Інформаційну базу дослідження становлять публікації вітчизняних і зарубіжних науковців, а також бази даних KOF [1] та NCSI [17].

Виклад основного матеріалу дослідження. Глобалізація як тренд світового устрою охоплює все більше сфер суспільного буття. Одним з

індикаторів глобалізації є формування світового інформаційного простору. На основі критеріального аналізу феномена глобалізації можна виділити такі особливості світового інформаційного простору: «…всеохоплюючий та сегментарний характер, системоутворювальний вплив на різні сфери суспільного буття та змістовна відповідність сфері функціонування інформаційної інфраструктури, багатосуб'єктність і багатооб'єктність, висока проникність, відсутність геополітичної відповідності, високий ступінь довіри, залежність від темпів інформаційно-технологічного розвитку та доступності технологій, складність правового регулювання через високу динамічність, гнучкість і геополітичну, культурну суперечність правових норм» [12, с. 106]. Таким чином, можна виділити просторово-часові, трансформаційні, ефекторні та динамічні особливості глобалізованого інформаційного простору. Складність і проблемність регулювання світового інформаційного простору зумовлена неконгруентністю моделі інформаційної безпеки особливостям 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.

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 [2]. Однак динамічність і пластичність світового інформаційного простору потребує трансформації звичних інституцій і структур, що актуалізує потребу в інституційних інноваціях, які можуть суперечити усталеним правовим засновкам та управлінським структурам [13]. Правове регулювання в такому випадку має «сліпі» зони через недостатню адаптивність.

Принцип верховенства норм міжнародного права передбачає пряме застосування міжнародних норм і стандартів без національних правових обмежень у забезпеченні інформаційної безпеки [2]. Однак є ризик юрисдикційних розбіжностей, що ускладнює створення єдиного міжнародного правового поля [14]. Ці розбіжності можуть мати глибинні культурні чи релігійні засновки, наприклад, у регулюванні питань цензури, приватності.

Принцип права власності передбачає забезпечення права суб'єкта на інформацію, що регулюється чинними нормативно-правовими актами [2]. Проблемою в межах реалізації цього принципа є регулювання обміну інформацією між іноземними партнерами щодо об'єктів права власності, використання програмного забезпечення іноземного походження, розташування хмарних сховищ і серверів.

Принцип економічної доцільності систем захисту інформації ґрунтується на заходах і необхідності збереження таємниці та конфіденційності інформації, пов'язаної з власністю споживача [2]. Зважаючи на швидкість поширення

інформації, використання штучного інтелекту для продукування дезінформації, розширення поля потенційної суб'єктності та домінуючі цінності в суспільстві, величина економічних витрат і масштабність покриття є дискусійним питанням.

Принцип об'єктивності в оцінці реальних і потенційних загроз інформаційній безпеці, стану нормативно-правової та організаційної бази, а також реальних можливостей використання матеріально-технічних, людських і фінансових ресурсів [2]. Основою реалізації є цілісність сприймання інфраструктурного середовища та моделі інформаційної безпеки, що має враховувати глибинний аналіз національного та світового інформаційного простору.

Принцип безперервності забезпечення інформаційної безпеки полягає в постійному моніторингу безпекової ситуації в інформаційному секторі із супутнім застосуванням загальних і специфічних заходів реагування на виявлені загрози [2]. Це потребує високої адаптивності, оскільки швидкий розвиток інформаційних технологій потребує відповідного реагування на появу нових загроз.

Концептуально розбудова системи інформаційної безпеки має відповідати наведеним принципам, які визначають її формально-процесуальні особливості, змістове ж наповнення має спиратися на сформовану політику інформаційної безпеки та державну стратегію її реалізації.

У своїй роботі O. Bortnikova пропонує такі критерії достатності державного регулювання для реалізації політики інформаційної безпеки [2]:

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

2) правосвідомість членів суспільства;

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

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

Ці 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. Ці обмеження визначаються специфікою національного інформаційного простору в у мовах глобалізації, однією з актуальних тенденцій якого є масштабування загроз інформаційній безпеці.

Своєю чергою, K. Buhaichuk виділяє емпіричним шляхом ієрархічну структуру чинників масштабування загроз інформаційній безпеці, їх наведено в табл. 1. Оцінка впливовості чинників масштабування загроз узгоджується з критеріями достатності державного регулювання для реалізації політики інформаційної безпеки.

Таблиця 1

Впливовість чинників масштабування загроз інформаційній безпеці

Ранг	Чинники	Зміст
1	Освітньо-кваліфікаційні	Освіченість та інформованість населення щодо загроз і заходів інформаційної безпеки
2	Психологічні	Психологічна готовність до глобальних викликів і стресостійкість
3	Національно-політичні	Визначення механізмів інформаційної безпеки як елемента 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 [5].

Оцінка впливовості чинників масштабування загроз узгоджується з критеріями достатності державного регулювання для реалізації політики інформаційної безпеки. Кожен із критеріїв позначається впливом якогось із чинників масштабування загроз інформаційній безпеці, що, безумовно, детермінує проблемність адаптивності державного регулювання 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.

Результати кореляційного аналізу зв'язку між показниками соціальної, політичної, економічної глобалізації за даними KOF за 2023 р. [1] та національним індексом кібербезпеки, показником цифрового розвитку, тенденцією розвитку кібербезпеки за даними NCSI за 2023 р. [17], обчислених для 149 країн, засвідчують, що інтенсивність глобалізаційних процесів передбачає необхідність розвитку кібербезпеки (табл. 2). Кібербезпека є компонентом інформаційної безпеки й може відображати загальну тенденцію.

Таблиця 2

Зв'язок глобалізації економічної, соціальної та політичної сфер із цифровим розвитком та забезпеченням кібербезпеки, 2023 р.

Показники		Економічна глобалізація	Соціальна глобалізація	Політична глобалізація
Індекс кібербезпеки	Коефіцієнт кореляції Пірсона	0,459	0,444	0,525
	Статистична значущість	<0,001	<0,001	<0,001
Цифровий розвиток	Коефіцієнт кореляції Пірсона	0,470	0,479	0,252
	Статистична значущість	<0,001	<0,001	0,002
Тенденція розвитку кібербезпеки	Коефіцієнт кореляції Пірсона	0,137	0,114	0,442
	Статистична значущість	0,095	0,167	0,001

Джерело: сформовано автором.

На основі встановлених статистично значущих зв'язків можна стверджувати, що чим більш інтенсивнішою та масштабнішою є глобалізація в соціальній та економічній сферах, тим вищим є рівень цифрового розвитку та розвиненішою є система кібербезпеки країни. У політичній сфері встановлено більший за силою зв'язок між глобалізацією та розвиненістю системи кібербезпеки, однак значно менший за силою зв'язок із цифровим розвитком. При цьому, чим більшою є вираженість політичної глобалізації, тим більш вираженою є тенденція посилення кібербезпеки. Такі зв'язки вказують, що цифровізація не є визначальним чинником посилення кібербезпеки при зростаючій політичній глобалізації, при цьому глобалізація саме в політичній сфері визначає тенденцію посилення кібербезпеки. 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 розподілу владних повноважень на політичній арені.

Із кожним роком глобалізаційні процеси посилюються. Побудова прогностичних регресійних моделей засвідчила подальше зростання темпів масштабування загроз [5]. K. Buhaichuk впорядковує за значущістю наслідки масштабування загроз інформаційній безпеці на основі оцінки 200 респондентів, професійна діяльність яких стосується безпосередньо систем захисту інформації. 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 масштабності загроз інформаційній безпеці наведено в табл. 3.

Таблиця 3

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 у безпеці та стабільності

Джерело: сформовано автором на основі дослідження K. Buhaichuk [5].

Серед визначених чинників масштабування загроз інформаційній безпеці технічно-технологічні займають середні за значущістю позиції, їхня роль може бути медіаційною. 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 для забезпечення персональних потреб на межі моральних та правових норм. 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 у технологічність інформаційного простору як загрози та захисту. Штучний інтелект, як трансформаційна технологія, розширює поняття суб'єктності, удосконалює людські можливості та змінює масштабність загроз.

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. 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 фактора [15].

Світовий інформаційний простір є сегментованим та об'єднує такі специфічні області як «…кіберпростір, комунікаційний простір, соціальний простір, освітній простір, інформаційно-технологічний простір» [12]. Такого виду платформи є основою для кластеризації загроз термінального характеру або процесуальних загроз із установленими 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. 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 [16].

Ситуаційну обізнаність можна розглядати на оперативному, тактичному та стратегічному рівнях [16]. Кожен із 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 і 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 [18].

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. 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 обсягу 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 [19].

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 використовують 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 [11].

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 [20]. 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 у 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 [10]. Моделі штучного інтелекту не мають позбуватися свого людського компонента, повинні бути розроблені «спільні когнітивні системи» для досягнення оптимального балансу між аналітиками та алгоритмами [19].

Кожна система, яка працює в цьому світі, підпадає під дію певних правил і законів, і штучний інтелект не є винятком. Є 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 [10].

Концепція етичного штучного інтелекту передбачає [20]:

- Повагу до людської автономії. Системи штучного інтелекту завжди повинні розроблятися на основі принципів проєктування, 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 усіх 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 використовують, тощо.

Використання 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 (рис. 1).

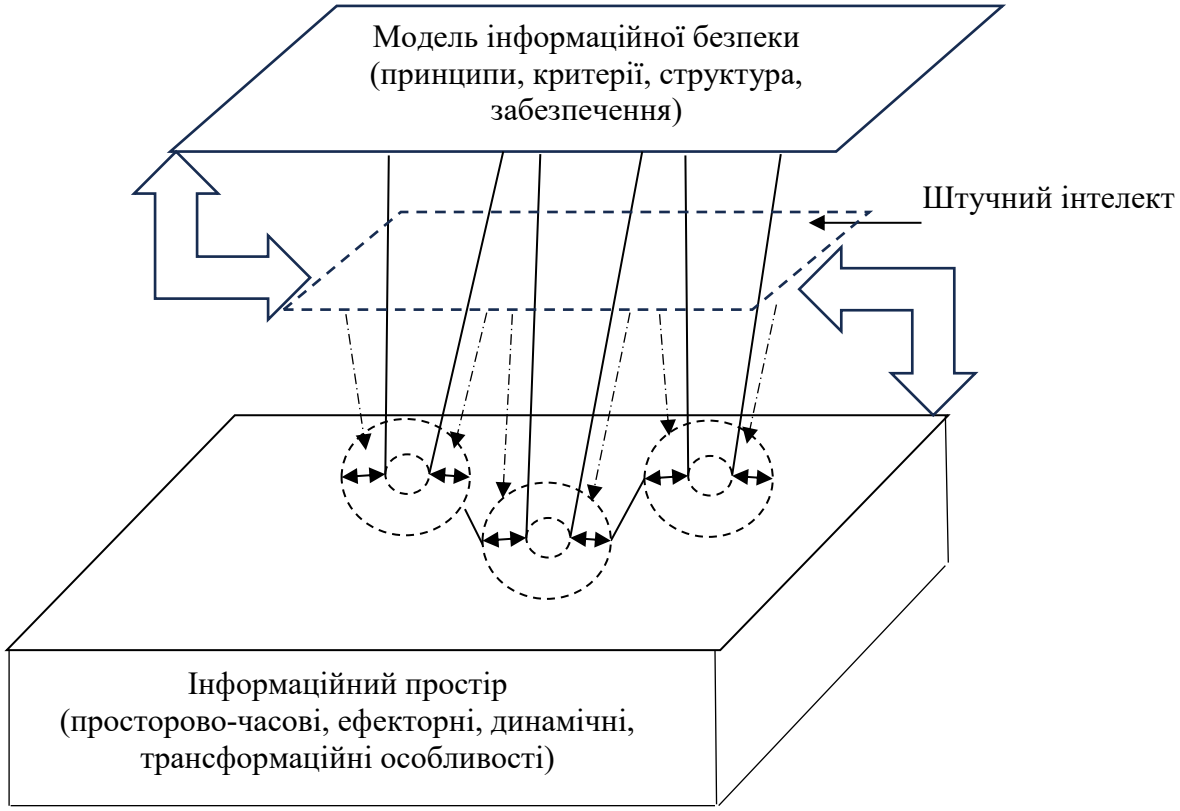

Рис. 1. Штучний інтелект в інтеграції інформаційної безпеки та інформаційного простору

Джерело: розроблено автором.

Концептуальна модель інформаційної безпеки практично реалізовується

фрагментарно, використання штучного інтелекту сприятиме більш повному її розгортанню. Використання штучного інтелекту підвищує ефективність інформаційної безпеки, розвиток моделі інформаційної безпеки сприяє розвитку систем штучного інтелекту. Особливості інформаційного простору впливають на вдосконалення систем штучного інтелекту, які, своєю чергою, трансформують інфраструктуру інформаційного простору. Будучи технологією глобалізаційного та цифрового походження, відповідаючи зростаючому масштабуванню загроз, узгоджуючись із тенденціями технологічної сингулярності, системи штучного інтелекту є органічними інфраструктурі світового інформаційного простору, їхнє використання дозволить подолати неконгруентність моделі інформаційної безпеки особливостям глобалізованого інформаційного простору.

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. Урахування цих особливостей сприятиме зменшенню невизначеності систем інформаційної безпеки та перегляду усталених принципів їхньої розробки щодо відповідності актуальним умовам зростаючої цифровізації світу.

Результати дослідження можуть бути використанні під час проєктування технологічної складової системи інформаційної безпеки, наприклад, розробки концепції інтегральної проєктивної системи інформаційної безпеки на основі принципу дуальності.

Висновки. Світовий інформаційний простір є інфраструктурним середовищем розгортання системи інформаційної безпеки. Концептуальні основи розробки та функціонування таких систем наштовхуються на проблемність у практичній реалізації через невідповідність динамічним умовам інформаційного простору. Його особливості мають ураховуватися для посилення ефективності захисту від зростаючих загроз сучасного цифрового світу. Аналіз особливостей інформаційного простору й інтеграційних можливостей штучного інтелекту є шляхом до зменшення невизначеності, підвищення швидкості та пластичності систем інформаційної безпеки в динамічних світових умовах. Як феномен глобалізації, інформаційний простір масштабується відповідно до темпів її зростання, залежно від розвиненості та доступності інформаційних технологій. Аналіз чинників і наслідків масштабування потребує перегляду суб'єктності в контексті інформаційної безпеки як щодо потенційних загроз, так і щодо захисту. Використання штучного інтелекту трансформує суб'єктність у цифрову площину, що знаменує фундаментальний перехід від простого агрегування даних до інтелектуального аналізу, що дає змогу не тільки виявляти загрози, а й здійснювати проактивний пошук.

Однак використання штучного інтелекту як і будь-якої технології має

регулюватися правилами. Використання надійного та етичного штучного інтелекту посилює інформаційну безпеку, збільшує довіру суспільства та зменшує невизначеність. 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 компонента, розробка «спільних когнітивних систем» є оптимальним балансом між аналітиками та алгоритмами.

Проведене дослідження має обмеження, що зумовлені специфікою предметної області в контексті воєнного стану в Україні та загальної міжнародної ситуації, позначеної наявним воєнним конфліктом. Питання інформаційної безпеки та активного використання технологій штучного інтелекту наразі формують актуальне проблемне поле національної безпеки, політичної впливовості на міжнародній арені та технологічної переваги в різних сферах суспільного буття. Відповідно це позначається на представленні відповідних досліджень і розробок у відкритих джерелах інформації, на використанні яких власне і ґрунтується ця теоретична оглядова робота. Проведення емпіричного дослідження в актуальних умовах має обмеження щодо публікації результатів у відкритих джерелах інформації через ризик потенційного використання даних ворожою стороною.

У подальшому поглиблення вивчення цієї проблематики передбачає розробку концепції інтегральної проєктивної системи інформаційної безпеки на основі принципу дуальності, який полягає у відповідності ключових вузлів в архітектоніці світового інформаційного простору точкам у спроєктованому інформаційному просторі системи безпеки. Кожній такій точці відповідає певний аналітичний механізм. Інтегральність системи забезпечується зв'язками між цими механізмами. Таким чином, ми відходимо від фрагментарного реагування на загрози, збільшуємо швидкість реакції та маємо пластичну систему безпеки на основі використання штучного інтелекту.

Список використаних джерел

1. KOF Index of Globalization. URL: https://kof.ethz.ch/en/forecasts-and-indicators/indicators/kof-globalisation-index.html.

2. Bortnikova O., Kashperska D., Leonov O., Rubel K. et al. Information security of the state: motives, necessity, and sufficiency criteria. *Lex Humana*. 2024. Vol. 16. No. 1. Pp. 1–19. URL: https://seer.ucp.br/seer/index.php/LexHumana/article/view/2837.

3. Wu J., Gao D., Haverly A., Mittal S. et al. AI ethics: a bibliometric analysis, critical issues, and key gaps. *International Journal of Business Analytics*. 2024. Vol. 11. Is. 1. Pp. 1–19. https://doi.org/10.48550/arXiv.2403.14681.

4. Глобенко С. Інформаційний простір державита проблеми забезпечення його захистув україні. *Науковий вісник: Державне управління*. 2023. № 1(13). С. 195–210. https://doi.org/10.33269/2618-0065-2023-1(13)-195-210.

5. Buhaichuk K., Warawa W., Batrachenko T., Cherniavska B. et al. Cybercrimes

in the global security system in modern conditions. *Lex Humana*. 2023. Vol. 15. No. 2. Pp. 26–44. URL: https://seer.ucp.br/seer/index.php/LexHumana/article/view/2474.

6. Chmyr Y., Nekryach A., Kochybei L., Dakal A. et al. 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;* eds. O. Radchenko, V. Kovach, I. Semenets-Orlova, A. Zaporozhets. Cham: Springer. Pp. 61–73. https://doi.org/10.1007/978-3-031-33724-6_4.

7. Бондар В. Т. Штучний інтелект як інструмент публічного управління в забезпеченні інформаційно-психологічної безпеки. Досвід США. *Наукові перспективи.* 2023. № 12(42). С. 81–87. https://doi.org/10.52058/2708-7530-2023-12(42)-80-87.

8. Ievdokymov V., Frikel A., Polishchuk V., Savchuk S., et al. Cybercrime and information protection in the field of state security: current threats and measures for their prevention. *Economic Affairs*. 2024. Vol. 69. Spec. is. Pp. 61–69. https://doi.org/10.46852/0424-2513.1.2024.8.

9. Hovorushchenko T., Izonin I., Kutucu H. Advancements in ai-based information technologies: solutions for quality and security. *Systems*. 2024. Vol. 12. Is. 2. 58. https://doi.org/10.3390/systems12020058.

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

11. Zacharis A., Katos V., Patsakis C. Integrating AI-driven threat intelligence and forecasting in the cyber security exercise content generation lifecycle. *International Journal of Information Security*. 2024. Vol. 23. Pp. 2691–2710. https://doi.org/ 10.1007/s10207-024-00860-w.

12. Dubovskyi O. Features of world information space in the context of criterion analysis of globalization phenomenon. *Acta De Historia & Politica: Saeculum XXI*. 2024. Vol. 8. Pp. 99–107. https://doi.org/10.26693/ahpsxxi2024.08.099.

13. Юськів Б. Глобалізація і трудова міграція в Європі: моногр. Рівне: вид. О. М. Зень, 2009. 476 с. URL: https://evnuir.vnu.edu.ua/bitstream/123456789/15964/1/Yuskiv_Global%20migration.pdf.

14. Lahmann H. Protecting the global information space in times of armed conflict. *International Review of the Red Cross*. 2020. Vol. 102. Is. 915. Pp. 1227–1248. https://doi.org/10.1017/S1816383121000400.

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

16. Skopik F., Bonitz A., Grantz V., Göhler G. From scattered data to actionable knowledge: flexible cyber security reporting in the military domain. *International Journal of Information Security*. 2022. Vol. 21. 1323–1347.

https://doi.org/10.1007/s10207-022-00613-7.

17. National Cyber Security Index (NCSI). e-Governance Academy. URL: https://ncsi.ega.ee.

18. White G. Strategic, tactical, and operational management security model. *Journal of Computer Information Systems*. 2009. Vol. 49(3). Pp. 71–75. Available at: https://www.researchgate.net/publication/289007413.

19. Ghioni R., Taddeo M., Floridi L. Open source intelligence and AI: a systematic review of the GELSI literature. *AI & Society*. 2024. Vol. 39. Pp. 1827–1842. https://doi.org/10.1007/s00146-023-01628-x.

20. European Commission. High-level expert group on artificial intelligence. Ethics guidelines for trustworthy AI. URL: https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai.

References

1. KOF Index of Globalization (n.d.). Available at: https://kof.ethz.ch/en/forecasts-and-indicators/indicators/kof-globalisation-index.html.

2. 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. Available at https://seer.ucp.br/seer/index.php/LexHumana/article/view/2837.

3. 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*, 11(1), 1–19. https://doi.org/10.4018/IJBAN.338367.

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

5. 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. Available at: https://seer.ucp.br/seer/index.php/LexHumana/article/view/2474.

6. 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. In O. Radchenko, V. Kovach, I. Semenets-Orlova, A. Zaporozhets (Eds.), *National Security Drivers of Ukraine. Contributions to Political Science* (pp. 61–73). Springer, Cham. https://doi.org/10.1007/978-3-031-33724-6_4.

7. 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.

8. 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*, 69, 61–69. https://doi.org/10.46852/0424-2513.1.2024.8.

9. Hovorushchenko, T., Izonin, I., & Kutucu, H. (2024). Advancements in ai-based information technologies: solutions for quality and security. *Systems*, 12(2), 58. https://doi.org/10.3390/systems12020058.

10. 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.

11. 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*, 23, 2691–2710. https://doi.org/10.1007/s10207-024-00860-w.

12. Dubovskyi, O. (2024). Features of world information space in the context of criterion analysis of globalization phenomenon. *Acta De Historia & Politica: Saeculum XXI*, 8, 99–107. https://doi.org/10.26693/ahpsxxi2024.08.099.

13. Yuskiv, B. (2009). *Hlobalizatsiia i trudova mihratsiia v Yevropi* [Globalization and labor migration in Europe]. O. M. Zen, Rivne.

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

15. 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.

16. 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.

17. National Cyber Security Index (NCSI) (n.d.). *e-Governance Academy*. URL: https://ncsi.ega.ee.

18. 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.

19. Ghioni, R., Taddeo, M., & Floridi, L. (2023). Open source intelligence and AI: a systematic review of the GELSI literature. *AI & Society*, 39, 1827–1842. https://doi.org/10.1007/s00146-023-01628-x.

20. European Commission (2019). *High-level expert group on artificial intelligence. Ethics guidelines for trustworthy AI*. Available at: https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai.