

socio-economic consequences and evaluating the level of effectiveness of the implementation process. This requires the formation of a new paradigm for the development of the digital economy and the provision of economic security in this area. The issue of using cloud technologies in the economic sphere also deserves attention. Since cloud technologies provide the possibility of duplication of information, simplification of remote work and security of important information, currently the question of popularizing the use of these technologies in both the public and private sectors has arisen. This can positively affect the level of economic security and national security in general. Also, the conducted scientific research allows us to talk about the importance of regulating issues of artificial intelligence development and introducing them in the field of economic security to preserve economic stability and general national security.

Key words: *government regulation, public administration, economic security, national security, digital economy, public administration bodies, innovations.*

Постановка проблеми у загальному вигляді. Вихід української економіки на траєкторію економічного зростання, а також набуття конкурентних переваг спонукає керівництво держави, компаній і впливових учасників сучасності створювати та впроваджувати інноваційні підходи до організації економічної діяльності. Метою цього є підвищення економічної ефективності та результативності діяльності, а також отримання прибутків. Використання інновацій має сприяти розвитку економіки країни. Тим часом традиційні методи повинні адаптуватися до умов сучасного суспільного розвитку.

Однією з глобальних тенденцій є максимальна цифровізація всіх процесів у державі, в тому числі й економічних. Прямий або опосередкований вплив цифрових технологій відчутний в усіх сферах економічної діяльності як на державному, так і на регіональному або локальному рівнях. Інформаційно-комунікаційна

галузь зазнає значного розвитку, про що свідчить динаміка останніх років. Розвинені країни світу перебувають на прогресивному рівні розвитку, де домінування інформаційних технологій дозволяє підвищити рівень ефективності економічних процесів у різних сферах. Разом з тим, інтенсивна цифровізація економіки актуалізує проблему забезпечення економічної безпеки, як окремої складової національної безпеки держави.

Аналіз посліdnіх досліджень і публікацій. Процес цифровізації знаходиться у центрі уваги дослідників з різних наукових напрямів. З точки зору публічного управління та забезпечення економічної безпеки країни різні аспекти зазначеного питання відображено у працях таких дослідників, як: К. Бліщук, О. Домша, Г. Давиденко, З. Живко, С. Родченко, Н. Лелюк, В. Козлов, М. Кузнецов, Т. Томашевська, О. Корнелюк, О. Паршина, Ю. Паршин, Ю. Савченко, О. Петрів. Попри значну кількість праць, важливим залишається визначення ступеню впливу сучасних тенденцій цифровізації на економічну безпеку держави в умовах швидкого розвитку технологій та кризових ситуацій, котрі супроводжують ведення бойових дій та гібридної війни.

Формулювання цілей статті (постановка завдання). Метою статті є дослідження концептуальних засад цифровізації економіки та визначення особливостей впливу процесів цифровізації на економічну безпеку.

Виклад основного матеріалу дослідження. Термін «цифрова економіка» має різноманітне значення, і наразі його розуміння залишається неоднозначним. Визначення цифрової економіки можна розглядати як економічну діяльність, що базується на використанні цифрових технологій та наявності електронних товарів чи послуг, які надані за допомогою цифрових технологій. Також, цифрова економіка може бути визначена як економіка, що ґрунтується на новітніх цифрових технологіях та методах вироблення, переробки, передачі, а також зберігання інформації. Дослідження Співробітників Світового банку підкреслюють необхідність великої уваги до покращення ділового клімату,

інвестицій в освіту у цьому напрямі та сприяння реструктуризації системи управління для країн, які прагнуть до максимальної віддачі від трансформацій у сфері інформаційно-комунікаційних технологій [9; с. 168].

Позитивні результати розвитку цифрової економіки, згідно з результатами сучасних досліджень, включають:

- 1) збільшення продуктивності праці.
- 2) підвищення рівня конкурентоспроможності бізнесу.
- 3) зменшення рівня виробничих витрат.
- 4) збільшення кількості робочих місць.
- 5) часткове вирішення проблеми соціальної нерівності.

Одночасно дослідження вказують на негативні аспекти цифровізації, серед яких [2; с. 61-63]:

1) ризик хакерських атак, що пов'язано із питанням захисту корпоративних та особистих даних.

2) так зване «цифрове рабство», тобто вирогідність використання корпоративних та особистих даних з метою маніпулювання поведінкою осіб.

3) підвищення рівня безробіття через ризик зменшення актуальності деяких професій та галузей економіки.

4) «цифровий розрив» – нерівність у доступі до цифрового середовища в різних країнах або в межах однієї країни.

Наразі все більшим стає вплив хакерських атак різні сектори суспільно-політичної та економічної діяльності, що стало реальною загрозою економічній безпеці країни як складової загальної національної безпеки (рис. 1).

Як можна побачити, згідно наведеної статистики, за I півріччя 2023 року більшість атак була на органи публічної влади різних рівнів та медіа, що опосередковано впливає на економічну безпеку. Також велику кількість атак було спрямовано на енергетичний сектор, телекомунікації, логістику та IT-сферу, що на пряму впливає на стан справ у економічному секторі та призводить до значних економічних втрат.

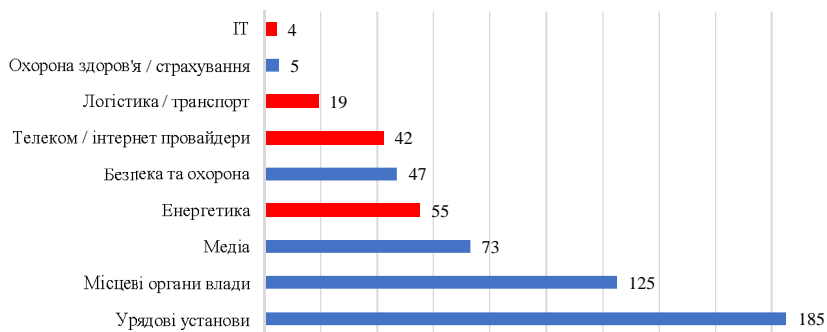


Рис. 1. Кількість хакерських атак за секторами,
I півріччя 2023 року.

Джерело: [12]

Яскравим прикладом надзвичайно великої загрози для економічної безпеки та загалом національної безпеки України стала атака на телекомунікаційного оператора Київстар. Це призвело до значних економічних втрат як державного, так і приватного сектора. Не менш важливим стало заворушення в українському суспільстві, оскільки Київстар є одним з найбільших в Україні операторів мобільного зв'язку (рис. 2).

Відсутність мобільного зв'язку може призвести до колапсу, оскільки це обмежує комунікацію та отримання інформації, може руйнувати зв'язки та загалом зупиняти економічні процеси, особливо за умови відсутності альтернативних каналів зв'язку.

Незважаючи на можливі загрози, важливо відзначити, що цифровізація швидко охоплює сферу послуг, торгівлю, фінансовий сектор, освіту та управління. Позитивні наслідки таких процесів стають ключовими як для держави, так і для підприємців. Серед переваг цифрової економіки виділяють високу швидкість, зменшення вартості послуг (в онлайн-режимі послуги коштують менше) та винайдення інноваційних джерел доходу. Крім того, підприємства отримують можливість виходити на глобальний ринок та підвищувати доступність своїх товарів та послуг як в

межах держави, так і за кордоном. Інноваційні товари можуть бути адаптовані до вимог замовника в короткі терміни, незважаючи на віддаленість виробничих об'єктів. Також важливо відзначити, що цифрова економіка розширює можливості надання нового різноманітного контенту споживачам: наукового, освітнього, розважального характеру.

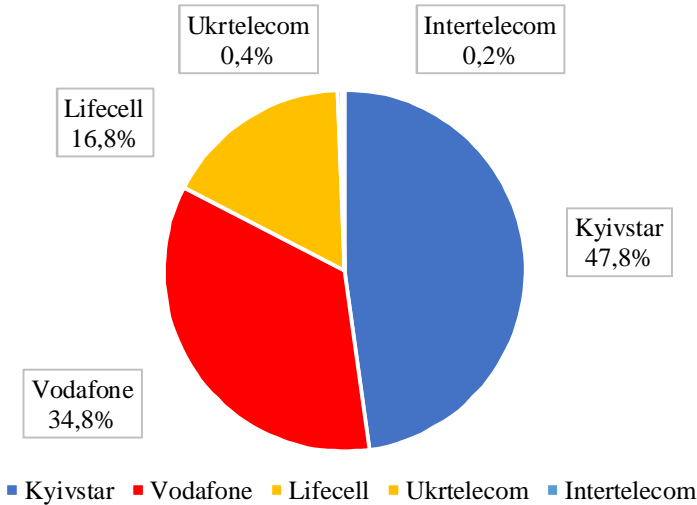


Рис. 2. Користувачі мобільного зв'язку в Україні за оператором.
Джерело: [14]

Процеси впровадження інформаційних технологій впливають на всі сфери суспільства і різні аспекти діяльності, включаючи професійне та особисте життя. Масштабні програми розвитку цифрової економіки та швидкі темпи поширення інформаційно-комунікаційних технологій в усі сфери суспільного життя визначають необхідність вироблення методології для визначення суспільно-економічних наслідків та оцінювання рівня ефективності процесу впровадження [15]. Це вимагає формування нової парадигми розвитку цифрової економіки та забезпечення економічної безпеки у даній сфері.

Звітування Всесвітньої організації інтелектуальної власності та оприлюднення Глобального індексу інновацій відкриває перед широким загалом картину глобальних інноваційних тенденцій в умовах економічної невизначеності. Цей щорічний звіт представляє рейтинг найбільш інноваційно спрямованих економік у світі серед 132 країн та визначає 100 найкращих інноваційних кластерів. Під час дослідження інновацій враховується понад 80 показників інноваційного потенціалу, таких як інвестиції в дослідження та розробку, витрати на освіту та виробництво високотехнологічних товарів. Важливо відзначити, що існують значущі розбіжності у інноваційному потенціалі країн, що опосередковано може впливати на економічну безпеку у розрізі збільшення цифрової складової у загальній економіці (рис. 3).

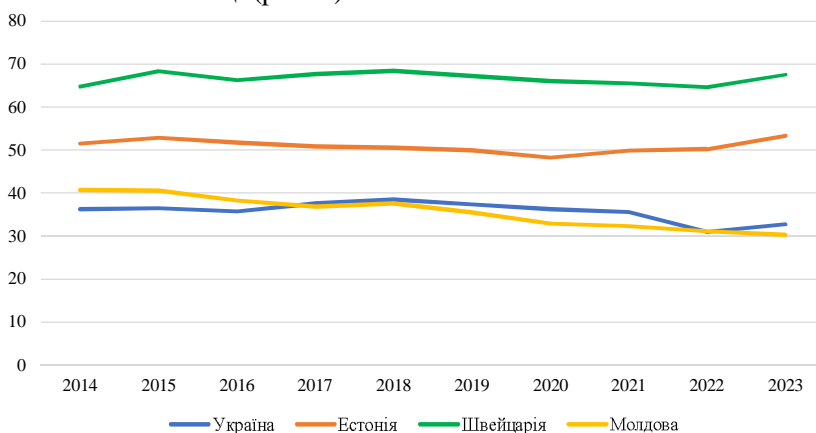


Рис. 3. Глобальний індекс інновацій.

Джерело: [13]

Для порівняння було взято:

- Швейцарію, котра у переважній більшості займає перші місця у рейтингу інноваційного розвитку;
- Естонію, котра вважається найрозвиненішою пострадянською країною у напрямку цифровізації соціально-економічних відносин та економіки в цілому;

– Молдову, котра також є пострадянською країною, розташована по сусідству та загалом має достатньо низький рівень розвитку економіки.

Як можна побачити з рисунку 3, Україна, нажаль, дуже відстає в плані розвитку інновацій, що загалом впливає на стан економіки, готовність до нових викликів, а також забезпечення економічної безпеки в умовах ведення гібридної війни.

Інформаційна індустрія, що включає в себе виробництво, збір, поширення та передачу інформації, є однією з найбільш динамічно розвиваючихся галузей світової економіки, з її зростанням на рівні 7,8% щорічно [6, с. 59]. Однак місце та роль інформаційної індустрії не обмежуються лише прямим внеском у валовий внутрішній продукт.

Стрімка цифровізація економіки в Україні має низку переваг:

1. Прогрес та розвиток всіх сфер економіки безпосередньо переплітаються з просуванням цифрової індустрії. В розвинених країнах нові технології (інноваційний потенціал) стимулюють збільшення національного доходу майже на 60%, тоді як праця, капітал і природні ресурси здійснюють свій внесок по 10% і 15% відповідно.

2. Експортна потужність, конкурентоспроможність продукції та створення значної кількості нових робочих місць на пряму залежать від прогресу цифрової інфраструктури.

3. Основним багатством будь-якого суспільства є людина. При цьому, рівень життя, освіти та культури кожного індивіда залежить від можливостей отримання, обробки та використання інформації. Традиційні джерела інформації, такі як книги та періодичні видання, разом із культурною, освітньою та розважальною інформацією (преса, радіо, телебачення), а також технічні засоби спілкування, як наприклад телефонний зв'язок, об'єднуються в єдине інформаційне середовище, яке дає доступ до безмежних ресурсів цифрової інформації у формі текстів, аудіо-, відео-, графічних та мультимедійних матеріалів. Це середовище використовується також для обміну та розповсюдження інформації.

4. Сьогоднішня інформаційна інфраструктура суспільства надає можливості, які раніше були недоступні людині, такі як дистанційна освіта, медичне обслуговування та робота вдома, що формує новий якісний спосіб життя, дозволяє оптимізувати робочі процеси та дозволяє зменшити витрати.

5. Інформаційна інфраструктура суспільства та технології дозволяють кардинально змінити способи та засоби функціонування органів публічної влади та управління на всіх рівнях через:

- підвищення ефективності виконання функцій владного апарату (наприклад, автоматизація документообігу, впровадження служб віддаленого обміну інформацією, таких як електронна пошта, факсимільний зв'язок, відеоконференції тощо);

- забезпечення усіма необхідними для управлінських рішень даними;

- забезпечення швидкої комунікації між управлінськими органами та представниками суспільства. Такий підхід робить діяльність органів публічної влади більш прозорою для суспільства і водночас відкриває можливості для швидкого врахування громадської думки та налагодження тісної взаємодії з різними соціальними групами [7].

Разом з тим, варто відмітити, що зазначені переваги можуть супроводжуватись низкою загроз економічній безпеці:

1) поширеність цифрових технологій та залежність національної економіки від них призводить до все більшої залежності економічних процесів від нових факторів впливу. це може бути як суто технічний фактор – відсутність електроенергії, так і технологічний – комп'ютерні віруси, хакерські атаки, помилки програмного забезпечення тощо.

2) віддаленість робочих місць вимагає обміну широким колом документації, у тому числі й такої, що становить таємницю. відповідно, виникає загроза втручання в такий документообіг та потрапляння важливої інформації у чужі руки.

3) необмежений доступ до цифрового середовища може бути оманливим, оскільки часто доволі важко визначити вірність

отриманої інформації. у таких умовах прийняття управлінських рішень та ведення економічної діяльності може ґрунтуватись на неточній або взагалі невірній інформації, що матиме негативний вплив на рівень економічної безпеки.

4) якість дистанційної освіти є суперечливою, оскільки багато в чому залежить від сумлінності особи, що навчається, а отримання з мережі недостовірної інформації може в подальшому вплинути на економічні процеси, у яких буде задіяна ця особа.

5) комунікація між органами публічної влади та суспільством, визначення, врахування та вплив на громадську думку може супроводжуватись недоброчесністю учасників та зовнішнім впливом. як результат – розхитування суспільно-політичної та економічної ситуації в країні [18].

Цифрова економіка базується на самому нижньому рівні ланцюга торговельно-виробничих відносин – цифрових компаніях, які активно працюють над адаптацією власних бізнес-процесів до функціонування у онлайн-режимі. Це охоплює управлінську діяльність, контроль та подальший аналіз усіх ключових бізнес-процесів у реальному часі, таких як проведення закупівель, реєстрація угод, узгодження договорів, організація бухгалтерського обліку, впровадження ефективної логістики, координація з партнерами, системний моніторинг контактів з клієнтами та технічна підтримка усіх бізнес-процесів.

Загальний цифровий супровід економічних процесів в Україні супроводжується значною неоднорідністю (рис. 4). Якщо доступ до мережі Інтернет мають майже всі підприємства, що зберіглося навіть в умовах широкомасштабної війни, то використання соціальних медіа характерна лише для третини підприємств. Подібне ігнорування швидких каналів зв'язку можна кваліфікувати як значне упущення, оскільки за допомогою використання соціальних медіа можна протидіяти загрозам економічної безпеки та загалом організувати превентивні заходи для попередження негативних наслідків.

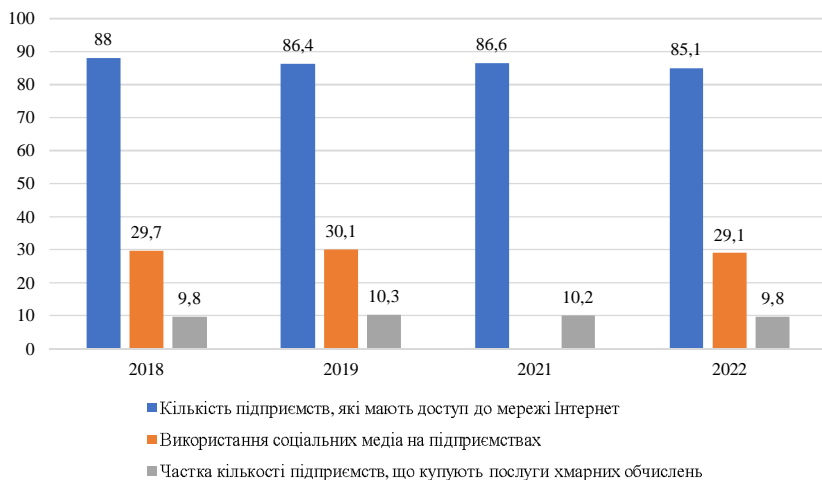


Рис. 4. Використання інформаційно-комунікаційних технологій на підприємствах у % до загальної кількості підприємств.

Джерело: [3]

Також заслуговує на увагу питання використання хмарних технологій у економічній сфері. В останні роки цей напрямок зазнав поширення (рис. 4), однак рівень поширення на рівні 10% є достатньо малим. Оскільки хмарні технології дають можливість дублювання інформації, спрощення віддаленої роботи та безпеку збереження важливої інформації, наразі постало питання популяризації використання цих технологій як в публічному так і приватному секторі. Це може позитивно вплинути на рівень економічної безпеки та національної безпеки загалом.

Протягом часу ведення повномасштабної війни в Україні було зроблено значні кроки у цьому напрямку. Згідно статистичної інформації, наданої телекомунікаційним оператором Київстар, серед різних галузей економіки України з травня 2022 року до червня 2023 року можна простежити значний приріст у використанні хмарних технологій (рис. 5).

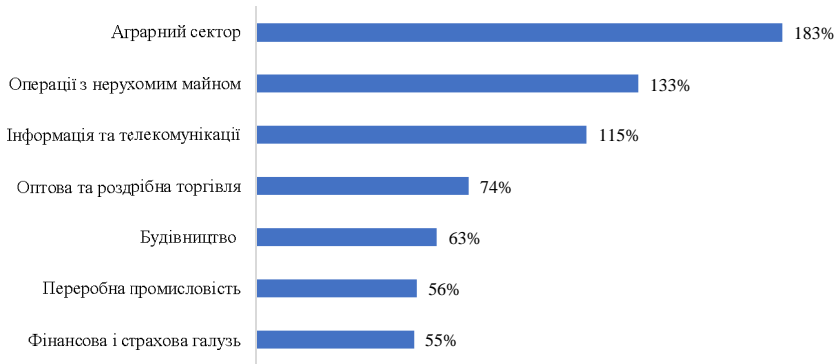


Рис. 5. Приріст використання хмарних технологій в Україні в різних галузях економіки з травня 2022 року до червня 2023 року
Джерело: [5]

Для успішної діяльності в умовах цифровізації економіки важливими є три складові елементи:

- 1) інфраструктура (телекомунікації, програмне забезпечення, доступ до Інтернету).
- 2) електронний бізнес (господарювання через Інтернет-мережу).
- 3) електронна комерція (розповсюдження товарів та послуг через Інтернет-мережу) [1].

Стосовно присутності цифрових технологій у економічній діяльності можна констатувати, що кількість підприємств, що супроводжують свою діяльність електронною торгівлею, є невеликою, однак стабільною. При цьому обсяги електронної торгівлі мають стабільну тенденцію до зростання (рис. 6). Звісно, що це має позитивний вплив на розвиток економіки країни, однак разом з цим варто говорити про необхідність приділяти увагу як публічним, так і приватним секторам економічній безпеці у цьому напрямку.

За останні кілька років стрімко набирають популярності інтелектуальні інформаційні технології. Вони вміють опрацьовувати різноманітні дані за допомогою алгоритмів штучного інтелекту для

отримання цілком нового, відмінного від попередньої інформації результату. Використання інтелектуальних інформаційних технологій дозволяє формулювати та корегувати дії, котрі раніше традиційно вважалися властивими лише людському інтелекту. Походження інтелектуальних інформаційних технологій пов'язане з впровадженням практичних систем прийняття рішень та штучного інтелекту, їхнє взаємодіюче використання сприяло підвищенню ефективності у процесі прийняття рішень [17].



Рис. 6. Кількість підприємств, які здійснювали електронну торгівлю та обсяг реалізованої продукції (товарів, послуг), отриманий від електронної торгівлі.

Джерело: [3]

Серед важливих характеристик інтелектуальних інформаційних технологій виділяється їх здатність до самостійного розвитку та навчання. Фактично будь-який інтелектуальний процес може бути описаний та симульований, що призводить до накопичення бази знань та бази даних з конкретними прикладами розв'язаних завдань. Використання у бізнес-процесах подібних технологій дає

можливість знаходити рішення на основі обмеженої інформації, оскільки інтелектуальні інформаційні технології не лише зберігають інформацію та досвід різних відомих фахівців у різних сферах життєдіяльності, але й генерують цілком нові альтернативи рішень. Застосування інтелектуальних інформаційних технологій прискорює аналіз проблем у різних галузях, включаючи технічні, економічні, соціальні та екологічні [4].

Однак, як і більшість досягнень людської цивілізації, вищезазначені технології можна використовувати як на користь, так і для того, щоб нанести шкоду. В контексті досліджуваної теми важливою проблемою для економічної безпеки як публічного, так і приватного сектору, стає результати роботи штучного інтелекту [16]. Наприклад, штучний інтелект може використовуватись для імітації фото- і відеозображень, голосу відомих людей або створення фейкових текстів.

Сучасний світ регулярно стикається з викликом у вигляді дезінформації, що активно генерується завдяки штучному інтелекту. Це призводить до значних ризиків, таких як підрив довіри до авторитетних джерел, маніпулювання громадською думкою та можливі репутаційні й фінансові втрати. У глобальному плані такі технології можуть бути використані у політичній діяльності та на міжнародній арені, що може призвести до непередбачуваних негативних наслідків.

Все вищезазначене викликає занепокоєння з боку представників влади у різних країнах та вимагає певної реакції. Так, уряд Великої Британії визнав штучний інтелект як загрозу в рамках «Національного реєстру ризиків». За даними реєстру на 2023 рік, це стало першим офіційним визнанням ризику пов'язаного із штучним інтелектом. Уряд Великої Британії наголосив, що розвиток сервісів зі штучним інтелектом та їх можливостей призводить до різноманітних наслідків, включаючи гострі ризики та розпалювання негативних думок серед людей. Одним із таких наслідків, як вказано у реєстрі, є зростання дезінформації в разі несумлінного використання систем штучного інтелекту, а також можливе зниження рівня економічної

конкурентоспроможності. Відзначивши це, уряд Великої Британії заявив про наміри організувати глобальний саміт стосовно безпеки використання штучного інтелекту, котрий об'єднає розвинені країни, компанії технологічного спрямування і дослідників у цій галузі, з метою координації заходів безпеки для оцінки та контролю ризиків, пов'язаних із штучним інтелектом [10].

Питання штучного інтелекту та його місця в забезпеченні економічної безпеки знайшло своє відображення у «Концепції розвитку штучного інтелекту в Україні» [11]. В цьому документі серед сучасних проблем соціально-економічного розвитку України зазначено:

- відсутність або неповне закріплення правових норм використання штучного інтелекту (включаючи сфери публічного управління, безпеки, оборони, економіки тощо), та неповна розробка законодавства щодо захисту особистих даних;
- низький рівень захисту даних та інформаційної безпеки через застарілі системи моніторингу та попередження інформаційних загроз, а також недостатнє використання потенціалу прогнозування для передбачення загроз і підготовки системи до можливих атак;
- відсутність єдиних стандартів для визначення етичних критеріїв при розробці та використанні технологій штучного інтелекту у різних сферах, видах діяльності та сферах національної економіки [11].

З погляду контролю за використанням штучного інтелекту в галузі економічної безпеки можна визначити наступні ключові напрямки:

- використання штучного інтелекту дає змогу виявляти, а також вчасно реагувати на кіберзагрози набагато оперативніше та точніше. Використання машинного навчання та аналіз значних обсягів даних допомагає виявляти загрози та зловмисну діяльність у цифровому просторі, сприяючи своєчасній нейтралізації загроз;
- впровадження штучного інтелекту в системи управління, прийняття рішень, моніторингу, запобігання та протидії загрозам в сфері економіки підвищує рівень економічної безпеки. При цьому,

автоматизовані системи прийняття рішень можуть ефективно управляти різними процедурами та забезпечувати захист важливої інформації;

– штучний інтелект здатен аналізувати значні обсяги інформації, а також робити прогнози стосовно можливих загроз, сприяючи більш ефективній реакції на потенційні джерела виникнення загроз економічної безпеки;

– розвиток штучного інтелекту у галузі економічної безпеки може стимулювати наукові дослідження та ведення інноваційної діяльності в економічній безпеці, сприяючи зростанню технологічного потенціалу держави та паралельному підвищенню рівня її конкурентоспроможності на міжнародній арені;

– запровадження моделювання на основі штучного інтелекту з метою передбачення негативних подій та вірогідних загроз економічній безпеці може допомагати вчасно реагувати та вживати відповідних заходів для організації превентивних заходів [8].

Отже, проведені наукові дослідження дозволяють говорити про важливість регулювання питань розвитку штучного інтелекту та запровадження їх у галузі економічної безпеки для збереження економічної стабільності та загальної національної безпеки.

Висновки. Отже, можна констатувати, що цифровізація економіки країни являє собою доволі визначальний фактор впливу на економічну безпеку. Поряд з великим переліком позитивних наслідків цифровізації, серед яких оптимізація економічних процесів, спрощення комунікацій та створення нових більш простих процедур, прослідковується й низка потенційних загроз. Це пов'язано із захистом інформації, маніпулюванням даними, використанням важливої інформації у підривній діяльності тощо. Однак, варто наголосити, що цифрові технології в економіці – це лише інструмент для досягнення поставлених цілей і тільки від суб'єкта їх використання буде залежати результат. Той самий штучний інтелект, як один зі складових елементів цифровізації може бути як загрозою економічній безпеці у разі ведення підривної діяльності, так і надійним інструментом забезпечення постійного

безробіття через ризик зменшення актуальності деяких професій та галузей економіки; «цифровий розрив» - нерівність у доступі до цифрового середовища в різних країнах або в межах однієї країни.

Доведено, що процеси впровадження інформаційних технологій впливають на всі сфери суспільства і різні аспекти діяльності, включаючи професійне та особисте життя. Масштабні програми розвитку цифрової економіки та швидкі темпи поширення інформаційно-комунікаційних технологій в усі сфери суспільного життя визначають необхідність вироблення методології для визначення суспільно-економічних наслідків та оцінювання рівня ефективності процесу впровадження. Це вимагає формування нової парадигми розвитку цифрової економіки та забезпечення економічної безпеки у даній сфері. Також заслуговує на увагу питання використання хмарних технологій у економічній сфері. Оскільки хмарні технології дають можливість дублювання інформації, спрощення віддаленої роботи та безпеку збереження важливої інформації, наразі постало питання популяризації використання цих технологій як в публічному так і приватному секторі. Це може позитивно вплинути на рівень економічної безпеки та національної безпеки загалом. Також проведені наукові дослідження дозволяють говорити про важливість регулювання питань розвитку штучного інтелекту та запровадження їх у галузі економічної безпеки для збереження економічної стабільності та загальної національної безпеки.

Ключові слова: державне регулювання, державне управління, економічна безпека, національна безпека, цифрова економіка, органи публічного управління, інновації.

Received: 23.10.23

References

1. Blishchuk, K.M., & Domsha, O.V. (2020). Tsyfrova ekonomika yak skladova rozvytku systemy publichnogo upravlinnia [Digital economy as a com-

ponent of the development of the public administration system]. *Efektivnist derzhavnoho upravlinnia – Efficiency of Public Administration*, 4(65), (pp. 183-194) [in Ukrainian].

2. Davydenko, H. (2023). *Tsyfrova inkluziia ta dostupnist: sotsialna didzhitalizatsiia: monografiia [Digital Inclusion and Accessibility: Social Digitization: A Monograph]*. TVORY, Vinnytsia, Ukraine [in Ukrainian].

3. State Statistics Service of Ukraine. (n.d.). *ukrstat.gov.ua*. Retrieved from: <https://ukrstat.gov.ua> [in Ukrainian].

4. Zhyvko, Z.B., Rodchenko, S.S., & Leliuk, N.Ye. (2022). Tsyfrova ekonomika: sutnist, oznaky ta zavdannia upravlinnia [Digital economy: essence, features and tasks of management]. *Naukovyi pohliad: ekonomika ta upravlinnia - Scientific view: economics and management*, 2, (pp. 31-37) [in Ukrainian].

5. Z pochatku velykoi viiny popyt na khmarni rishennia zbilshyvsia u 7 raziv, – statystyka Kyivstaru [Since the beginning of the Great War, the demand for cloud solutions has increased 7 times, according to Kyivstar statistics]. (n.d.). *www.unian.ua*. Retrieved from: <https://www.unian.ua/economics/telecom/z-pochatku-velikoji-viyni-popit-na-hmarni-rishenny-a-zbilshivsvya-u-7-raziv-statistika-kijivstaru-12429441.html> [in Ukrainian].

6. Kozlov, V.V., & Tomashevska, T.V. (2021). Tsyfrova ekonomika: peredumovy, zahrozy ta perspektyvy [Digital economy: prerequisites, threats and prospects]. *Statystyka Ukrainy – Statistics of Ukraine*, 2, (pp. 58-66) [in Ukrainian].

7. Kozlov, V.V., Tomashevska, T.V., & Kuznetsov, M.I. (2020). Tsyfrova ekonomika: peredumovy ta perspektyvy [Digital economy: preconditions and prospects]. Proceedings from DSou: financial, economic and humanitarian aspects'20: *VII Mizhnarodna naukovo-praktychna konferentsiia – VII International Scientific and Practical Conference*. (pp. 303–307). Kyiv. Retrieved from: http://194.44.12.92:8080/jspui/bitstream/123456789/5234/1/10-11-36ip-ник%202020_0311-0315.pdf [in Ukrainian].

8. Korneliuk, O. (2023). Rozvytok ta rehuliuвання shtuchnoho intelektu v Ukraini u voiennyi ta povoienni periods: suchasni tendentsii ta perspektyvy [Development and regulation of artificial intelligence in Ukraine in the war and post-war periods: current trends and perspectives]. *Tsyfrova ekonomika ta ekonomichna bezpeka – Digital economy and economic security*, 8 (08), (pp. 105-111) [in Ukrainian].

9. Parshyna O.A., Parshyn Yu.I., Savchenko Yu.V. (2019). Ekonomichna bezpeka v umovakh didzhitalizatsii: suchasnyi stan ta perspektyvy rozvytku informatsiinoho suspilstva [Economic security in the conditions of digitalization: the current state and prospects for the development of the information society].

Naukovyi visnyk Dnipropetrovskoho derzhavnoho universytetu vnutrishnikh sprav – Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs, 2, (pp. 167-174) [in Ukrainian].

10. Petriv, O. (2023). *Dezinformatsiia ta shtuchnyi intelekt: (ne)vydyma zahroza suchasnosti [Disinformation and artificial intelligence: an (in)visible threat to modernity]*. Center for Democracy and Rule of Law. Retrieved from: <https://cedem.org.ua/analytics/dezinformatsiya-shtuchnyi-intelekt> [in Ukrainian].

11. Rozporiadzhennia Kabinetu Ministriv Ukrainy Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini vid 02.12.2020 No 1556-p. [Decree of the Cabinet of Ministers of Ukraine on the approval of the Concept of the development of artificial intelligence in Ukraine dated 02.12.2020 No 1556-p]. *zakon.rada.gov.ua*. Retrieved from: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text> [in Ukrainian].

12. Rosiiski kiberoperatsii. Analytika za pershe pivrichchia 2023 roku. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy [Russian cyber operations. Analytics for the first half of 2023. State Service of Special Communications and Information Protection of Ukraine]. (2023). *cip.gov.ua*. Retrieved from: <https://cip.gov.ua> [in Ukrainian].

13. Global Innovation Index. WIPO. (n.d.). *www.wipo.int*. Retrieved from: https://www.wipo.int/global_innovation_index/en [in English].

14. TeleGeography. (n.d.). *www2.telegeography.com*. Retrieved from: <https://www2.telegeography.com> [in English].

15. Antonova, L., & Antonov, A. (2023). Perspektivy vdoskonalennia derzhavnoho rehuliuвання zovnishnoekonomichnoi diialnosti v Ukraini kriz pryzmu zabezpechennia ekonomichnoi bezpeky derzhavy. [Prospects for improving the state regulation of foreign economic activity in Ukraine through the prism of ensuring the economic security of the state]. *Publichne upravlinnia ta administruvannia – Public administration and regional development*, (21), (pp. 759-788). Retrieved from: <https://doi.org/10.34132/pard2023.21.07> [in Ukrainian].

16. Zhovnirchuk, Y., Prykhodko, I., Romin, A., Bandura, I., & Vavreniuk, S. (2023). Public Management of SMART Specialization of Sustainable Development of the Region in the System of Ensuring innovation Security. *International Journal of Sustainable Development and Planning*, (Vol. 18), 2, (pp. 385-391). Retrieved from: <http://doi.org/10.18280/ijstdp.180206> [in English].

17. Bondar, H.L. (2023). Tsyfrovizatsiia ta spivpratsia Yevropeiskoho soiuzu ta Ukrainy [Digitization and cooperation of the European Union and

Ukraine]. *Publichne upravlinnia ta rehionalnyi rozvytok – Public administration and regional development*, (20), (pp. 330-352). Retrieved from: <https://doi.org/10.34132/pard2023.20.03> [in Ukrainian].\

18. Yemelyanov, V., & Bondar, H. (2019). Kiberbezpeka yak skladova natsionalnoi bezpeky ta kiberzakhyst krytychnoi infrastruktury Ukrainy [Cyber security as a component of national security and cyber protection of critical infrastructure of Ukraine]. *Publichne upravlinnia ta rehionalnyi rozvytok – Public administration and regional development*, (5), (pp. 493-523). Retrieved from: <https://doi.org/10.34132/pard2019.05.02> [in Ukrainian].

Відомості про авторів / Information about the Authors

Віталій Равлюк: Державне публічне акціонерне товариство «Національна акціонерна компанія «Украгролізінг»: вул. Мечникова, 16-а, Київ, 01601, Україна.

Vitaliy Ravlyuk: State public joint-stock company «National joint-stock company «Ukragroleasing»: st. Mechnikova, 16-a, Kyiv, 01601, Ukraine.

ORCID. ORG./ 0009-0001-2875-1442

E-mail: Vvr1969@ukr.net