СЕКЦІЯ 3
ЕКОНОМІЧНА, ІНФОРМАЦІЙНА, ВОЄННА, ЕНЕРГЕТИЧНА БЕЗПЕКА: АДАПТИВНІ МЕХАНІЗМИ МІНІМІЗАЦІЇ РИЗИКІВ У ЦИФРОВОМУ ПРОСТОРІ

Модератори секції: Клопов Іван – д.е.н., проф., Мороз Олег – к.е.н., доц., Крупа Андрій – аспірант спеціальності «Менеджмент».

DOI https://doi.org/10.36059/978-966-397-447-7-3

УДК 351.86:321

АРАБАДЖИЄВ ДМИТРО ЮРІЙОВИЧ,
д.політ.н., проф., начальник науково-дослідної частини,
проф. кафедри бізнес-адміністрування та менеджменту
зовнішньоекономічної діяльності
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: dimariy026@gmail.com
ORCID ID: https://orcid.org/0000-0002-4772-081X

ПОЛІТИЧНА БЕЗПЕКА ЯК СТРАТЕГІЧНИЙ ЧИННИК ЗБЕРЕЖЕННЯ НАЦІОНАЛЬНИХ ІНТЕРЕСІВ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ

Політична безпека є ключовим аспектом національної безпеки, що охоплює захист політичних інститутів, процесів, ідеологій та державного суверенітету від внутрішніх і зовнішніх загроз. Вона включає в себе стабільність державної влади, законність і прозорість політичних процесів, дотримання прав людини, запобігання політичним конфліктам і екстремізму. Політична безпека стосується захисту від зовнішнього впливу, такого як втручання інших держав у внутрішні політичні справи, інформаційна війна, пропаганда або інші форми гібридної війни, які можуть дестабілізувати країну. У сучасних умовах значне значення має забезпечення кібербезпеки, що захищає політичні структури від кібератак і маніпуляцій у цифровому просторі [1].

Сучасні виклики політичній безпеці включають зростання популізму, політичну поляризацію, втручання іноземних держав у виборчі процеси, а також використання новітніх технологій для впливу на політичну

свідомість громадян. Важливою складовою політичної безпеки є ефективне управління і запобігання корупції, що сприяє довірі громадян до державних інституцій і стабільності політичної системи. Політична безпека тісно пов'язана з іншими аспектами національної безпеки, такими як економічна, військова, соціальна, інформаційна безпека, має фундаментальне значення для збереження державного суверенітету та незалежності [2].

Політична безпека – стан захищеності політичної системи, держав них інститутів, суверенітету та національної ідентичності від внутрішніх і зовнішніх загроз, які можуть дестабілізувати або зруйнувати політичний порядок країни. Ця концепція охоплює захист від впливу інших держав, організацій або окремих осіб, що можуть впливати на політичну стабільність через різноманітні методи, включаючи інформаційну війну, пропаганду, економічний тиск або втручання у внутрішні справи. Політична безпека є важливою складовою національної безпеки, оскільки політична стабільність і суверенітет держави безпосередньо впливають на її здатність забезпечувати безпеку в інших сферах, таких як економіка, оборона та соціальна сфера (табл. 1).

Таблиця 1 – **Ключові аспекти політичної безпеки**

Ключові аспекти	**Зміст та характеристика**
1	2
Стабільність політичної системи	Здатність політичних інститутів ефективно функціонувати без значних змін або загроз дестабілізації. Збереження законності, легітимності та прозорості політичних процесів. Запобігання екстремізму, радикалізму та політичній поляризації.
Захист державного суверенітету	Охорона територіальної цілісності та незалежності держави від зовнішніх загроз. Захист від втручання іноземних держав у внутрішні політичні справи, включаючи інформаційні атаки та пропаганду. Ефективне управління зовнішньою політикою та міжнародними відносинами. Захист державного суверенітету. Забезпечення контролю держави над своєю територією, населенням і ресурсами, а також недопущення втручання з боку інших держав або суб'єктів міжнародного права.
Захист національної ідентичності	Підтримка і розвиток національної культури, мови, релігії та інших аспектів, що формують унікальність нації, а також боротьба проти загроз асиміляції або культурного розмивання.

Продовження таблиці 1

1	2
Політична стабільність державний лад	Недопущення політичних криз, які можуть призвести до переворотів, революцій, громадянських війн або інших форм насильства, що ставлять під загрозу.
Кібербезпека	Захист політичних інститутів і процесів від кібератак, які можуть дестабілізувати державу або вплинути на політичну свідомість громадян. Забезпечення безпеки інформаційних систем, які використовуються в державному управлінні та під час виборів.
Захист конституційного ладу	Забезпечення дотримання Конституції та законів, які регулюють політичну систему. Запобігання спробам узурпації влади або насильницьких змін у політичній системі.
Політична легітимність і довіра громадян	Забезпечення довіри громадян до політичних інститутів через відкриті, прозорі та справедливі виборчі процеси. Боротьба з корупцією та зловживанням владою, які можуть підірвати довіру громадян до держави. Забезпечення участі громадян у політичному житті через механізми демократії.
Інформаційна безпека	Захист від інформаційних атак, дезінформації та пропаганди, що можуть вплинути на політичну стабільність. Розвиток інформаційної грамотності серед населення для запобігання маніпуляціям у ЗМІ та соціальних мережах.
Правове забезпечення політичної безпеки	Розробка і впровадження правової бази, яка регулює політичну діяльність і забезпечує захист від загроз політичній стабільності. Своєчасне оновлення законодавства для адаптації до нових викликів і загроз.
Стабільність політичних інститутів	Підтримання безперервного і ефективного функціонування держав- них органів, таких як уряд, парламент, судова система, щоб уникнути кризових ситуацій або політичного хаосу.
Правоохоронна та контррозвідувальна діяльність	Робота силових структур, спрямована на виявлення, запобігання і нейтралізацію загроз політичній безпеці, таких як тероризм, екстремізм, шпигунство тощо.
Виборча безпека	Забезпечення чесних і прозорих виборів, що є основою демократичного суспільства, та захист від зовнішнього втручання в цей процес.
Інформаційна безпека	Захист суспільства від маніпуляцій, дезінформації та пропаганди, спрямованих на дестабілізацію внутрішньої ситуації або вплив на політичні процеси.

Складові політичної безпеки можна поділити на кілька основних компонентів, кожен з яких має критичне значення для забезпечення стабільності та стійкості політичної системи. Ці складові політичної безпеки взаємопов'язані й утворюють цілісну систему, яка дозволяє державі ефективно функціонувати, підтримувати стабільність і захищати свої інтересияк на внутрішньому, так і на міжнародному рівнях. Слід виявити умови, які сприяють забезпеченню політичної безпеки [3].

Органи національної безпеки завжди наполягали на тому, щоб вважати людей основною відправною точкою та опорою забезпечення національної безпеки, що національна безпека – для людей. Безпека в різних галузях взаємопов'язана та впливає одна на одну. Органи національної безпеки завжди дотримувалися загальної концепції національної безпеки як керівництва, приймаючи підтримку політичної безпеки як основне завдання, координуючи та зміцнюючи роботу в традиційних галузях безпеки, таких як військова та внутрішня безпека, та нетрадиційних галузях безпеки, таких як наука та технологія, фінанси та біологія, запобігання та усунення інших областей.

Забезпечення політичної безпеки вимагає постійної уваги та зусиль з боку держави, суспільства та міжнародної спільноти, оскільки загрози можуть мати динамічний і непередбачуваний характер. Зарубіжний досвід забезпечення політичної безпеки є різноманітним і залежить від політичних, соціальних, культурних та історичних особливостей кожної країни. Без політичної безпеки будь-яка країна неминуче розвалиться на частини, і неможливо буде говорити про її велике відродження чи процвітання. Суверенітет, незалежність та територіальна цілісність є передумовою та основою виживання та розвитку країн, зокрема, народження сучасних національних держав ще більше затвердило основні норми міжнародних відносин, такі як національну рівність, суверенну незалежність, територіальну цілісність, невтручання у внутрішні справи [4].

Основою політичної безпеки є безпека режиму та системної безпеки. Органи національної безпеки завжди віддавали найвищий пріоритет підтримці політичної безпеки, приймаючи політичну безпеку як головний пріоритет. Зрозуміти природу політичної безпеки людей, це створити фундаментальну гарантію того, щоб люди могли жити та працювати у мирі та достатку. Підтримка політичної безпеки є фундаментальним інтересом усіх етнічних груп країни. Для цього корисним для нас є зарубіжний досвід забезпечення політичної безпеки.

Сьогодні штучний інтелект ставить нові виклики політичній безпеці. Технологічні зміни мають дві сторони. Штучний інтелект – це одночасно нова можливість та новий виклик для підтримки політичної безпеки. Одна

із проблем: популяризація та застосування технологій штучного інтелекту призвели до тенденції «децентралізації» політичної влади. У період розвитку штучного інтелекту дані уособлюють силу, суб'єктами, які контролюють дані, є органи державної влади, а також недержавні суб'єкти, такі як окремі особи, бізнес-групи та громадські організації. «Багатовузловий, безцентровий» дизайн структури «Інтернет-даних» визначає, що суб'єкти, які займають будь-яку позицію в онлайн-спільноті, не можуть мати більшого статусу, ніж суб'єкти, що займають інші позиції. Ця особливість послаблює традиційну офлайнову бюрократичну структуру національного управління та односторонню модель управління, а також владу політич- ного дискурсу.

Оскільки технології штучного інтелекту та монополія на дані продовжують розширюватись, то й розширення влади капіталу ставить під загрозу межі національної влади. Розвиток та зміни продуктивних сил неминуче спричинять коригування виробничих відносин, включаючи структуру політичної влади. Коли технологія штучного інтелекту широко використовуватиметься в різних економічних та соціальних галузях і викликатиме зміни, це сприятиме відповідним коригуванням структури національного управління та моделі розподілу влади [5].

З іншого боку, потужна стимулююча роль технологій штучного інтелекту та перспективи її економічного та соціального застосування призвели до перетікання в неї капіталу. В епоху штучного інтелекту гігантські компанії, що спираються на сильний капітал, поступово монополізують технології та контролюють дані. Технологія штучного інтелекту, а також дані та алгоритми, що лежать в її основі, тонко спрямовують громадську думку, впливаючи на політичні міркування та вибір людей та опосередковано контролюючи політичні тенденції. В епоху штучного інтелекту дані та алгоритми – це нова сила. Різні політичні операції, пов'язані з національними виборами в останні роки, показали, що наявність даних та технологій може певною мірою впливати на політичний порядок денний.

Технології штучного інтелекту можуть використовуватись політично ворожими силами для здійснення проникнення, підривної діяльності, диверсій та сепаратистської діяльності. Існує безліч прикладів використання передових технологій для загрози політичній безпеці інших країн. Після появи комп'ютерних мережевих технологій вони почали використовувати зловмисниками для реалізації кіберкрадіжки, кібератак, кіберзмови, поширення політичних чуток, ідеологічного проникнення і атак. В епоху штучного інтелекту наслідки атаки на систему штучного інтелекту країни або використання штучного інтелекту для здійснення проникнення, підривної, диверсійної та сепаратистської діяльності є серйознішими,

ніж раніше. Розвиток технологій штучного інтелекту створює серйозні проблеми участі суверенних країн у міжнародній конкуренції. Штучний інтелект в даний час є однією з передових технологій, а його основні технології в основному освоєні розвиненими країнами, такими як США та Європа. Ці країни використовують його для підвищення рівня автоматизації виробництва, підвищення продуктивності праці та прискорення переміщення обробних виробництв.

Необхідно підвищувати обізнаність про ризики, уважно стежити за розвитком технологій та програмами штучного інтелекту, регулярно вивчати та оцінювати політичні ризики, які може принести штучний інтелект, а також покращувати можливості виявлення, запо бігання та усунення ризиків [1].

Список використаних джерел:

1. Воронкова В. Г., Метеленко Н. Г., Ажажа М. А., Арабаджиєв Д. Ю., Нікітенко В. О., Дашков А. О., Венгер О. М., Фурсін О. О., Шарапова Т. А., Цикін Д. С. Інтеграція цифрових технологій в систему безпеки: адаптація до нових викликів і можливостей. *Цифрова трансформація промислового менеджменту у контексті викликів, можливостей та змін* : колективна монографія / за ред. д.філософ.н., проф. В. Г. Воронкової, д.е.н., проф. Н. Г. Метеленко. Львів – Торунь : Liha-Pres, 2024. 592 с.
2. Воронкова В. Г., Череп А. В,, Нікітенко В. О., Череп О. Г. Політика національної безпеки як чинник забезпечення стабільності та захисту інтересів держави. *Contemporary ukrainian science: theoretical and practical achievements* : collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California : GS Publishing Services, 2024. С. 40–55.
3. Теоретико-методичні основи забезпечення соціально-економічної безпеки економіки України в умовах діджиталізації бізнес-процесів : колективна монографія / А. В. Череп, В. Г. Воронкова, І. М. Дашко, Ю. О. Огренич, О. Г. Череп. Львів – Торунь : Liha-Pres, 2024. 202 с.
4. Череп А. В., Воронкова В. Г., Нікітенко В. О., Череп О. Г. Стратегії протидії кіберзагрозам як фактор забезпечення стійкості національної безпеки у цифрову епоху. *Modern science: multidisciplinary discourses* : collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman, Oaks, California : GS Publishing Services, 2024. С 56–74.
5. Череп А. В., Воронкова В. Г., Нікітенко В. О., Череп О. Г. Стратегії протидії кіберзагрозам як фактор забезпечення стійкості національної безпеки у цифрову епоху. *Modern science: multidisciplinary discourses* : collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman, Oaks, California : GS Publishing Services, 2024. 120 p. С. 56–74.

УДК 004:69.059.7:355.4

ВАРАВКА НАТАЛІЯ В'ЯЧЕСЛАВІВНА,
аспірантка другого курсу спеціальності 073 «Менеджмент»
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)

РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ СТІЙКОСТІ СОЦІАЛЬНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ ПІД ЧАС ВІЙНИ

У сучасному світі цифрові інструменти стали невід'ємною частиною соціальної інфраструктури, трансформуючи способи надання послуг, комунікації та організації суспільного життя. Ця інтеграція технологій створює нові можливості для розвитку та вдосконалення соціальних сервісів.

Війна, яка триває в Україні, поставила перед суспільством нові виклики. Соціальна інфраструктура, зокрема освіта, охорона здоров'я, соціальний захист, транспорт і комунікації, зазнала значних втрат, але водночас продемонструвала велику стійкість. В умовах кризи цифрові інструменти стали невід'ємною частиною підтримки та відновлення соціальної інфраструктури. Їхня роль полягає не лише в забезпеченні безперебійної роботи систем, але й у створенні нових можливостей для подолання наслідків війни.

Однією з основних функцій соціальної інфраструктури є надання послуг населенню, навіть у надзвичайних умовах. Цифрові платформи, такі як «Дія» та спеціалізовані системи електронного документообігу, дозволяють громадянам отримувати необхідні послуги дистанційно. Це включає реєстрацію переселенців, доступ до соціальних виплат, консультації з юридичних питань та отримання гуманітарної допомоги. Цифрові рішення також дозволяють державним органам ефективно управляти ресурсами, координувати дії на місцях і швидко реагувати на зміни в ситуації.

Війна змусила мільйони українських дітей і студентів перейти на дистанційне навчання. Цифрові інструменти, такі як платформи GoogleClassroom, Zoom та інші освітні сервіси, забезпечують безперервність навчального процесу. Вони не лише дозволяють учням здобувати знання, але й підтримують їхній моральний стан, створюючи відчуття стабільності. Адаптивні системи навчання з використанням штучного інтелекту допомагають враховувати індивідуальні потреби учнів і підвищувати ефективність засвоєння матеріалу.

В умовах обмеженого доступу до медичних закладів телемедицина стала важливим засобом надання медичної допомоги. Цифрові інструменти дозволяють лікарям консультувати пацієнтів дистанційно, а також слідкувати за станом здоров'я у реальному часі за допомогою мобільних додатків і спеціальних пристроїв. Крім того, цифрові платформи допомагають координувати розподіл гуманітарної медичної допомоги, забезпечуючи доступ до ліків і необхідного обладнання.

Цифрові інструменти активно використовуються для оцінки стану пошкодженої інфраструктури та планування її відновлення. Геоінформаційні системи (ГІС) та аналіз даних зі супутників дозволяють точно визначати масштаби руйнувань і пріоритезувати роботи з відновлення. Цифрові моделі допомагають прогнозувати потреби в ресурсах і визначати оптимальні шляхи для їх розподілу. Це дозволяє зменшити витрати часу та коштів на відновлення критичних об'єктів.

Соціальні мережі та цифрові платформи стали інструментами для підтримки соціальних зв'язків та комунікації. Вони дозволяють координувати дії волонтерів, об'єднувати громади та поширювати важливу інформацію серед населення. Також цифрові інструменти забезпечують зворотний зв'язок між владою та громадянами, що сприяє кращому розумінню потреб суспільства і швидкому реагуванню на них.

В умовах постійних атак, переміщення населення та руйнування критичних об'єктів, одним із рішень потреби в інноваційних підходах до управління соціальною інфраструктурою стало застосування штучного інтелекту (ШІ), що дозволяє оперативно адаптуватися до змін, забезпечуючи стійкість і розвиток критичних систем. Одним із ключових напрямів використання ШІ є управління гуманітарною допомогою. Завдяки аналізу великих обсягів даних можна точно визначити, де і коли потрібна допомога. ШІ допомагає ефективно реєструвати внутрішньо переміщених осіб (ВПО), обробляти їхні запити на житло, роботу та соціальні виплати. За допомогою спеціалізованих платформ з використанням алгоритмів машинного навчання можна аналізувати потреби кожного переселенця та пропонувати персоналізовані рішення. Це значно знижує навантаження на органи соціального захисту і підвищує якість обслуговування. Система охорони здоров'я в умовах війни зазнала значних втрат. ШІ допомагає оптимізувати управління медичними ресурсами. Наприклад, алгоритми можуть прогнозувати потребу в медикаментах, ліжках у лікарнях або навіть розробляти маршрути для евакуації поранених. Штучний інтелект підтримує розвиток дистанційної освіти. Платформи з адаптивним навчанням, які використовують ШІ, дозволяють дітям, навіть у зонах бойових дій, отримувати якісну освіту. Вони підлаштовуються під індивідуальні

потреби учнів, забезпечуючи їхню активну участь у навчальному процесі. Після завершення активних бойових дій Україна зіткнеться з завданням відновлення зруйнованої інфраструктури. ШІ може допомогти у плануванні реконструкції. Алгоритми аналізують стан зруйнованих об'єктів і пропонують найбільш ефективні стратегії їх відновлення. Крім того, вони сприяють оптимальному розподілу фінансових і матеріальних ресурсів. В умовах війни виникають нові ризики, які потребують оперативного реагування. ШІ здатний прогнозувати можливі сценарії розвитку подій на основі аналізу даних, що дозволяє вчасно вжити заходів для зниження ризиків. Це особливо важливо для забезпечення безперервності роботи критичних об'єктів соціальної інфраструктури.

На сьогоднішній день соціальна інфраструктура України стикається з необхідністю швидкого прийняття рішень. Використання технологій BigData стає ключовим інструментом для подолання цих завдань, забезпечуючи оперативність, точність та ефективність у процесах планування та управління. Переваги використання BigData в швидкості прийняття рішень (обробка великих обсягів даних у режимі реального часу дозволяє швидко адаптуватися до змінюваних обставин), прозорості і підзвітності (завдяки відкритим даним забезпечується прозорість процесів розподілу ресурсів, що знижує ризики корупції та нецільового використання коштів) та прогнозуванні і плануванні (BigData дозволяє моделювати можливі сценарії розвитку подій, що сприяє ефективному стратегічному плануванню). Необхідно зауважити, що є ряд викликів, які треба враховувати при використанні BigData в умовах війни. По-перше, це доступ до даних, тому що у воєнний час збір даних може бути обмежений через руйнування інфраструктури або відсутність доступу до окремих регіонів. По-друге, – забезпечення безпеки даних: питання кібербезпеки стає надзвичайно важливим, оскільки дані можуть стати об'єктом атак з боку ворога. Крім того, необхідно враховувати недостатній рівень цифрової грамотності, що потребує навчання спеціалістів та користувачів для ефективного використання BigData. Після завершення війни технології BigData матимуть одне з вирішальних значень для відбудови країни. Вони сприятимуть інтеграції відновлених об'єктів у єдину цифрову систему, що дозволить забезпечити їхню ефективну експлуатацію. Крім того, використання даних для аналізу демографічних змін та економічних тенденцій допоможе формувати довгострокові стратегії розвитку соціальної інфраструктури.

Список використаних джерел:

1. Біла книга з регулювання ШІ в Україні. Червень 2024 р. *Міністерство цифрової трансформації України.*

2. Матеріали VIII Міжнародної науково-практичної конференції «Управління розвитком соціально-економічної системи» 21–24 березня 2024 р. м. Харків. Міністерство освіти і науки України ; Державний біотехнологічний університет.

3. Кравчина О. Є. «Методики оцінки ефективності використання цифрових інструментів у навчальному процесі. *Інформаційний бюлетень.* 2024. № 6. Інститут цифровізації освіти НАПН України.

4. Порохова О. Є. Сутність і проблематика штучного інтелекту в управлінні проектами [Електронний ресурс]. 2020 р. Одеський національний університет імені І. І. Мечникова. URL: http://dspace.onua.edu.ua/ bitstream/handle/11300/15083/Порохова%20О.%20Є.%20Сутність%20і%20проблематика%20штучного%20інтелекту.pdf?sequence=1&isAllowed=y

5. Національний інститут стратегічних досліджень «Цифрова трансформація економіки України в умовах війни». Жовтень 2024 року.

6. Міністерство цифрової трансформації України (2023). «Дія: досвід цифровізації державних послуг в умовах воєнного стану».

7. UNDP Ukraine (2023). "Digital Solutions for Social Infrastructure Recovery in Ukraine".

8. World Bank Group (2023). "Ukraine: Digital Transformation for Social Resilience During Crisis".

9. Закон України «Про цифрові інновації в соціальній сфері» (2023).

10. Постанова КМУ «Про затвердження Порядку використання цифрових інструментів у соціальній інфраструктурі в умовах воєнного стану» (2023).

11. Портал *Дія*. URL: diia.gov.ua

12. Єдиний портал державних послуг України. URL: guide.diia.gov.ua

13. Ukraine Digital Transformation Report Portal. URL: ukraine.ua/invest-trade/digitalization

УДК 331.108:005.7

ГОРОШКО СЕРГІЙ ОЛЕКСАНДРОВИЧ,
магістрант спеціальності 073 «Менеджмент»
Запорізький національний університет (м. Запоріжжя, Україна)

ЕФЕКТИВНЕ УПРАВЛІННЯ ПЕРСОНАЛОМ У ПЕРІОДИ ЗМІН І ВИКЛИКІВ

Управління персоналом в умовах кризи вимагає стратегічного підходу, який враховує не тільки економічні й організаційні аспекти, а й людський фактор. Кризові ситуації можуть бути викликані економічними спадами, пандеміями, соціально-політичними змінами чи іншими форс-мажорними

обставинами. У таких умовах компанії повинні зосередитися на підтримці стабільності, ефективності та згуртованості команди.

Серед основних аспектів управління персоналом в умовах кризи зазначимо наступні:

1. Чітка та прозора комунікація

Криза часто супроводжується підвищеною тривожністю та невизначеністю. Для зменшення негативного впливу важливо забезпечити регулярне інформування співробітників про стан справ у компанії, її стратегічні плани та очікування від команди. Керівники повинні надавати чіткі відповіді на запитання, пояснювати рішення та бути відкритими до зворотного зв'язку. Використання цифрових платформ для комунікації, таких як корпоративні портали чи месенджери, допоможе підтримувати зв'язок навіть у дистанційному форматі роботи.

2. Психологічна підтримка

Під час кризи працівники можуть переживати підвищений стрес, страх втрати роботи чи зниження доходів. Організація має подбати про створення комфортного емоційного середовища. Це може включати доступ до консультацій психологів, організацію тренінгів з управління стресом, підтримку ментального здоров'я через програми корпоративного благополуччя.

3. Оптимізація робочих процесів

Криза вимагає швидкого перегляду існуючих процесів та пріоритетів. Варто визначити найважливіші завдання та сконцентрувати ресурси на їх виконанні. Використання цифрових інструментів для автоматизації, розробка гнучких графіків роботи та впровадження віддалених форматів можуть значно підвищити ефективність і знизити витрати. Лідери повинні демонструвати високий рівень емпатії та підтримки. Уміння вислухати, зрозуміти проблеми співробітників та запропонувати конкретні рішення зміцнюють довіру до керівника. Якщо організація може уникнути звільнень, вона повинна забезпечити стабільну оплату праці. У випадках неминучого скорочення важливо вести відкритий діалог, пропонувати компенсаційні пакети чи допомогу в працевлаштуванні.Управління персоналом в умовах кризи є багатогранним завданням, яке вимагає поєднання стратегічного планування, лідерства, технологічних інновацій та підтримки команди. Успіх у подоланні кризових ситуацій значною мірою залежить від того, наскільки організація зуміє зберегти свою команду мотивованою, згуртованою та готовою до адаптації. В умовах кризи надзвичайно важливо зберігати моральний дух та продуктивність команди. Це можна досягти за допомогою декількох ключових заходів, а саме:

• Програми визнання досягнень. Навіть найменші успіхи варто публічно відзначати. Просте «дякую» або символічна нагорода можуть

значно підвищити рівень залученості та мотивації співробітників. Важливо створювати атмосферу, де кожен відчуває себе цінним.

• Забезпечення можливостей для професійного розвитку. Організація навчальних курсів, тренінгів чи семінарів не лише підвищує компетентність команди, але й додає впевненості у професійних перспективах. Співробітники повинні розуміти, що їх розвиток є пріоритетом навіть у складні часи.

• Справедливий розподіл навантаження. Нерівномірне розподілення завдань може спричинити вигорання, особливо під час стресових ситуацій. Чітке планування та розподіл обов'язків дозволяють уникнути перевантаження та створюють відчуття командної підтримки.

У кризових умовах головними викликами для організації стають підтримка мотивації персоналу, швидка адаптація до змін та забезпечення безперебійної роботи. Успішна реалізація цих завдань можлива лише за умови комплексного підходу, який включає стратегічне планування, впровадження сучасних технологій і турботу про команду. Публічне визнання досягнень співробітників, створення можливостей для професійного розвитку, справедливий розподіл навантаження, а також технологічна підтримка сприяють збереженню високого морального духу навіть у складні часи. Гнучкість і здатність швидко змінювати стратегії відповідно до поточних умов дозволяють організації не лише реагувати на кризу, але й знаходити в ній можливості для зростання. Водночас використання технологічних рішень забезпечує стабільність і підвищує ефективність процесів.

Отже, об'єднання людського потенціалу, інноваційних підходів і стратегічного бачення є ключем до успіху в подоланні кризових викликів та забезпеченні стабільного майбутнього компанії.

Список використаних джерел:

1. Воронкова В. Г. Цифровий менеджмент як чинник як чинник ефективного управління сучасними організаціями. *Геостратегічні трансформації та траєкторія національної безпеки в контексті відбудови і сталого розвитку України* : матеріали Міжнародної науково-практичної конференції (25–26 травня 2023 року, м. Запоріжжя) / наук. ред. Н. Г. Метеленко ; Інженерний навчально-науковий інститут ім. Ю. М. Потебні Запорізького національного університету. Одеса : Олді+, 2023. С. 266–270.

2. Воронкова В. Г., Нікітенко В. О. Філософія цифрової людини і цифрового суспільства: теорія і практика : монографія. Львів – Торунь : Liha-Pres, 2022. 460 с. *Цифрова трансформація промислового менеджменту: теорія і практика* : монографія / за ред. д.філософ.н., проф. В. Г. Воронкової, д.е.н., проф. Н. Г. Метеленко. Львів – Торунь : Liha-Pres, 2023. 816 с.

3. Цифрова трансформація промислового менеджменту у контексті викликів, можливостей та змін : колективна монографія / за ред. д.філософ.н., проф. В. Г. Воронкової, д.е.н., проф. Н. Г. Метеленко. Львів – Торунь : Liha-Pres, 2024. 592 с.

УДК 331

ДАШКОВ АРТУР ОЛЕКСАНДРОВИЧ,
здобувач третього рівня вищої освіти ступеня доктора філософії
Запорізький національний університет (м. Запоріжжя, Україна)

МЕНЬШИКОВ МИКИТА СЕРГІЙОВИЧ,
магістрант спеціальності 281 «Публічне управління та адміністрування»
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)

АЖАЖА МАРИНА АНДРІЇВНА,
д.н.держ.упр., проф. кафедри управління та адміністрування
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
ORCID ID: https://orcid.org/0000-0003-3549-7718

ІНТЕГРАЦІЯ ПІДПРИЄМНИЦТВА І МАРКЕТИНГУ В МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Підприємництво відіграє ключову роль у зміцненні економічної незалежності та стійкості держави, оскільки воно забезпечує розвиток національної економіки, створення робочих місць, залучення інвестицій та підвищення конкурентоспроможності на міжнародному рівні. Проаналізуємо кілька способів, як підприємництво сприяє цьому процесу:

1. Створення робочих місць та зниження безробіття:

– підприємництво створює нові можливості для працевлаштування, що безпосередньо впливає на зниження рівня безробіття та покращення соціальної стабільності;

– підприємці часто стимулюють розвиток нових секторів економіки, що допомагає не тільки створювати нові робочі місця, а й диверсифікувати економіку країни, роблячи її менш залежною від зовнішніх факторів.

2. Підвищення конкурентоспроможності та інноваційність:

– підприємці стимулюють розвиток нових технологій, що підвищує конкурентоспроможність країни; власники бізнесу часто впроваджують інновації в процеси виробництва, обслуговування та управління, що дозволяє знизити витрати та підвищити ефективність;

– активне підприємництво сприяє розвитку конкуренції, що стимулює підприємства підвищувати якість товарів та послуг, веде до розвитку економічної структури, зміцнення позицій на міжнародному ринку та залучення іноземних інвестицій.

3. Розвиток внутрішнього ринку та скорочення залежності від зовнішніх факторів:

– підприємницька діяльність стимулює інвестиції як з боку національних, так і з боку іноземних інвесторів, що сприяє економічному зростанню, покращенню фінансової стабільності держави і зменшенню залежності від зовнішніх кредиторів або ресурсів;

– диверсифікація економіки: підприємництво сприяє розвитку нових галузей і секторів, що допомагає знизити залежність економіки від однієї галузі (наприклад, від експорту природних ресурсів), що робить країну більш стійкою до коливань світових ринків.

4. Стимулювання внутрішнього споживчого попиту:

– підприємництво стимулює внутрішній попит на продукти та послуги, що є важливим фактором для підтримки економічної стабільності та зростання; бізнеси створюють нові продукти, послуги та моделі бізнесу, що зменшує необхідність імпорту;

– активне підприємництво забезпечує збільшення податкових надходжень до державного бюджету, що дозволяє уряду мати більше ресурсів для фінансування соціальних програм, інфраструктурних проектів та інших важливих ініціатив, що зміцнюють національну стабільність.

5. Підвищення економічної стійкості через диверсифікацію ресурсів:

– підприємництво сприяє створенню різноманітних бізнес-моделей, що зменшує економічну уразливість від зовнішніх шоків (економічних криз, зміни цін на ресурси тощо); диверсифікація ресурсів та виробництва дозволяє державі підтримувати стабільність навіть у разі негативних змін на зовнішньому ринку;

– завдяки підприємництву країна здатна швидше адаптуватися до змін на глобальному ринку, таких як зміна попиту, технологічні інновації або глобальні економічні кризи.

6. Розвиток інфраструктури та покращення соціальних умов:

– підприємці, особливо в нових галузях (наприклад, IT, зелені технології), стимулюють розвиток інфраструктури, що підвищує якість життя громадян і робить економіку більш стійкою;

– підприємницька активність забезпечує фінансування різних соціальних проектів, що сприяє загальному підвищенню рівня життя, покращенню доступу до освіти та охорони здоров'я.

7. Підвищення національної безпеки через економічну незалежність:

– підприємства, що працюють у галузях енергетики та ресурсів, можуть сприяти зниженню залежності країни від імпорту енергоносіїв, що є важливим чинником для забезпечення національної безпеки;

– підприємництво сприяє розвитку національних інфраструктур і технологій, що можуть бути критично важливими для безпеки держави, зокрема в умовах глобальних загроз (наприклад, кібербезпека, охорона здоров'я, наука і технології).

8. Підвищення стійкості до глобальних економічних і політичних загроз:

– підприємництво створює нові можливості для розвитку зовнішньої торгівлі та економічних зв'язків, що дозволяє країні не лише зберігати свою економічну незалежність, а й зміцнювати позиції на міжнародній арені;

– активне підприємництво дозволяє країні швидше адаптуватися до змін у міжнародній політиці та економіці, що підвищує її стійкість до кризових ситуацій.

Підприємництво є основою для формування економічної незалежності та стійкості держави, оскільки воно сприяє створенню робочих місць, розвитку інновацій, диверсифікації економіки та збільшенню фінансової стабільності. Активний підприємницький сектор допомагає країні знижувати залежність від зовнішніх факторів, підвищує конкурентоспроможність і забезпечує її економічну безпеку в умовах глобальних викликів.

Маркетинг відіграє ключову роль у формуванні позитивного іміджу країни та мобілізації суспільства, оскільки він допомагає створювати стратегії комунікації, які сприяють зміцненню репутації, залученню інвестицій, розвитку зовнішніх економічних відносин і підтримці національного духу (табл. 1).

Таким чином, маркетинг відіграє важливу роль у формуванні позитивного іміджу країни та мобілізації суспільства. Він не тільки сприяє залученню інвестицій та розвитку економіки, а й підтримує національну єдність, підвищує патріотизм і громадську свідомість, а також допомагає просувати країну на міжнародній арені. Використання маркетингових стратегій дозволяє країнам ефективно реагувати на виклики глобалізації та зміцнювати внутрішню стабільність.

Таблиця 1 – **Показники для вимірювання ролі маркетингу у формуванні позитивного іміджу країни та мобілізації суспільства**

Показники	Індикатори	Опис
1	2	3
1. Формування національного бренду та іміджу країни	1.1. Створення позитивного образу на міжнародній арені	1.1.1. Маркетинг сприяє створенню і просуванню бренду країни на міжнародному рівні, який має привертати інтерес інвесторів, туристів, а також сприяти покращенню іміджу на глобальній арені. 1.1.2. Маркетинг активно використовує концепцію «м'якої сили», яка полягає у впливі через культуру, цінності та ідеї, що приваблюють інші країни та міжнародну спільноту, сприяючи національній стабільності та розвитку.
	1.2. Політика іміджевого маркетингу	1.2.1. За допомогою маркетингових стратегій країна може активно позиціонувати себе як лідера в певних сферах (економіка, культура, інновації), що дозволяє покращити її статус на міжнародній арені. 1.2.2. Важливу роль відіграє маркетинг у формуванні інформаційної політики країни через медіа, соціальні мережі, інтерв'ю з міжнародними лідерами, що дозволяє донести до світової аудиторії позитивні риси країни
2. Мобілізація суспільства та формування громадянської свідомості	2.1. Виховання національної гордості та патріотизму	2.1.1. Маркетинг допомагає формувати у громадян національну гордість, підвищувати рівень патріотизму та стимулювати до активної участі в громадському житті через позитивні кампанії, що демонструють досягнення країни та важливість єдності. 2.1.2. Маркетингові стратегії можуть включати кампанії, що акцентують увагу на соціальних ініціативах, волонтерстві, збереженні культурної спадщини або екологічних питаннях.
	2.2. Просування державних ініціатив та реформ	2.2.1. Маркетинг активно використовує комунікаційні стратегії для популяризації соціальних, економічних чи політичних ініціатив уряду. 2.2.2. За допомогою маркетингових інструментів можна залучити громадян до участі в місцевих ініціативах, розвитку інфраструктури або підтримці громадських організацій, що зміцнюють соціальний капітал

Продовження таблиці 1

1	2	3
3. Залучення інвестицій та підтримка економічного зростання	3.1. Формування позитивного інвестиційного клімату	3.1.1. Маркетинг активно сприяє створенню сприятливого інвестиційного клімату, залучаючи інвесторів через кампанії, які підкреслюють стабільність економіки, вигідне географічне положення, розвиток інфраструктури та перспективи для бізнесу в країні. 3.1.2. Підтримка бізнесу, особливо малого та середнього, через маркетингові інструменти та державну підтримку стимулює зростання економіки та мобілізує підприємців до інвестицій у національний розвиток
	3.2. Залучення туристів	3.2.1. Позитивний імідж країни, побудований за допомогою маркетингу, дозволяє значно підвищити туристичну привабливість.
4. Підвищення національної єдності та підтримка внутрішнього розвитку	4.1. Підвищення довіри до інститутів влади	4.1.1. За допомогою маркетингових кампаній можна підвищити прозорість дій уряду, залучити населення до участі в обговореннях важливих політичних рішень, таким чином зміцнюючи довіру до державних інститутів і забезпечуючи стабільність. 4.1.2. Використання маркетингових кампаній для підкреслення важливості єдності нації, співпраці між різними соціальними групами сприяє згуртованості суспільства в умовах внутрішніх і зовнішніх викликів
	4.2. Адаптація до глобальних змін	4.2.1. В умовах глобальних викликів маркетинг допомагає державі адаптуватися до змін у зовнішньому середовищі, наприклад, через адаптацію до нових технологій, зміну глобальних економічних тенденцій, або кризових ситуацій. 4.2.2. Маркетингові кампанії допомагають мобілізувати ресурси для розвитку певних сфер (освіта, охорона здоров'я, екологія), акцентуючи на важливості цих сфер для національної безпеки та процвітання

Сучасний світ стикається з численними глобальними викликами, такими як економічні кризи, війна, зміни клімату, пандемії, технологічні революції та геополітичні нестабільності. У цих умовах підприємницькі інновації та маркетингові технології відіграють важливу роль у забезпеченні гнучкості та

конкурентоспроможності підприємств. Вони адаптуються до нових реалій, забезпечуючи стійкість бізнесу та можливості для зростання.

Підприємницькі інновації та маркетингові технології швидко адаптуються до сучасних глобальних викликів через використання новітніх технологій, інноваційних бізнес-моделей та гнучких маркетингових стратегій. Завдяки цьому підприємства можуть не тільки ефективно реагувати на зміни у глобальній економіці та соціумі, але й забезпечувати своє виживання та зростання в умовах глобальних криз, економічної нестабільності та швидких технологічних змін.

Підприємницькі інновації і маркетингові технології мають різні сфери застосування і підходи до адаптації в умовах сучасних глобальних викликів:

– підприємницькі інновації спрямовані на поліпшення внутрішніх процесів, зниження витрат, розвиток нових продуктів і технологій, що дозволяють бізнесам бути більш гнучкими та конкурентоспроможними.

– маркетингові технології орієнтовані на зовнішні ринки та ефективне спілкування з клієнтами, використовуючи новітні цифрові інструменти, що дозволяють брендам бути ближчими до своїх споживачів і ефективно реагувати на зміни в попиті та поведінці аудиторії.

Обидва аспекти є важливими для адаптації до глобальних викликів, однак їх інструменти та фокуси суттєво відрізняються, що дозволяє підприємствам успішно працювати в умовах непередбачуваних змін.

Список використаних джерел:

1. Більовська О., Майстро Р. Особливості підприємницької діяльності в умовах воєнного стану в Україні. *Вісник Національного технічногоуніверситету «Харківський політехнічний інститут». Економічні науки.* 2023. № 2. С. 50–54. DOI: https://doi.org/10.20998/2519-4461.2023.2.50.

2. Васюта В., Чорновол Н., Горбунова М. Роль підприємницької діяльності в розвитку національної економіки. *Галицький економічний вісник.* 2022. Вип. 78–79. № 5–6. С. 130–137. URL: https://doi.org/10.33108/galicianvisnyk_tntu2022.05_06.130

3. Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення : монографія / Криштанович М. Ф., Пушак Я. Я., Флейчук М. І., Франчук В. І. Львів : Сполом, 2020. 418 с.

4. Мозговий Є. В. Державна підтримка підприємців під час війни. *Бізнес Інформ*. 2024. № 6. С. 202–207. DOI: https://doi.org/10.32983/2222-4459-2024-6-202-207

5. Москаленко О. Як пост-пандемічна економіка трансформується в повоєнну в Україні: виклики для економічної політики та суспільства? *Bezpieczny Bank.* 2022. № 86(1). С. 9–32. DOI: https://doi.org/10.26354/bb.1.1.86.2022.

6. Мурована Т. О. Вітчизняне підприємництво в умовах воєнного стану: основні тенденції та методи підтримки. *Економіка та суспільство.* 2023. Вип. 47. DOI: https://doi.org/10.32782/2524-0072/2023-47-49.

УДК 339.5:339.9

ДУЮН ОЛЕСЯ ДМИТРІВНА,
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: olesiaduyun@gmail.com

ГОЛОМБ ВІКТОРІЯ ВОЛОДИМИРІВНА,
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: viktoria.golomb@gmail.com
ORCID ID: https://orcid.org/0000-0003-4053-9310

СУЧАСНИЙ СТАН ЗОВНІШНЬОЇ ТОРГІВЛІ УКРАЇНИ

Міжнародна торгівля є ключовим компонентом сучасної світової економіки, і для України її значення важко переоцінити. Розташована на перехресті торговельних шляхів, країна має значний потенціал для розвитку зовнішньоекономічних зв'язків. Однак сучасний стан української торгівлі залишається складним, зумовленим низкою внутрішніх та зовнішніх чинників. Після здобуття незалежності Україна зіткнулася з необхідністю переорієнтації економіки на ринкові засади та інтеграції у глобальну економіку. Перехід супроводжувався складнощами, пов'язаними з розпадом радянських економічних зв'язків, переходом до ринкових механізмів ціноутворення та адаптацією до нових умов міжнародної торгівлі.

Розглянемо динаміку зовнішньої торгівлі України з 2005 по 2023 роки (рис. 1).

На рисунку представлено динаміку зовнішньої торгівлі України, що демонструє циклічні зміни, обумовлені як внутрішніми, так і зовнішніми факторами.

На початку аналізованого періоду, обсяги експорту становили близько 32 млрд доларів США, а імпорту – 34 млрд доларів. Потрібно зазначити, що протягом всього періоду в Україні спостерігається негативне сальдо зовнішньої торгівлі, тобто імпорт переважає над експортом. До 2008 року показники зовнішньоторговельної діяльності подвоїлися: експорт зріс до 63 млрд доларів (+100 %), імпорт – до 80 млрд доларів (+100 %). Така динаміка пояснюється активним зростанням глобальної економіки та високим попитом на українську продукцію. У 2009 році внаслідок світової фінансової кризи обсяги торгівлі суттєво знизилися. Це було обумовлено зменшенням зовнішнього попиту на українські товари, особливо в сировинних галузях.

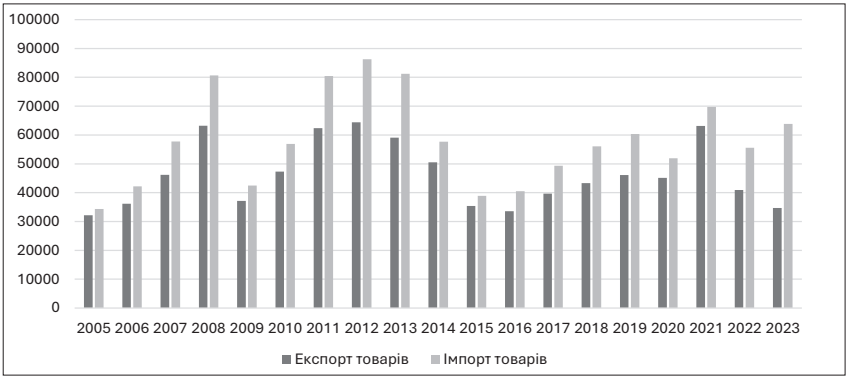

Рис. 1. Динаміка зовнішньої торгівлі України [1]

Період 2010–2013 років характеризувався відносною стабільністю. У 2012 році обсяги експорту досягли рекордного значення – 64 млрд доларів, імпорту – 86 млрд доларів. Така ситуація пояснюється стабільністю внутрішнього виробництва та активністю міжнародної торгівлі.

Протягом наступних 2014–2016 років відбувалося істотне скорочення обсягів зовнішньої торгівлі. У 2016 році експорт зменшився до 33 млрд доларів, а імпорт – до 40 млрд доларів. Основними чинниками стали анексія Криму, військовий конфлікт та економічна рецесія.

Поступове відновлення зовнішньої торгівлі спостерігалося у 2017–2021 роках, що свідчить про адаптацію економіки до нових умов, стабілізацію внутрішнього виробництва та розвиток зовнішніх ринків.

Війна у 2022 році мала катастрофічний вплив на зовнішню торгівлю України. Обсяг експорту впав до 34 млрд доларів (падіння на 50 % порівняно з 2021 роком), а імпорту – до 55 млрд доларів. Причинами стали зруйнована інфраструктура, втрати виробничих потужностей та ускладнення логістичних маршрутів.

За даними Державної служби статистики, експорт товарів з України скоротився на 18 % до 2022 року, тоді як імпорт в Україну навпаки зріс майже на 15 %. У результаті негативне зовнішньоторговельне сальдо досягло $27,4 млрд.

Структура експорту України демонструє суттєву залежність від сировинних та низькотехнологічних товарів. Основу експортного потенціалу становлять продовольчі товари (63 %) та мінеральні продукти, що підкреслює важливість сільського господарства та природних ресурсів у зовнішньоекономічній діяльності. Насамперед це продукція сільського

господарства (зернові культури, тваринні та рослинні жири, харчові продукти), мінеральна продукція (до цієї групи входять руди, сірка, крейда, вапняк, цемент), деревина, продукція хімічної промисловості, а також різні промислові товари (до них належать товари домашнього вжитку, дитячі іграшки, спортивний інвентар). Серед імпорту товарів ключову роль займає група – машини, устаткування, транспортні засоби та прилади (31 %), а також мінеральні продукти (16 %).

Основний обсяг зовнішньої торгівлі України припадає на Євросоюз. Країни ЄС у 2023 році купили 65 % українського експорту (23,2 млрд доларів), а імпорт із ЄС становив 51 % (32,6 млрд доларів). Частка країн СНД в експорті становила лише 4 % ($1,6 млрд), частка СНД в імпорті – 2 % (1,2 млрд доларів). Ще 31 % українського експорту ($11,1 млрд) припадає на інші регіони, як-от: США, Канада, країни Азії та Африки. Імпорт в Україну із цих держав у 2023 році досяг 47 % (30 млрд доларів) [2].

Сучасний стан міжнародної торгівлі в Україні характеризується значними викликами через війну та економічну нестабільність.

Український експорт залишається переважно сировинно орієнтованим, що робить економіку вразливою до коливань світових цін. Зерно, металургійна продукція та енергетичні ресурси становлять основну частину експорту, що обмежує можливості для отримання високих прибутків. Низька додана вартість продукції є серйозною перешкодою для довгострокового економічного зростання [3].

Недостатня розвиненість транспортної інфраструктури, зокрема залізничної та портової, ускладнює доставку українських товарів на світові ринки. Логістичні проблеми посилюються через руйнування інфраструктури внаслідок військових дій.

Багато українських підприємств потребують модернізації та впровадження інноваційних технологій для підвищення конкурентоспроможності. Це є важливим завданням для стимулювання експорту продукції з вищою доданою вартістю [4].

Однак, існують можливості для відновлення і розвитку зовнішньоекономічних зв'язків. Завдяки підтримці міжнародних партнерів і внутрішнім реформам Україна має шанс відновити свою позицію на світовій арені торгівлі та підвищити конкурентоспроможність своєї продукції. Для покращення ситуації в міжнародній торгівлі Україні необхідно запровадити цілісну державну підтримку при формуванні міжнародних відносин. Це включає вдосконалення потенційних переваг українського виробництва, розвиток інноваційної бази та стимулювання переробних галузей.

Список використаних джерел:

1. Державна служба статистики України. URL: https://www.ukrstat.gov.ua/ (дата звернення: 15.11.2024).
2. Redko K. Yu., Tkachenko I. O. Analysis of the structure of the international trade between Ukraine and the EU. *Економічний вісник НТУУ «КПІ».* 2021. № 18. URL: http://ev.fmm.kpi.ua/article/view/231178 (дата звернення: 01.11.2024).
3. Гаврилюк І. І. Розвиток міжнародної торгівлі в системі міжнародних економічних відносин в Україні. *Економіка та суспільство*. 2022. Вип. 45. С. 15–19.
4. Шамборовський Г. О. Сучасний стан та перспективи зовнішньої торгівлі України. *АГРОСВІТ.* 2024. № 9. С. 28–34.

УДК 004.942:658.5

КЛОПОВ ІВАН ОЛЕКСАНДРОВИЧ,
Запорізький національний університет (м. Запоріжжя, Україна)
E-mail: uaklopov@gmail.com
ORCID ID: https://orcid.org/0000-0002-2199-2462

АЛЕНІЧЕВ В'ЯЧЕСЛАВ ЄВГЕНІЙОВИЧ,
Запорізький національний університет (м. Запоріжжя, Україна)

СОЛДАТОВА ЄЛИЗАВЕТА ОЛЕКСАНДРІВНА,
Запорізький національний університет (м. Запоріжжя, Україна)

ЦИФРОВІ ДВІЙНИКИ В ПРОМИСЛОВОСТІ: ІННОВАЦІЙНІ ПІДХОДИ ДО ОПТИМІЗАЦІЇ ВИРОБНИЧИХ ПРОЦЕСІВ

Цифрові двійники – це інноваційна технологія, що швидко завойовує провідні позиції в сучасній промисловості. Цей концепт поєднує віртуальну модель фізичного об'єкта чи процесу з можливістю їхнього інтерактивного аналізу у реальному часі. Завдяки інтеграції технологій штучного інтелекту, Інтернету речей (IoT) та великих даних, цифрові двійники стають незамінним інструментом для підприємств, які прагнуть оптимізувати свої виробничі процеси. У той час як традиційні підходи до виробництва зосереджуються на фізичних системах, цифрові двійники дозволяють спрогнозувати їхню поведінку, виявити потенційні проблеми та випробувати нові рішення ще до їхнього впровадження.

Сучасна промисловість стикається з викликами, такими як необхідність зниження витрат, підвищення якості продукції та забезпечення гнучкості у відповідь на змінні ринкові умови. Цифрові двійники пропонують ефективні способи розв'язання цих проблем шляхом впровадження віртуальних симуляцій і точного моніторингу в реальному часі.

Основою для цифрових двійників є інтеграція фізичних і віртуальних систем через датчики, моделі та аналітику, що дозволяє ефективно імітувати поведінку фізичних об'єктів на всіх етапах їхнього життєвого циклу [1].

Однією з ключових характеристик цифрових двійників є їхня здатність до інтеграції з новітніми технологіями, такими як Інтернет речей (IoT), машинне навчання і великі дані, що дозволяє їм не лише відображати поточний стан системи, але й прогнозувати майбутні сценарії. Наприклад, дослідники пропонують використовувати ймовірнісні графічні моделі для формалізації взаємодії між фізичними та віртуальними компонентами, що робить створення цифрових двійників масштабованим і більш точним [4].

Для забезпечення ефективного впровадження цифрових двійників важливо розробити чіткі концептуальні рамки та стандарти. Наприклад, дослідження показують, що структуровані підходи до створення цифрових двійників, такі як використання систематизованих характеристик і функцій, дозволяють уніфікувати процеси розробки і забезпечити більшу ефективність у різних галузях промисловості [3].

Цифрові двійники знайшли широке застосування в різних галузях промисловості завдяки їхній здатності моделювати фізичні процеси та аналізувати дані в реальному часі. У виробництві вони допомагають оптимізувати процеси шляхом моделювання ланцюгів постачання, прогнозування несправностей обладнання та забезпечення безперервності операцій. Наприклад, у будівництві цифрові двійники використовуються для моделювання будівельних конструкцій та управління їхнім життєвим циклом, об'єднуючи статичну та динамічну інформацію в єдину інтерактивну платформу [6].

В енергетиці цифрові двійники сприяють підвищенню ефективності використання ресурсів та забезпечують підтримку рішень щодо оптимізації роботи мереж. Наприклад, використання цифрових двійників у відновлювальних джерелах енергії дозволяє відстежувати стан вітрових турбін та прогнозувати їх продуктивність, що забезпечує більш раціональне використання обладнання [2].

У машинобудуванні цифрові двійники дозволяють моделювати поведінку складних технічних систем, таких як двигуни, з метою їхнього вдосконалення. Цей підхід використовує симуляційні та фізичні моделі, доповнені аналізом великих даних, для виявлення можливих проблем ще на етапі проектування, що значно знижує витрати на розробку і експлуатацію [4].

Автомобільна промисловість активно використовує цифрові двійники для підвищення якості продукції та скорочення термінів розробки нових моделей. Наприклад, технологія цифрових двійників використовується для тестування аеродинамічних властивостей автомобілів у віртуальному середовищі, що дозволяє уникнути дорогих фізичних експериментів і прискорити процес проектування [3].

Цифрові двійники суттєво змінюють підхід до управління виробничими процесами, забезпечуючи більш ефективне планування і прогнозування. Однією з ключових переваг є можливість моделювати виробничі лінії у віртуальному середовищі, що дозволяє визначати оптимальні сценарії роботи, мінімізувати збої та збільшувати продуктивність. Наприклад, використання цифрових двійників у прогнозуванні технічного стану обладнання знижує ймовірність поломок і простоїв, що підвищує загальну ефективність виробництва [1].

Друга ключова перевага – це покращення моніторингу і управління якістю продукції. Завдяки інтеграції з Інтернетом речей (IoT) та штучним інтелектом цифрові двійники дозволяють у реальному часі відслідковувати показники якості та автоматично виявляти дефекти. Це не лише забезпечує більш високий рівень якості, але й знижує витрати на контроль та усунення дефектів у готовій продукції [5].

Цифрові двійники також відіграють важливу роль в оптимізації логістики та управління ланцюгами постачання. Наприклад, вони дозволяють моделювати і прогнозувати можливі затримки або збої в постачаннях, а також розробляти ефективніші маршрути транспортування. Це особливо важливо у складних виробничих системах, де навіть незначні затримки можуть мати значний вплив на продуктивність [4]. Окрім оптимізації виробничих процесів, цифрові двійники сприяють покращенню адаптивності підприємств до змін ринку. Можливість швидкого тестування нових сценаріїв і моделей у віртуальному середовищі дозволяє підприємствам оперативно реагувати на змінні запити клієнтів та ринкові умови. Це знижує ризики, пов'язані з впровадженням інновацій, і сприяє збереженню конкурентоспроможності підприємства [3].

Перспективи розвитку цифрових двійників у промисловості значною мірою пов'язані з подальшим вдосконаленням технологій штучного інтелекту, Інтернету речей (IoT) та великих даних. Комбінація цих технологій дозволяє підвищити точність і швидкість обробки даних, забезпечуючи більш глибокий аналіз і прогнозування. Наприклад, інтеграція цифрових двійників із технологіями машинного навчання дає змогу ефективніше управляти складними виробничими системами, особливо у реальному часі [4].

У майбутньому цифрові двійники стануть важливою частиною екологічно орієнтованих технологій, сприяючи зниженню вуглецевого сліду виробництва. Вони допоможуть підприємствам моделювати сценарії енергоефективності, оцінювати екологічний вплив процесів і розробляти стратегії сталого розвитку. Наприклад, в енергетиці цифрові двійники використовуються для оптимізації роботи відновлювальних джерел енергії та підвищення ефективності їх використання [2]. Однією з найперспективніших областей розвитку є використання цифрових двійників у створенні автономних систем. Наприклад, у автомобільній промисловості та логістиці вони можуть забезпечувати управління автономними транспортними засобами, створюючи точні симуляції дорожніх умов та оптимальні маршрути. Такі рішення сприяють підвищенню безпеки та ефективності транспортування [3].

Іншою перспективною галуззю є інтеграція цифрових двійників у концепцію Індустрії 4.0, де вони сприятимуть повній цифровізації виробничих процесів. Це включає можливість об'єднання всіх елементів виробництва в єдину віртуальну платформу, що забезпечить безперервний контроль, оптимізацію і швидку адаптацію до змін. Такий підхід значно підвищує ефективність виробничих систем та зменшує витрати, створюючи нові можливості для інновацій.

Висновки. Цифрові двійники стали одним із ключових інструментів сучасної промисловості, забезпечуючи ефективне управління виробничими процесами, підвищення продуктивності та зниження витрат. Завдяки інтеграції з такими технологіями, як штучний інтелект, великі дані та Інтернет речей, цифрові двійники дозволяють моделювати, прогнозувати та оптимізувати складні системи у реальному часі. Їх впровадження у різних галузях, включаючи енергетику, автомобільну промисловість та будівництво, демонструє значний економічний потенціал та відкриває нові можливості для інноваційного розвитку.

Перспективи використання цифрових двійників виходять далеко за межі поточних реалізацій. Вони стануть основою для створення автономних систем, сприятимуть досягненню екологічних цілей і глибшій інтеграції концепції Індустрії 4.0. Зважаючи на зростаючу потребу в адаптивності та сталому розвитку, цифрові двійники забезпечують підприємствам конкурентні переваги, створюючи нові можливості для розвитку технологій майбутнього.

Список використаних джерел:

1. Eramo R., Bordeleau F., Combemale B., Brand M., Wimmer M., Wortmann A. Conceptualizing Digital Twins. *IEEE Software*. 2022. № 39(3). P. 39–46.

2. Gourisetti S., Bhadra S., Sebastian-Cardenas D., Touhiduzzaman M., Ahmed O. A Theoretical Open Architecture Framework and Technology Stack for Digital Twins in Energy Sector Applications. *Energies*. 2023. № 16(13). P. 4853.

3. Jones D., Snider C., Nassehi A., Yon J., Hicks B. Characterising the Digital Twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology*. 2020. № 29. P. 36–52.

4. Kapteyn M., Pretorius J., Willcox K. A probabilistic graphical model foundation for enabling predictive digital twins at scale. *Nature Computational Science*. 2020. № 1(5). P. 337–347.

5. Liu M., Fang S., Dong H., Xu C. Review of digital twin about concepts, technologies, and industrial applications. *Journal of Manufacturing Systems*. 2020. № 58. P. 48–65.

6. Li S., Yang Q., Xing J., Chen W., Zou R. A Foundation Model for Building Digital Twins: A Case Study of a Chiller. *Buildings*. 2020. № 12(8). P. 1079.

УДК 658.5:615.1

КОЧЕТОВ ВЛАДИСЛАВ МИКОЛАЙОВИЧ,
магістрант спеціальності 073 «Менеджмент»
Запорізький національний університет (м. Запоріжжя, Україна)

ФОРМУВАННЯ СИСТЕМИ АНТИКРИЗОВОГО УПРАВЛІННЯ У ФАРМАЦЕВТИЧНІЙ ГАЛУЗІ

Фармацевтична галузь є критично важливою для забезпечення суспільного здоров'я, адже вона відповідає за виробництво, постачання та доступність життєво необхідних лікарських засобів. Особливо це актуально в умовах кризових ситуацій, таких як пандемії, економічні чи політичні кризи, які створюють додаткові виклики для функціонування галузі. У такі моменти навіть короткочасний збій у ланцюгах постачання чи виробництва медикаментів може мати катастрофічні наслідки для здоров'я мільйонів людей.

Створення ефективної системи антикризового управління стає ключовим завданням для забезпечення стабільності фармацевтичної галузі. Вона має охоплювати всі аспекти діяльності – від прогнозування ризиків до швидкого реагування на форс-мажорні обставини. Така система дозволяє не лише зберегти стабільність функціонування галузі, а й забезпечити безперебійне постачання медикаментів, що є особливо важливим у моменти пікового попиту на певні препарати (наприклад, антивірусні засоби під час пандемій).

Крім того, системний підхід до антикризового управління допомагає мінімізувати ризики фінансових втрат, забезпечити адаптацію до нових умов ринку та підвищити довіру з боку споживачів і партнерів. Це включає створення резервних планів, стратегічну диверсифікацію постачальників, інвестування у гнучкі технології виробництва та посилення комунікацій як всередині організації, так і з зовнішнім середовищем.

Таким чином, фармацевтична галузь не лише виконує свою безпосередню функцію збереження здоров'я населення, але й стає одним із ключових елементів національної безпеки, особливо в умовах глобальної нестабільності. Ефективне антикризове управління дає змогу галузі вистояти у найскладніших умовах і залишатися надійною опорою для суспільства.

У сучасному світі фармацевтична галузь стикається з дедалі складнішими викликами, які вимагають нових підходів до антикризового управління. Наприклад, під час пандемії COVID-19 значна частина країн зіткнулася з гострим дефіцитом лікарських засобів, засобів індивідуального захисту та вакцин. Це підкреслило важливість наявності ефективної системи планування та швидкого реагування, яка могла б передбачати та запобігати таким кризам.

Одним із ключових аспектів антикризового управління є побудова стійких ланцюгів постачання. В умовах глобалізації фармацевтична галузь часто залежить від імпорту сировини або напівфабрикатів, що робить її вразливою до зовнішніх факторів, таких як геополітичні конфлікти, торговельні санкції чи природні катастрофи. Для зниження таких ризиків необхідно диверсифікувати джерела постачання, створювати регіональні виробничі потужності та забезпечувати стратегічні запаси сировини та готової продукції.

Не менш важливою є роль інноваційних технологій. Впровадження автоматизованих систем контролю запасів, прогнозування попиту за допомогою штучного інтелекту, а також використання цифрових платформ для комунікації з постачальниками та споживачами дозволяють значно підвищити ефективність управління в кризових умовах. Особливе значення має розвиток гнучких виробничих потужностей, які можуть бути оперативно переналаштовані для випуску найбільш затребуваних ліків.

Успішне антикризове управління також потребує ефективної співпраці з державними органами. Уряди багатьох країн вже запроваджують програми підтримки фармацевтичних компаній у кризових ситуаціях, такі як субсидії на створення стратегічних запасів ліків чи пільгове кредитування на розширення виробництва. Водночас фармацевтичні компанії мають активно співпрацювати з регуляторами для спрощення процедур

сертифікації нових препаратів і забезпечення доступу населення до необхідних медикаментів.

Антикризове управління у фармацевтичній галузі також включає роботу з комунікаціями. В умовах кризи важливо забезпечити прозорість у взаємодії з громадськістю, пояснювати причини можливих затримок чи дефіциту ліків і демонструвати зусилля компанії для розв'язання проблем. Ефективна комунікація дозволяє зберігати довіру споживачів і зміцнює репутацію фармацевтичної компанії.

Підсумовуючи, зазначимо, що формування системи антикризового управління має бути довгостроковим процесом, спрямованим на створення стійкої та адаптивної фармацевтичної галузі. Це не лише захищає бізнес і забезпечує його конкурентоспроможність, але й гарантує, що суспільство завжди матиме доступ до життєво важливих медикаментів, навіть у найскладніші часи.

Список використаних джерел:

1. Антошко Т. Р., Романок І. О. Економічні проблеми фармацевтичного підприємства України. *Сучасні проблеми економіки і підприємництво.* 2015. Вип. 16. С. 151–156.

2. Жалінська І. В., Контефт В. П. Сучасні заходи антикризового управління на фармацевтичних та аптечних підприємствах України. *Вісник Миколаївського нац. ун-ту імені В. О. Сухомлинського.* 2016. Вип. 14. С. 352–356.

3. Цифрова трансформація промислового менеджменту: теорія і практика : монографія / за ред. д.філософ.н., проф. В. Г. Воронкової, д.е.н., проф. Н. Г. Метеленко. Львів – Торунь : Liha-Pres, 2023. 816 с.

4. Цифрова трансформація промислового менеджменту у контексті викликів, можливостей та змін : колективна монографія / за ред. д.філософ.н., проф. В. Г. Воронкової, д.е.н., проф. Н. Г. Метеленко. Львів – Торунь : Liha-Pres, 2024.592 с.

УДК 338.246:005.334]:004]:339.9

МАРКОВА СВІТЛАНА ВІКТОРІВНА,
Запорізький національний університет (м. Запоріжжя, Україна)
E-mail: Mrsvvi2@gmail.com
ORCID ID: https://orcid.org/0000-0003-0675-0235

МАРКОВ ІВАН ЄВГЕНОВИЧ,
Запорізький національний університет (м. Запоріжжя, Україна)
ORCID ID: http://orcid.org/0009-0002-8003-5686

ІНТЕГРАЦІЯ АДАПТИВНИХ МЕХАНІЗМІВ МІНІМІЗАЦІЇ РИЗИКІВ У ЦИФРОВОМУ ПРОСТОРІ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В УМОВАХ ГЛОБАЛЬНИХ ЗАГРОЗ

У сучасному світі безпека є багатогранним поняттям, яке охоплює не лише традиційний фізичний захист, а й економічну стабільність, інформаційну стійкість, енергетичну незалежність та кібербезпеку. Глобалізація, цифровізація та інтенсивний розвиток технологій трансформували уявлення про безпеку, зробивши її залежною від динамічних змін у світі та виникнення нових типів загроз. Сучасна система безпеки держави та суспільства ґрунтується на комплексному підході, який охоплює економічну, інформаційну, воєнну та енергетичну складові (рис. 1). Всі ці елементи взаємопов'язані, проте інформаційна безпека виступає ключовою ланкою, адже саме вона забезпечує стабільність і надійність функціонування інших сфер.

У сучасному світі глобалізація та цифровізація створюють нові можливості для розвитку, але водночас відкривають двері для виникнення масштабних загроз. Глобальні виклики, такі як кіберзлочинність, тероризм, економічна нестабільність та енергетичні кризи, мають транснаціональний характер, що ускладнює їх подолання традиційними методами. Забезпечення безпеки стає пріоритетом для держав, міжнародних організацій і бізнесу, адже саме вона є основою стабільного функціонування суспільства. Особливого значення набуває захист цифрового простору, який є критично важливим для економічної, інформаційної, воєнної та енергетичної безпеки. В умовах зростання кількості кіберзагроз та їхньої складності традиційні підходи виявляються неефективними. Необхідно впроваджувати інноваційні та адаптивні механізми для швидкого реагування на загрози, а також створювати стратегії, що передбачають попередження потенційних ризиків. Глобальний характер загроз вимагає об'єднання зусиль на міжнародному рівні. Координація між урядами, приватним сектором і громадськістю є ключовим фактором для забезпечення безпеки.

Рис. 1. Складові безпеки держави

Швидкий розвиток технологій та зростання масштабів цифрової трансформації роблять традиційні методи захисту недостатніми. Сучасні загрози є динамічними, а зловмисники активно використовують штучний інтелект, соціальну інженерію та інші складні техніки. Тому адаптивні механізми, які враховують специфіку нових викликів і здатні оперативно реагувати на загрози, є необхідною умовою для підтримки інформаційної, економічної та воєнної безпеки. Інтеграція таких механізмів є важливим інструментом для міжнародної співпраці у протидії глобальним загрозам. Координація зусиль між державами, компаніями та науковими інституціями дозволяє ефективніше виявляти, аналізувати та нейтралізувати ризики. Таким чином, тема інтеграції адаптивних механізмів мінімізації ризиків є не лише актуальною, але й визначальною для забезпечення безпеки у цифрову епоху.

Інформаційна безпека має пріоритетне значення, оскільки контроль над інформаційними потоками визначає спроможність держави оперативно реагувати на кризи, захищати критичну інфраструктуру та

запобігати маніпуляціям. Інформаційні атаки можуть дестабілізувати економічні системи, порушити роботу енергомереж і знизити ефективність оборонних заходів. У сучасних умовах інформаційний простір є одночасно і джерелом ризиків, і засобом забезпечення безпеки. Інформаційна безпека також є основою для розвитку технологічних інновацій, координації міжнародного співробітництва та формування суспільної довіри до державних і приватних структур. Без належного захисту даних неможливо забезпечити ані економічну стабільність, ані енергетичну незалежність, ані ефективну оборону. Саме тому інформаційна безпека має розглядатися як центральний елемент стратегії забезпечення національної безпеки.

Кібератаки (табл. 1) мають серйозні негативні наслідки для діяльності країн, порушуючи функціонування критичної інфраструктури, таких як енергомережі, транспорт, фінансові системи та державне управління. Напади на державні установи можуть призвести до втрати конфіденційних даних, порушення національної безпеки та дестабілізації економіки. Наприклад, атаки на електромережі або системи водопостачання створюють загрозу життєдіяльності громадян і викликають соціальну напруженість. Такі інциденти також підривають довіру громадян до урядових органів і створюють політичну нестабільність.

Таблиця 1 – **Наслідки кібератак, 2022–2023 рр. [1]**

Рік	Жертва кібератаки	Наслідки	Сума збитків
2022	Коста-Рика	Збитки становлять 1,3 млрд доларів США (30 мільйонів USD на день за півтора місяця).	1,3 млрд USD
	Axie Infinity (Ronin Network)	Викрадено 600 мільйонів доларів США.	600 млн USD
	Binance	Викрадено 570 мільйонів доларів США.	570 млн USD
2023	MOVEit	Від витоку інформації постраждало 2393 організації та від 69 до 73,8 мільйона людей.	Невідомо
	DarkBeam	Викрадено понад 3,8 мільярда електронних скриньок користувачів із паролями.	Невідомо
	Johnson Controls International	Викрадено понад 27 ТБ корпоративних даних і зашифровано віртуальні машини компанії VMWare ESXi.	Невідомо

На глобальному рівні кібератаки впливають на економіку, викликаючи збитки для компаній, які обчислюються мільярдами доларів, і гальмуючи

міжнародну торгівлю. Порушення в ланцюгах постачання, крадіжки інтелектуальної власності, витоки даних і фінансовий саботаж підривають конкурентоспроможність бізнесу. Кібератаки на транснаціональні корпорації, банківські системи чи комунікаційні мережі можуть спричинити ланцюгові наслідки, які зачіпають економіку цілих регіонів. Це вимагає міжнародної співпраці та посилення заходів кібербезпеки для мінімізації глобальних ризиків.

Кібератаки у 2022 та 2023 роках завдали багатомільярдних збитків, серед яких найбільш фінансово збитковими стали атаки на Коста-Рику, Axie Infinity та Binance. Проте у 2023 році спостерігається збільшення кількості атак з величезним масштабом викрадення даних, вартість яких важко оцінити. Це підкреслює необхідність розробки надійних механізмів оцінки збитків та вдосконалення засобів кіберзахисту, аби мінімізувати наслідки у майбутньому

Адаптивні механізми мінімізації ризиків у цифровому просторі є основою для підтримання економічної безпеки. До них належать впровадження блокчейн-технологій для прозорості транзакцій, використання штучного інтелекту для виявлення шахрайських схем, резервне копіювання даних у хмарних сервісах і створення кіберстійких фінансових систем. Ці заходи дозволяють не лише мінімізувати втрати, але й забезпечують конкурентоспроможність економіки в умовах динамічних змін.

Економічна безпека є ключовим чинником стабільності та розвитку держави, оскільки вона визначає здатність економіки функціонувати в умовах внутрішніх і зовнішніх викликів. У сучасному цифровому просторі економічна безпека набула нового значення через стрімкий розвиток технологій, глобалізацію бізнес-процесів і зростання кіберзагроз. Вразливість фінансових систем, електронної комерції та критичної інфраструктури посилюється в умовах зростаючої залежності від цифрових технологій.

Цифровий простір також відкриває нові можливості для економічного зростання, але водночас створює ризики, пов'язані з фінансовими кризами, порушенням ланцюгів постачання та зламом електронних систем управління. У цьому контексті адаптивні механізми є важливими інструментами для швидкого реагування на загрози, підвищення стійкості економічної системи та захисту інтересів держави й бізнесу. Економічна безпека в цифрову епоху стає фундаментом для національної стійкості та глобальної інтеграції.

Адаптивні механізми мінімізації ризиків у цифровому просторі є основою для забезпечення стійкості. Вони включають системи кіберзахисту, які використовують штучний інтелект для виявлення та нейтралізації загроз,

впровадження багаторівневої автентифікації, шифрування даних і постійний моніторинг інформаційних систем. Особливо важливою є швидкість реагування на кіберінциденти, що дозволяє мінімізувати їхній вплив і забезпечувати безперервність функціонування цифрових платформ.

Забезпечення інформаційної безпеки потребує системного підходу, який включає розробку ефективних політик захисту, впровадження сучасних технологій кібербезпеки, підвищення рівня цифрової грамотності населення та міжнародну співпрацю. Тільки поєднання технічних, організаційних і освітніх заходів дозволить забезпечити стійкість до загроз та зберегти довіру до інформаційних систем, що є основою розвитку цифрового суспільства. Для забезпечення комплексної безпеки у цифровому просторі необхідна синергія зусиль держави, бізнесу та громадянського суспільства. Адаптивні механізми мінімізації ризиків повинні базуватися на інноваційних технологіях, таких як штучний інтелект, квантова криптографія та блокчейн. Важливим є також розвиток міжнародної співпраці у сфері кібербезпеки, обмін досвідом і створення єдиних стандартів.

Отже, сучасний цифровий простір є стратегічно важливим елементом функціонування держав, бізнесу та суспільства. Проте зростаюча кількість глобальних загроз, таких як кібератаки, витоки даних і дестабілізація критичної інфраструктури, потребує негайного реагування. Інтеграція адаптивних механізмів мінімізації ризиків є ключовим підходом для забезпечення економічної, інформаційної, воєнної та енергетичної безпеки. Використання сучасних технологій та координація зусиль на національному і міжнародному рівнях дозволяють створити ефективну систему захисту, яка здатна оперативно реагувати на виклики і запобігати катастрофічним наслідкам. Необхідно:

1. Розробка національних стратегій кібербезпеки, а саме визначити чіткі пріоритети, включаючи захист критичної інфраструктури, підвищення обізнаності громадян та створення спеціалізованих кіберцентрів.

2. Впровадження автоматизованих систем моніторингу, штучного інтелекту та машинного навчання для швидкої ідентифікації та нейтралізації загроз.

3. Посилення обміну інформацією між державами та організаціями для виявлення нових типів загроз і розробки глобальних стандартів кібербезпеки.

4. Регулярні навчання та тестування систем.

5. Розвиток кіберосвіти. Включення курсів з кібергігієни у програми навчальних закладів та організація тренінгів для працівників ключових галузей.

Імплементація цих рекомендацій сприятиме підвищенню стійкості до ризиків у цифровому просторі та забезпечить стабільність в умовах глобальних загроз.

Список використаних джерел:

1. Прогноз кіберзагроз 2024. *H-X Technologies.* URL: https://www.h-x.technology/ua/blog-ua/cyber-threats-forecast-2024-ua (дата звернення: 15.11.2024).

УДК 614.2:004.773

МАРТИНЮК ОКСАНА МИКОЛАЇВНА,
магістрантка спеціальності 281 «Публічне управління та адміністрування»
Запорізький національний університет (м. Запоріжжя, Україна)

НІКІТЕНКО ВІТАЛІНА ОЛЕКСАНДРІВНА,
д.філос.н., проф. кафедри управління та адміністрування
Запорізький національний університет (м. Запоріжжя, Україна)
E-mail: vitalina2006@ukr.net
ORCID ID: https://orcid.org/0000-0001-9588-7836

ЦИФРОВІ ТЕХНОЛОГІЇ В УПРАВЛІННІ ЗАКЛАДАМИ ОХОРОНИ ЗДОРОВ'Я

Цифрова трансформація охорони здоров'я є одним із ключових напрямів розвитку сучасної медицини. Заклади охорони здоров'я стикаються з необхідністю адаптації до нових умов, таких як зростання обсягу даних, підвищення вимог пацієнтів до якості обслуговування та обмеженість ресурсів. Використання цифрових технологій дозволяє створити більш ефективну та прозору систему управління, що відповідає сучасним викликам, підвищує якість медичних послуг і сприяє економії ресурсів.

Роль цифрових технологій у закладов охорони здоров'я

Цифрові технології відкривають широкі можливості для підвищення ефективності закладів охорони здоров'я, серед яких:

Електронні медичні картки (ЕМК): дозволяють зберігати повну інформацію про пацієнта, забезпечуючи швидкий доступ до історії захворювань, аналізів, лікування тощо. Це сприяє більш точній діагностиці та оптимізації лікувального процесу. Електронні медичні картки забезпечують спільний доступ до даних між різними закладами охорони здоров'я.

Це особливо важливо у випадках, коли пацієнт проходить лікування в кількох установах або звертається за екстреною допомогою. Використання ЕМК значно скорочує потребу в паперових записах, що зменшує адміністративне навантаження на медичний персонал і знижує ризик втрати даних. Завдяки деталізованій інформації про пацієнта, лікарі можуть розробляти індивідуальні плани лікування, враховуючи попередню медичну історію, алергії та особливості організму. ЕМК дозволяють автоматично оновлювати інформацію про результати аналізів, проведені процедури та зміни в стані здоров'я пацієнта. Це забезпечує лікарів актуальною інформацією в реальному часі.

Системи управління лікарнями (HIS): автоматизують адміністративні та клінічні процеси, зменшуючи навантаження на персонал і мінімізуючи ризик помилок. Системи управління лікарнями (HIS) дозволяють оптимізувати роботу медичних закладів, забезпечуючи координацію між різними відділеннями, автоматизацію записів на прийом, управління ліжковим фондом та ресурсами. Завдяки HIS стає можливим точніше планувати графіки роботи персоналу, враховувати потік пацієнтів і ефективніше використовувати обладнання.

Такі системи також забезпечують централізоване управління фінансами, включаючи облік витрат на ліки, матеріали та інші ресурси, що дозволяє закладам знижувати фінансові втрати. HIS сприяють поліпшенню контролю за дотриманням стандартів якості медичних послуг та протоколів лікування, оскільки автоматично фіксують всі дії, що здійснюються в процесі лікування.

Додатково, HIS інтегруються з іншими цифровими технологіями, такими як електронні медичні картки, системи обробки даних лабораторних досліджень та телемедичні платформи. Це створює єдину екосистему, яка спрощує доступ до інформації та підвищує ефективність прийняття рішень.

Загалом, системи управління лікарнями значно полегшують організацію роботи закладів охорони здоров'я, знижуючи адміністративне навантаження, підвищуючи точність операцій і покращуючи якість медичних послуг для пацієнтів.

Телемедицина: розширює доступність медичних послуг для пацієнтів, особливо у віддалених регіонах, завдяки консультаціям і діагностиці онлайн. Телемедицина відкриває нові можливості для надання медичної допомоги, роблячи її доступнішою для пацієнтів, особливо тих, хто проживає у віддалених чи малодоступних регіонах. Завдяки сучасним цифровим технологіям, пацієнти можуть отримувати консультації лікарів онлайн, не виходячи з дому, що економить час і зменшує витрати на транспорт.

Окрім консультацій, телемедицина дозволяє проводити дистанційну діагностику за допомогою передачі медичних зображень, даних з пристроїв моніторингу стану здоров'я, таких як кардіомонітори, глюкометри, пульсоксиметри тощо. Це забезпечує швидке реагування на зміну стану пацієнта та дозволяє лікарям контролювати хронічні захворювання або стани, що потребують регулярного спостереження. Також телемедицина активно використовується для отримання «другої думки» від спеціалістів з інших міст чи навіть країн, що підвищує якість медичних рішень і розширює можливості для пацієнта.

Аналітика великих даних дозволяє прогнозувати поширення хвороб, оптимізувати використання ресурсів і розробляти стратегії протидії епідеміям. Аналітика великих даних відіграє ключову роль у трансформації системи охорони здоров'я, забезпечуючи новий рівень прогнозування та управління. Завдяки аналізу великих обсягів інформації з різних джерел, таких як електронні медичні записи, дані про спалахи захворювань, соціальні мережі, мобільні додатки тощо, можливо ефективно реагувати на сучасні виклики. Прогнозування поширення хвороб: Аналіз великих даних дозволяє виявляти закономірності у поширенні захворювань, враховуючи різноманітні фактори: сезонність, мобільність населення, кліматичні умови. Це допомагає визначати зони ризику та передбачати можливі спалахи інфекцій, забезпечуючи проактивний підхід у боротьбі з ними. За допомогою аналітики великих даних лікарні можуть краще планувати розподіл медичного персоналу, обладнання, лікарських засобів та інших ресурсів. Наприклад, у разі прогнозування підвищеного попиту на ліжка у відділеннях інтенсивної терапії, лікарня може завчасно вжити відповідних заходів. Аналітика дозволяє швидко оцінювати ситуацію під час епідемій та коригувати стратегії боротьби з поширенням хвороб. Це може включати моделювання сценаріїв введення карантинних заходів, прогнозування ефективності вакцинації або розробку рекомендацій для окремих груп населення. Крім того, аналітика великих даних сприяє більш точній персоналізації лікування, допомагаючи лікарям приймати обґрунтовані рішення на основі статистики та попереднього досвіду. Завдяки цьому підходу охорона здоров'я стає більш адаптивною, ефективною та стійкою до викликів майбутнього.

Цифрові інструменти суттєво впливають на ефективність і якість управління закладами охорони здоров'я:

- Зниження витрат: Автоматизація процесів скорочує витрати на адміністрування та зменшує кількість помилок.
- Підвищення точності діагностики: Штучний інтелект аналізує великі обсяги медичних даних, виявляючи закономірності, які можуть бути непомітними для лікарів.

• Скорочення часу обслуговування: Автоматизовані системи запису та черг забезпечують швидке обслуговування пацієнтів.

• Безперервність медичної допомоги: Інтегровані системи забезпечують доступ до медичних даних пацієнтів у різних медичних установах, що є особливо важливим у невідкладних випадках.

Попри значні переваги, впровадження цифрових технологій супроводжується певними труднощами:

• Низький рівень цифрової грамотності: Медичний персонал не завжди готовий використовувати нові технології, що може уповільнювати їх впровадження.

• Захист персональних даних: Ризики кіберзагроз вимагають надійних механізмів захисту конфіденційної інформації.

• Висока вартість: Інвестиції в цифровізацію є значними, що може бути перешкодою для менш фінансово забезпечених закладів.

• Законодавчі обмеження: Необхідність адаптації нормативної бази до цифрових інновацій є важливим аспектом для успішної трансформації.

5. Пропозиції щодо розвитку цифрових технологій у сфері охорони здоров'я.

Для подолання викликів та максимального використання можливостей цифрових технологій пропонуються такі заходи:

• Підвищення кваліфікації персоналу: Організація тренінгів та навчальних програм з використання цифрових інструментів.

• Створення інтегрованої системи: Впровадження єдиної національної платформи електронної охорони здоров'я для координації між закладами.

• Пілотні проєкти: Тестування нових технологій у невеликих масштабів для оцінки їх ефективності та адаптації до потреб системи.

• Фінансова підтримка: Залучення державних і приватних інвестицій для модернізації закладів охорони здоров'я.

Цифрові технології є важливим фактором модернізації системи охорони здоров'я, що сприяє покращенню якості медичних послуг, оптимізації ресурсів та підвищенню задоволеності пацієнтів. Їхнє ефективне використання вимагає комплексного підходу, який враховує освітні, фінансові, технічні та правові аспекти. Орієнтуючись на потреби суспільства та впроваджуючи інновації, система охорони здоров'я може досягти нового рівня ефективності та доступності.

Список використаних джерел:

1. Про схвалення Концепції розвитку електронної охорони здоров'я : розпорядження Кабінету Міністрів України від 28.12.2020 р. № 1671-р. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1671-2020-%D1%80#n8.

2. Редькін Р. Електронний рецепт: досвід Чехії. *Фармацевт Практик*. 2018. № 3. С. 14–15.

3. Nilsson E., Sverker A., Bendtsen P., Eldh A. C. A human, organization, and technology perspective on patients' experiences of a chat-based and automated medical history-taking service in primary health care: Interview study among primary care patients. *J. Med. Internet Res.* 2021. Vol. 23(10).

УДК 30:332.14:338.242

МАЦКУЛЯК АРТЕМ АНДРІЙОВИЧ,
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: a.matskulyak@gmail.com

ГОЛОМБ ВІКТОРІЯ ВОЛОДИМИРІВНА,
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: viktoria.golomb@gmail.com
ORCID ID: 0000-0003-4053-9310

ОЦІНКА СТАНУ КЛАСТЕРНОГО РОЗВИТКУ В УКРАЇНІ

Кластеризація економіки є інструментом підвищення конкурентоспроможності, який довів свою ефективність у багатьох країнах світу. Скандинавські держави, Німеччина та Італія є яскравими прикладами, де кластери стали основою економічного зростання. В Україні концепція кластерного розвитку почала впроваджуватися з початку 2000-х років, проте значного поширення вона набула лише останніми роками. Метою цього дослідження є оцінка сучасного стану кластерного розвитку в Україні, аналіз проблем і розробка рекомендацій для посилення впливу кластерів на національну економіку.

Кластер – це територіальна група взаємопов'язаних компаній, науково-дослідних установ, освітніх закладів та інших організацій, які взаємодіють для досягнення синергетичного ефекту [2]. Основними складовими кластерів є:

– підприємства ядра: виробники продукції чи послуг;

– інфраструктура підтримки: наукові установи, освітні заклади, фінансові установи;

– органи місцевого самоврядування: координують розвиток кластерів.

У світі існує безліч прикладів успішного кластерного розвитку. Наприклад, Кремнієва долина в США є еталоном технологічного кластеру, де об'єднання компаній, університетів і державної підтримки створило потужну екосистему інновацій.

Що стосується кластеризації в Україні, то цей процес перебуває на етапі становлення. Хоча ідея кластерів є популярною серед регіональних лідерів, її реалізація часто не має системного характеру. Станом на 2024 рік в Україні діє близько 43 активних кластерів, які розподілені нерівномірно. Діяльність кластерів найактивніше розвивається у великих містах.

Зокрема, ІТ-кластери найбільше розвинені у Львові, Києві та Харкові. Вони об'єднують компанії, що працюють у сфері розробки програмного забезпечення та аутсорсингу. Львівський ІТ-кластер – один із найбільш успішних прикладів координації між бізнесом, університетами та міською владою та сфокусований на розвитку високотехнологічного бізнесу. Агропромислові кластери поширені в Черкаській, Херсонській та Вінницькій областях. Вони спрямовані на впровадження інновацій у сільському господарстві. Туристичні кластери сконцентровані у Карпатському регіоні, що демонструє позитивні тенденції у створенні туристичних кластерів, які поєднують готелі, туристичні агентства та місцеві громади.

Ще одним прикладом успішного кластеру є Запорізький кластер «Інжиніринг – Автоматизація – Машинобудування» (ІАМ) – громадська неприбуткова спілка, що об'єднує на добровільних засадах підприємців регіону. Місією кластеру є зростання економічного потенціалу Запорізької області через підвищення конкурентоспроможності учасників кластеру та розвитку регіональної інноваційної екосистеми промислових високотехнологічних секторів. В основі кластеру ІАМ – співпраця широкого кола гравців в наступних економічних секторах: Інжиніринг, Автоматизація, Машинобудування [1].

Основним цілями та завданнями Запорізького кластеру є:

1. Налагодження широкої співпраці між всіма категоріями учасників кластеру з метою вироблення високотехнологічних продуктів з високою доданою вартістю, а також спільної реалізації інжинірингових проектів.

2. Зростання конкурентоспроможності та експортного потенціалу через кращу та спільну реалізацію наявних інструментів експортної підтримки, та створення нових можливостей.

3. Спільне вирішення комплексу проблемних питань регіону в області промисловості та високих технологій – як проблеми утримання персоналу, ріст навичок та кваліфікації, залучення інвестицій, створення нових робочих місць.

4. Вирішення питань вдосконалення процесів на підприємствах та в організаціях-учасниках кластеру ЕАМ.

5. Краща співпраця та синергія з регіональними органами влади та місцевого самоврядування [1].

Незважаючи на доведену високу ефективність кластерів та кластерних структур у забезпеченні національного, регіонального та місцевого розвитку як в ЄС, так і в інших країнах світу, в Україні процесам створення та ефективної діяльності кластерів не приділяється належної уваги.

Основними причинами слабкої ролі кластерів в соціальноекономічному розвитку країни в цілому і окремих регіонів є такі:

– відсутність належного нормативно-правового забезпечення процесів створення та функціонування кластерів;

– відсутність механізмів стимулювання створення та ефективного функціонування кластерів на державному і регіональному рівнях;

– низький рівень запровадження смарт-спеціалізації регіонів і територіальних громад;

– слабке (формальне) відображення процесів кластеризації в стратегіях регіонального розвитку та планах дій щодо їх реалізації;

– низький рівень комунікацій в системі бізнес-громада-наука-влада щодо створення кластерів;

– недосконале експертне та інформаційне супроводження, відсутність статистичного спостереження процесів створення та діяльності кластерів [3].

Кластери виникають самостійно, проте інтенсивність цього процесу залежить від створених центральними та регіональними органами влади відповідних умов.

По-перше, актуальним та важливим є створення сприятливого середовища для створення та функціонування кластерів. Передумовами для цього є: сформована нормативно-правова база; розподіл повноважень між центральними та регіональними органами влади щодо проведення кластерної політики; взаємопов'язані державні, галузеві та регіональні програми (стратегії) розвитку, зокрема щодо створення та ефективного функціонування кластерів.

По-друге, необхідне стимулювання процесів розвитку кластерів. Воно може здійснюватись як через пряму фінансову підтримку кластерних ініціатив, так і через непрямі механізми. Непряме стимулювання може здійснюватись в рамках загальнонаціональних, галузевих та регіональних стратегій, зокрема стратегій смартспеціалізації регіонів і територіальних громад; стратегій підтримки малого та середнього бізнесу (МСБ) (основний елемент підприємницької ініціативи та базового елементу створення

кластерів); підтримку технологічних трансформацій та суттєвої модернізації існуючих виробництв; проведення конкурсів, спрямованих на розвиток компетенцій, навчання, проведення інформаційних компаній, фінансування профільних фундаментальних досліджень та розробок; сприяння виходу на експортні ринки та збільшення участі в глобальних ланцюгах доданої вартості (інтернаціоналізація кластерних ініціатив).

По-третє, рушієм створення кластерів є ефективна смарт-спеціалізація регіонів і територіальних громад. Смарт-спеціалізація та кластеризація мають спільних стейкхолдерів (бізнес, наука, влада, громада). Їх спільними ознаками є орієнтація на інноваційний розвиток, спрямованість на підвищення регіональної конкурентоспроможності та збільшення участі регіонів у глобальних ланцюгах доданої вартості (ГЛДВ). Інтенсивний розвиток кластерів є одним з основних критеріїв успішної смарт-спеціалізації регіонів і територіальних громад [3].

Кластерний розвиток має великий потенціал для економіки України, але його реалізація потребує вирішення ключових проблем. Системний підхід, ефективне державне управління та взаємодія між учасниками кластерів здатні забезпечити стабільний розвиток і підвищити конкурентоспроможність України на світовій арені.

Список використаних джерел:

1. Запорізький кластер ЕАМ. URL: https://www.iamcluster.zp.ua (дата звернення: 10.11.2024).

2. Самборський О. В., Гласов П. В. Сучасна кластерна політика України: проблеми та перспективи. *АГРОСВІТ*. 2021. № 11. С. 57–64.

3. Щодо сприяння розвитку регіональних кластерів в Україні. URL: https://niss.gov.ua/sites/default/files/2021-08/klustery.pdf (дата звернення: 10.11.2024).

УДК 338.24:355.45:004.056.5(477)

МЕТЕЛЕНКО НАТАЛЯ ГЕОРГІЇВНА,
д.е.н., проф., директор
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: natalia.metelenko@gmail.com
ORCID ID: http: orcid.org/0000-0002-6757-3124

ШАРАПОВ ВЛАДИСЛАВ СЕРГІЙОВИЧ,
здобувач третього рівня вищої освіти ступеня PhD, спеціальність 073 «Менеджмент»
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: sharapov.vlse@gmail.com
ORCID ID: http: orcid.org/0000-0002-0994-955X

ЕКОНОМІЧНА БЕЗПЕКА В УМОВАХ ВІЙНИ ТА ЦИФРОВІЗАЦІЇ: АДАПТИВНІ МЕХАНІЗМИ ЗАХИСТУ НАЦІОНАЛЬНИХ ІНТЕРЕСІВ

У сучасному світі економічна безпека є основою стабільного функціонування держав, національних економік та суб'єктів господарської діяльності. Вона охоплює всі аспекти, що забезпечують стійкість до внутрішніх і зовнішніх загроз, таких як економічні кризи, тероризм, екологічні катастрофи та, аспект, що останнім часом стає все більш актуальним – кіберзагрози. Сучасні глобалізація та цифровізація не лише спрощують доступ до ресурсів і можливості для розвитку, але й відкривають нові канали для зловмисних атак, шкідливих впливів і злочинних схем. Це створює додаткові труднощі у забезпеченні економічної безпеки в умовах глобального інформаційного простору, в якому зростає роль новітніх технологій.

Особливе значення ця проблема набуває для України, яка вже декілька років є учасницею активного повномасштабного військового конфлікту. Війна з Російською Федерацією поставила під загрозу не лише фізичну безпеку держави, але й стабільність її економічних структур. У цьому контексті кіберпростір став новим фронтом боротьби: інформаційні атаки, кібершантаж, спроби зламів державних систем і порушення функціонування критичної інфраструктури стають реальністю кожного дня.

Цифровізація економічних процесів значно полегшує доступ до інформації, забезпечує зручні інструменти для бізнесу і державного управління, але водночас створює уразливості, які використовуються як зовнішніми

ворогами, так і внутрішніми дестабілізаторами. З початком війни у цифровому просторі з'явилися нові загрози, які мають потужний вплив на економічну ситуацію: атаки на фінансові системи, саботаж торгових операцій, розлагодження роботи енергетичних і транспортних мереж. Кіберзагрози стали складовою частиною гібридної війни, і тому питання економічної безпеки через призму цифрових технологій стало надзвичайно актуальним для України.

Враховуючи ці обставини, необхідність ефективних механізмів мінімізації ризиків і адаптації до нових умов є ключовою вимогою для забезпечення національної економічної безпеки. Україна змушена постійно шукати нові способи захисту своєї економіки в умовах не тільки традиційних загроз, але й цифрових викликів, що можуть мати довготривалі негативні наслідки для її стабільності.

У зв'язку з вищенаведеним, набуває актуальності дослідження необхідності використання адаптивних механізмів, які здатні реагувати на швидко змінювані умови і на нові кіберзагрози. Це стосується як державного управління, так і бізнес-структур, що повинні будувати свою стратегію на підґрунті максимальної кібербезпеки та готовності до впливу агресора в цифровому просторі.

Таким чином, питання економічної безпеки в умовах війни та цифровізації стало важливою темою для досліджень і розробки конкретних стратегій, спрямованих на збереження та захист національних інтересів України у новій реальності. Враховуючи зростання ролі технологій у сучасному світі, важливо не тільки зрозуміти сутність нових загроз, але й розробити адаптивні інструменти та механізми, здатні забезпечити економічну стійкість держави.

Дослідженню тематики економічної безпеки в умовах цифровізації приділяє увагу все більша кількість вчених. Дубляна Н. І. та Обрамич О. С. розглянули теоретичні засади дослідження сутності цифрової безпеки й визначили її місце у загальній системі безпеки підприємств [1]. Горохова Т. В. у своїй роботі [2] провела аналіз особливостей функціонування суб'єктів господарювання в умовах цифровізації та виокремила основні завдання цифрової трансформації в концепції економічної безпеки. Бакай В. Й. визначив у дослідженні [3] основні проблеми економічної безпеки. Разом з цим, Проскура В. Ф., Черничко Т. В., Верецький Д. [4] сформували систему показників економічної безпеки суб'єктів господарської діяльності. Чайкіна А. О., Маслій О. А. та Черв'як А. В. визначили сучасні чинники підвищення ефективності економічної безпеки країни в умовах цифрової трансформації [5]. Череп А. В. та Сарбєй Л. С. дослідили використання цифровізації у якості інструменту відновлення

економіки держави у повоєнний період [6]. Воронкова В. Г., Бєлоусов В. В., Колюх В. О. проаналізували у своїй роботі використання бізнес-аналітики як ресурсу аналітично-інформаційного забезпечення управління [7], а Коптєва Г. М. приділила увагу дослідженню засобів забезпечення економічної безпеки суб'єктів господарювання в умовах цифрової трансформації [8].

Основною метою нашої роботи є визначення ключових аспектів економічної безпеки в умовах війни та цифровізації, проведення аналізу наявних викликів для України та розробка рекомендацій щодо мінімізації ризиків через адаптивні механізми.

Економічна безпека є критично важливим елементом функціонування будь-якої держави, оскільки забезпечує її стабільність, збереження національних інтересів і можливість ефективного розвитку. Вона включає в себе здатність країни протистояти як внутрішнім, так і зовнішнім загрозам, що можуть виникати через економічні, політичні, соціальні чи екологічні фактори. Традиційно до основних складових економічної безпеки відносяться фінансова стабільність, енергетична незалежність, продовольча безпека, здатність до мобілізації ресурсів та інші фактори, що забезпечують країні необхідні умови для безперебійного функціонування. Однак у сучасному світі ці традиційні аспекти набули нового змісту в умовах цифрової ери та військових конфліктів, передбачаючи ще й здатність протистояння кіберзагрозам, інформаційним атакам і економічному шантажу.

У наш час, коли економіка стає все більш залежною від інформаційних технологій, цифрова безпека перетворюється на невід'ємну частину загальної економічної безпеки держави. Інформаційні технології та кіберінфраструктура становлять основу не тільки для ведення бізнесу, але й для забезпечення функціонування критично важливих секторів економіки, таких як енергетика, фінанси, транспорт та телекомунікації.

В умовах війни, особливо такої, як війна в Україні, коли агресор активно використовує кіберзброю як частину своєї стратегії, цифрова безпека стає пріоритетом національної безпеки. Кібератаки, націлені на критичні інфраструктури держави, можуть спричинити серйозні економічні та соціальні наслідки, порушуючи нормальне функціонування державних та приватних установ. У ситуації, коли війна активізує інформаційну боротьбу, не тільки кібератаки, а й інформаційні війни (фейкові новини, дезінформація, маніпуляція громадською думкою) можуть мати суттєвий вплив на економічну ситуацію в країні. Тому важливо розглядати економічну безпеку як комплексний елемент, що поєднує не лише традиційні засоби захисту, але й цифрові механізми, що дозволяють протистояти таким загрозам.

Однією з найсерйозніших загроз є саме кіберзагрози, які можуть призвести до значних економічних втрат. Кіберзлочинці та державні актори, які ведуть кібервійни, можуть спрямовувати свої атаки на фінансові установи (можуть включати зломи банківських систем, атаки на платіжні системи, викрадення грошей чи даних користувачів, що призведе до економічних збитків та втрати довіри до фінансової системи), критичну інфраструктуру (знищення або модифікація даних в енергетичних та логістичних системах, що можуть спричинити зупинку виробництва, перебої з постачанням енергоносіїв та порушення життєзабезпечення), урядові бази даних і енергетичні системи. Серед типів кіберзагроз можна виокремити кібератаки, шкідливі програми та віруси (наприклад, атаки типу "ransomware", які блокують доступ до важливих даних і вимагають викуп, можуть вплинути на нормальне функціонування державних і приватних компаній, порушити комунікації і бізнес-процеси). Війна в Україні продемонструвала серйозні наслідки таких атак, зокрема, атаки на енергетичні об'єкти та банки, які спричинили як короткочасні, так і довготривалі економічні проблеми.

Інформаційні війни є ще одним важливим аспектом, що загрожує економічній безпеці держави. В умовах війни дезінформація та маніпулювання фактами можуть стати потужним інструментом для підриву економічної стабільності. Розповсюдження фейкових новин, спотворення інформації про стан економіки або зниження довіри до фінансової системи можуть призвести до паніки серед громадян, зниження інвестиційної привабливості та зупинки економічного розвитку. Додатково подібні атаки можуть викликати соціальні протести, масові відтоки капіталу та навіть спекуляції на фінансових ринках, що також може призвести до економічної дестабілізації. До основних видів інформаційних загроз можна віднести фейкові новини і пропаганду (поширення неправдивої інформації про фінансовий стан держави, політичну ситуацію або зміни в економічній політиці можуть призвести до паніки серед громадян, падіння курсу валюти, зменшення інвестицій та відтоку капіталу), кризову комунікацію (війна та економічні труднощі можуть бути використані агресором для інформаційного тиску, підриву довіри до уряду, посилення соціальних протестів та економічних санкцій), фальшиві економічні прогнози (дезінформація про прогнози економічного розвитку, кризу в окремих галузях або проголошення дефолту можуть суттєво вплинути на інвесторів і бізнес, знижуючи рівень інвестиційної привабливості країни).

Цифровізація відкриває нові можливості для агресора щодо використання економічних маніпуляцій як засобу тиску. Використання цифрових платформ для економічного шантажу може передбачати застосування

криптовалют та інших анонімних платіжних систем (для обходу санкцій, фінансування тероризму чи інших незаконних економічних операцій), перехоплення важливих даних (у разі доступу до державних або комерційних баз даних можливо здійснити шантаж щодо розголошення інформації, яка має важливе економічне значення).

У сучасному цифровому середовищі економічна безпека держави залежить від здатності швидко реагувати на змінювані умови та нові загрози. З огляду на постійне оновлення кіберзагроз та глобальних економічних викликів, Україні потрібно розробляти і впроваджувати адаптивні механізми захисту своєї економіки, здатні оперативно реагувати на нові загрози, а саме: технологічні рішення для зміцнення економічної безпеки, удосконалення нормативно-правової бази, розвиток співпраці на міжнародному рівні, забезпечення кібербезпеки критичної інфраструктури та інформаційної прозорості.

Розвиток технологій, таких як штучний інтелект, блокчейн та BigData даних, дозволяє створювати системи для моніторингу та прогнозування можливих загроз, своєчасного виявлення кіберінцидентів та атак. Штучний інтелект, зокрема, може використовуватись для автоматизації процесів виявлення та нейтралізації кіберзагроз в реальному часі.

Крім технологічних рішень, необхідно також посилювати правову основу, що регулює сферу цифрової безпеки. Створення чітких правил для захисту даних, кіберзлочинності, криптовалютних транзакцій та електронних платіжних систем дозволить не лише забезпечити більшу прозорість і безпеку, а й сформує юридичні інструменти для протидії новим формам економічних атак.

Оскільки кіберзагрози мають глобальний характер, важливим кроком є зміцнення міжнародної співпраці в галузі цифрової безпеки. Спільні ініціативи, обмін інформацією про загрози та розробка єдиних стандартів кіберзахисту дозволять знизити ймовірність глобальних кібератак і зменшити їхній негативний вплив на економіку.

Забезпечення кібербезпеки критичних інфраструктур є важливим елементом національної безпеки, оскільки порушення їх роботи може мати серйозні наслідки для економіки та стабільності країни. Для цього необхідно проводити регулярні аудити безпеки, щоб виявляти вразливості та забезпечувати захист від кіберзагроз. Оскільки технології швидко змінюються, важливо постійно оновлювати системи захисту, впроваджувати новітні технології, як штучний інтелект і блокчейн, для моніторингу та реагування на атаки. Особлива увага має бути приділена захисту критичних даних і резервному копіюванню інформації, зокрема у фінансовому та енергетичному секторах. Спільна робота держави

і приватних компаній є ключовою для створення ефективних стандартів безпеки. Окрім цього, навчання персоналу, що забезпечує функціонування критичних інфраструктур є важливим аспектом для зниження ризиків, пов'язаних з людським фактором. Тільки комплексний підхід до кібербезпеки допоможе зберегти стабільність важливих секторів економіки.

Інформаційна прозорість є важливим компонентом економічної безпеки, особливо в умовах війни та цифровізації. Для зменшення впливу фейкових новин і маніпуляцій на економіку потрібно посилити контроль за інформаційним середовищем. Це включає створення платформ для моніторингу та боротьби з дезінформацією, використання штучного інтелекту для автоматичного виявлення фейкових новин, а також розвиток медіаграмотності серед населення. Необхідно забезпечити прозорість офіційної інформації, що знижує можливість виникнення маніпуляцій, підвищуючи довіру до економічної стабільності. Додатково важливо сприяти співпраці з міжнародними організаціями для обміну даними про дезінформаційні загрози.

Висновок. Економічна безпека є основою стабільності та розвитку будь-якої держави, зокрема в умовах глобалізації, цифровізації та сучасних викликів. Для України, яка перебуває в умовах війни з Російською Федерацією, питання економічної безпеки набуває особливої актуальності. Кіберзагрози та інформаційні війни стали новими важливими аспектами, що впливають на економічну стабільність країни. Цифровізація не лише відкриває нові можливості для розвитку, але й створює нові уразливості, які можуть бути використані агресором.

Адаптивні механізми, що дозволяють оперативно реагувати на нові загрози, зокрема шляхом розвитку технологій штучного інтелекту, блокчейну та Big Data, є необхідними для збереження національної економічної безпеки. Додатково потребуються зміцнення кібербезпеки критичних інфраструктур, удосконалення нормативно-правової бази, а також посилення міжнародної співпраці у сфері цифрової безпеки.

Забезпечення інформаційної прозорості й боротьба з дезінформацією також є важливими складовими стратегії економічної безпеки. Для цього необхідно створювати механізми контролю за інформаційним середовищем, використовувати штучний інтелект для виявлення фейкових новин, а також активно співпрацювати з міжнародними партнерами.

Висновки. Таким чином, комплексний підхід до економічної безпеки, що поєднує традиційні методи захисту з інноваційними цифровими рішеннями, є необхідним для забезпечення стабільності та захисту національних інтересів України в умовах сучасних викликів.

Список використаних джерел:

1. Дуляба Н. І., Обрамич О. С. Теоретичні засади дослідження сутності цифрової безпеки. *Економіка та суспільство.* 2023. № 55. URL: https://economyandsociety.in.ua/index.php/journal/article/view/2887 (дата звернення: 01.11.2024).
2. Горохова Т. В. Економічна безпека цифрового підприємства промислово-енергетичного комплексу в сучасних умовах господарювання. *Цифрова економіка та економічна безпека.* 2022. № 2(02). С. 99–103. URL: http://dees.iei.od.ua/index.php/journal/article/view/74/71 (дата звернення: 02.11.2024).
3. Бакай В. Й. Забезпечення економічної безпеки підприємства на основі використання цифрових технологій. *Вісник ХНУ. Серія: Економічні науки.* 2020. № 4(1). С. 32–35. URL: http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/01/7-19.pdf (дата звернення: 02.11.2024).
4. Проскура В. Ф., Черничко Т. В., Верецький Д. Сучасні підходи до визначення рівня економічної безпеки підприємства в умовах цифровізації. *Цифрова економіка та економічна безпека.* 2024. № 4(13). С. 61–67. URL: http://dees.iei.od.ua/index.php/journal/article/view/416 (дата звернення: 02.11.2024).
5. Чайкіна А. О., Маслій О. А., Черв'як А. В. Сучасні драйвери підвищення економічної безпеки країни в умовах цифрової трансформації. *Сталий розвиток економіки.* 2024. № 2(49). С. 307–313. URL: https://economdevelopment.in.ua/index.php/journal/article/view/979/938 (дата звернення: 02.11.2024).
6. Череп А. В., Сарбєй Л. С. Цифровізація як інструмент відбудови економіки України в повоєнний період. *Молодий вчений.* 2023. № 12(124). URL: https://molodyivchenyi.ua/index.php/journal/article/view/6032/5900 (дата звернення: 02.11.2024).
7. Воронкова В. Г., Бєлоусов В. В., Колюх В. О. Бізнес-аналітика як стратегічний ресурс інформаційно-аналітичного забезпечення управління підприємствами та організаціями в умовах цифрової трансформації. 2024. № 5(14). URL: http://dees.iei.od.ua/index.php/journal/article/view/439/421 (дата звернення: 02.11.2024).
8. Коптєва Г. М. Забезпечення економічної безпеки підприємства торгівлі в умовах цифровізації. НТУ «Харківський політехнічний інститут». 2020. URL: https://core.ac.uk/outputs/333611508/?source=oai (дата звернення: 02.11.2024).

УДК 338.242.4

МОРОЗ ОЛЕГ СЕМЕНОВИЧ,
к.е.н., доцент
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького Національного Університету (м. Запоріжжя, Україна)
E-mail: oleg.moroz.55@ukr.net
ORCID ID: http://orcid.org/0000-0001-7336-8023

ЕКОНОМІЧНА БЕЗПЕКА ЯК ФУНДАМЕНТ ВІДБУДОВИ УКРАЇНИ

Досвід країн, які у свій час пережили військові вторгнення, або громадянські війни (Грузія, Боснія та Герцеговина, Хорватія, Корея, Японія, Німеччина), показує що опісля завершення бойових дій на перший план висувалося посилення державної безпеки (власних кордонів, армії, створення безпечного середовища як всередині, так і зовні країни). При цьому, в наслідок того, що ці країни зазнавали значних руйнувань та економічних збитків, однією з першочергових проблем, які поставали перед ними, була також і проблема забезпечення певного рівня економічної безпеки на підґрунті максимальної організованості та концентрації зусиль в напрямах відновлення та вдосконалення відносин в сферах виробництва, розподілу, обміну та споживання на засадах здатності домовлятися як всередині країни, так і ззовні.

Метою даного дослідження є висвітлення окремих аспектів економічної безпеки в умовах відбудови країни у повоєнний час та подолання наслідків війни.

Саме поняття «*безпека*» можна охарактеризувати як повна відсутність або мінімізація рівня небезпеки, забезпечення, збереження та вдосконалення певного рівня стабільності і стійкості (політичної, економічної, соціальної тощо) в державі, який забезпечує як безумовне виконання чинних законів і нормативно-правових актів на основі підтримання правопорядку, так і розвиток міжнародного співробітництва на основі добросусідства, захищеності та партнерства [1, с. 54].

Чинне законодавство України, ототожнюючи національну та державну безпеку, визначає їх як досягнення захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. При цьому, національні інтереси України визначаються як життєво важливі інтереси людини, суспільства і держави, реалізація

яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян [2, ст. 1].

Таким чином, національна (державна) безпека має декілька *рівнів (об'єктів) безпеки*, а саме: а) *державний рівень безпеки*, як безпека з точки зору певного соціально-політичного інституту, який зобов'язаний здійснювати управління комплексом внутрішніх та зовнішніх функцій забезпечення життєдіяльності суспільства на території країни; б) населення цієї країни, як об'єкт забезпечення безпеки, що утворює її *суспільний рівень безпеки*; в) *регіональний рівень безпеки* характеризує безпеку для певних об'єднань громадян, що мешкають не окремих територіях країни, які утворюють територіальні громади регіонів країни; г) *безпека господарюючих суб'єктів*, що функціонують в країні для задоволення як власних, так і колективних, регіональних та навіть суспільних та національних інтересів; д) *безпека окремих осіб* – громадян країни, що перебувають як на території країни, так і за її межами, а також громадян інших країн, які на законних підставах перебувають в країні.

З іншого боку кожен із зазначених об'єктів (рівнів) національної (державної) безпеки, як і ця безпека в цілому, має певну низку *акцентів* щодо формування, існування та розвитку безпеки цього об'єкту (рівня) – певного комплексу так званих «*функціональних безпек*». Серед таких безпекових акцентів можна зазначити, зокрема, такі як: а) військово-політичні безпекові аспекти (воєнна та політична (міжнародна та внутрішньо-політична) безпека), а також суспільно-громадські безпекові аспекти (безпека суспільства та безпека громадсько-державного ладу), які в цілому можна розглядати в якості державної безпеки, як невід'ємної частини національної безпеки, яка багато в чому визначає умови її існування; б) валютно-фінансові та економічні безпекові аспекти, які можна розглядати з точки зору економічної безпеки; в) соціогуманітарні безпекові аспекти, що формують соціальну безпеку, яка разом з економічною безпекою визначають напрями, параметри та темпи реалізації соціально-економічної політики держави; г) інформаційні безпекові аспекти, що формують як інформаційну безпеку в цілому, так і кібербезпеку, зокрема; д) ціла низка інших безпекових аспектів (ресурсо-технологічні, інфраструктурні, енергетичні тощо), які визначають відповідні функціональні напрями забезпечення безпеки певного об'єкту.

Стратегія забезпечення як базового, так і оптимально-необхідного рівня безпеки по кожному з наведених безпекових аспектів (функціональних безпек) має знайти своє відображення як в стратегії національної безпеки України в цілому, стосовно цілей, завдань і механізмів захисту

національних інтересів України, так і в стратегіях існування та розвитку кожного з об'єктів (безпекових рівнів). При цьому, стратегічне бачення відносно забезпечення та посилення кожної з функціональних безпек, мусить стати як окремим елементом та складником, так і певною частиною загальної безпекової стратегії, яка визначатиме її спрямування, пріоритети та напрями розвитку об'єкту управління в цілому. Метою безпекової стратегії, як візії бажаного стану об'єкту з позиції «де ми маємо бути», полягає у визначенні напрямів формування і реалізації відповідної політики (тактики реалізації стратегії) досягнення цієї позиції виходячи з позиції «де ми є» тут і зараз.

Економічна безпека, як складова частина національної безпеки, є цілісною системою економічних, правових, організаційних, політичних та правоохоронних заходів, спрямованих на забезпечення: а) *захисту економічної системи* від існуючих та можливих майбутніх загроз, негативного впливу на цю систему чинників внутрішнього та зовнішнього середовища; б) дотримання певного стану *економічних відносин* у різних сегментах економічної системи (матеріально-виробничої, комерційно-підприємницької, фінансово-банківської, інвестиційно-інноваційної, податкової підсистем тощо) [3, с. 62].

Таким чином, стан економічної безпеки країни в цілому віддзеркалює стан її економіки та існуючих економічних відносин (відносин, пов'язаних з виробництвом, розподілом та споживанням), при якому забезпечується: а) достатній економічний та оборонний потенціал, що здатний гарантовано забезпечити захист національних інтересів; б) задоволення економічних потреб суспільства на основі здатності забезпечувати мінімально необхідний обсяг виробництва продуктів та товарів для її самостійного виживання, розвитку та економічного благополуччя; в) контроль держави за рухом і використанням національних ресурсів та захист економічних інтересів країни на національному й міжнародному рівнях, а також належна протидії економічним злочинам.

Станом економічної безпеки визначаються також основні засади соціальної безпеки – починаючи з визначення параметрів, критеріїв та індикаторів державної (відповідно і регіональної, галузевої та бізнесової) соціальної політики, яка в прикладному сенсі віддзеркалює забезпечення належного рівня соціальної безпеки, закінчуючи визначенням ризиків та загроз, що впливають на можливості щодо реалізації соціальних інтересів окремої особи, групи осіб (громади) або суспільства в цілому.

Саме тому, визнаючи, що забезпечення державної безпеки є умовою існування держави, а соціальної безпеки – її метою, можна *дійти до висновку*, що економічна безпека є тією складовою частиною національної

безпеки, яка забезпечує *фундамент і матеріальну основу* існування та розвитку як держави та суспільства в цілому, так і окремих територіальних об'єднань (регіонів), галузей та сфер діяльності, господарюючих суб'єктів та окремих осіб, зокрема.

До елементів, що є складовими економічної безпеки по її об'єктах (рівнях) можна, зокрема, віднести такі як: природні багатства, виробничі і невиробничі фонди, нерухомість, матеріальні і нематеріальні, а також паливно-енергетичні, фінансові та людські ресурси, господарюючі суб'єкти, окремі особи тощо.

Формуючи підходи та розкриваючи заходи щодо забезпечення безпеки того чи іншого об'єкту (рівня) в цілому, та їх економічної безпеки, зокрема, необхідно враховувати на наявність у кожного з безпекових об'єктів (рівнів) *власних домінантів* щодо безпеки, які можуть не лише виступати у вигляді певної невідповідності та суперечливості, а навіть переходити у конфлікт інтересів. Так, зокрема, існує певне розходження між сприйняттям як параметрів і критеріїв економічної безпеки, так і методів та засобів її забезпечення, наприклад, між державою і певними регіонами, галузями та господарюючими суб'єктами, між господарюючими суб'єктами та окремими особами, тощо.

Таким чином, можна дійти до *висновку*, що одним з основних завдань, які постають з позиції забезпеченням національної безпеки України в повоєнний період, стає задача *гармонізації відносин* між різними об'єктами (рівнями) економічної безпеки та недопущення конфлікту їх інтересів.

Відбудова України в повоєнний період, з точки зору забезпечення економічної безпеки, враховуючи на стан економічної системи країни в цілому та економічних відносин, зокрема, ускладняється цілою низкою чинників, в тому числі такими як: а) обмеженість власних ресурсів для подолання наслідків руйнувань, спричинених війною, для відбудови інфраструктури (енергетичної, логістичної, фінансової тощо) країни в цілому та окремих її регіонів, зокрема, а також відновлення окремих бізнесових активів та виробничих потужностей; б) демографічні втрати в країні в цілому та окремих її регіонах, зокрема, спричинених війною, а також суттєве зменшення трудового потенціалу країни в цілому (значні обсяги міграції населення на тривалий час, що створює передумови для перетворення її в трудову еміграцію в першу чергу для кваліфікованої робочої сили) та її інноваційного потенціалу (зменшення наукової бази для фундаментальних та галузевих наукових досліджень, а також дослідних та проектно-конструкторських установ), зокрема; в) наявність несприятливого (в наслідок існування в умовах післявоєнного стану низки ризиків, пов'язаних як з безпековими викликами післявоєнного стану, так

і наявністю суттєвої заборгованості країни перед країнам-партнерами та окремим транснаціональним структурам за результатами війни) для розвитку вітчизняного бізнесу інвестиційного клімату в Україні; г) загострення в посткризовий період конкурентної боротьби як на міжнародній арені в межах світового господарства в цілому, так і в окремих галузях та видах діяльності, зокрема, тощо.

Відбудова України, яка передбачає значне підвищення рівня життя українців та створення конкурентного середовища для повернення громадян, які були змушені покинути країну на підґрунті структурного відновлення усіх галузей та сфер життя. **[**4**]** Відповідно для досягнення визначеної мети необхідно забезпечити умови для посилення економічної безпеки як країни в цілому, так і окремих її об'єктів (рівнів), зокрема.

Економічна безпека, що визначається станом економічної системи та існуючих в цій системі економічних відносин, характеризується *моделлю розбудови економіки*, яка має визначити напрями та темпи розбудови економічної системи на засадах *інноваційної економіки*, як економіки, що спирається на інтелект новаторів і вчених, втілений в розвиток високотехнологічних та інформаційних сфер економіки. Саме розбудова такої моделі економіки країни, на тлі потреб та зацікавленості наших партнерів в ліквідації наслідків війни (хоча б з метою забезпечення умов повернення боргів), а також існуючого позитивного іміджу країни серед представників передових економік світу, може скласти фундамент майбутнього відновлення економіки країни. Обґрунтуванням такого підходу до відновлення України у повоєнний період на засадах інноваційної економіки полягає, на наш погляд, в тому, що інші моделі розбудови економіки не дозволять цього тому що: а) *ресурсна економіка*, як економіка, що спирається на видобуток, первинну переробку та доставку сировини та корисних копалин, що була притаманна Україні останні десятиліття, не в змозі, забезпечити економічні можливості для подолання економічних та соціально-політичних наслідків війни; б) відродження *індустріальної економіки*, як економіки, що спирається на розвинуте індустріальне виробництво, що було властиво економічній системі Україні в складі СРСР, на тлі руйнувань інфраструктури і бізнесових структур, а також загострення внутрішньої та міжнародної конкуренції є дуже проблематичним; в) побудова *економіки фінансів*, економіки, що базуються на концентрації фінансів (капіталу) й фінансових операціях та спирається на використання міцної національної валюти (на рівні міжнародної валюти), а також на високий рівень національної безпеки країни, є практично неможливим.

Проте впровадження тієї чи іншої моделі економічної системи та характеру економічних відносин потребує:

• формування та розвиток сучасної системи економічної безпеки, специфічними засадами якої є не тривіальність, адаптивність, гнучкість, стійкість, ефективність, надійність, самоорганізація тощо;

• створення сприятливих умов для інноваційно-інвестиційної діяльності з розширенням можливостей залучення як іноземних та міжнародних, так і вітчизняних інвесторів та стейкхолдерів;

• проведення, жорсткої та цілеспрямованої протекціоністської державної політики (навіть в супереч окремим вимогам ВТО);

• посилення: а) контролю грошових потоків та звітування про використані кошти, формування прозорого середовища для тендерів; б) заходів щодо забезпечення прозорої звітності перед кредиторами та донорами економіки для поліпшення іміджу та конкурентного становища; в) заходів, відносно забезпечення усіма доступними та можливими шляхами безпекових гарантій та засобами оборони тощо.

Таким чином, можна дійти до *висновку*, що саме реалізація всебічно обґрунтованої та збалансованої системи економічної безпеки на підґрунті політики економічних перетворень, спрямованих на подолання наслідків війни та отримання очікуваних і здійсненних її результатів, надає можливість не лише зміцнити загальний рівень національної безпеки країни в цілому, а також фундамент її державної безпеки та визначити критерії та параметри щодо формування соціальної безпеки країни, зокрема.

Список використаних джерел:

1. Нижник Н. Р., Ситник Г. П., Білоус В. Т. Національна безпека України : методологічні аспекти, стан і тенденції розвитку. Київ : Преса України, 2020. 304 с.

2. Про національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII. *Відомості Верховної Ради (ВВР).* 2018. № 31. Ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

3. Економічна безпека держави : навчально-методичний посібник / за ред. З. Б. Живко. Черкаси : видавець Чабаненко Ю. А., 2019. 240 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3466/1/НМП_Економічна%20безпека%20держави.pdf

4. Проєкт «Національна економічна стратегія України 2030». URL: https://nes2030.org.ua/

УДК 338.22:004

НІКОЛАЄНКО ЄВГЕН АНАТОЛІЙОВИЧ,
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: Nikolaenkoevgen77@gmail.com
ORCID ID: http://orcid.org/0009-0009-2876-7928

ЦИФРОВА ЕКОНОМІКА ТА ЕКОНОМІЧНА БЕЗПЕКА В КОНТЕКСТІ УПРАВЛІННЯ ВИРОБНИЧО-ГОСПОДАРСЬКОЮ ДІЯЛЬНІСТЮ ПІДПРИЄМСТВА В УМОВАХ ВІЙСЬКОВОГО ЧАСУ ТА ПІСЛЯВОЄННОЇ ВІДБУДОВИ

Актуальність обраної теми обумовлена тим, що цифрові технології, такі як автоматизація, штучний інтелект, аналіз великих даних та хмарні рішення, дозволяють підприємствам підтримувати зв'язок із клієнтами та постачальниками, ефективно управляти ресурсами та виробничими процесами, а також знижувати залежність від фізичних інфраструктур. В умовах війни та післявоєнної відбудови цифровізація може стати основою для швидкої адаптації бізнесу до нових умов, що дозволяє зменшити ризики та підвищити ефективність. Водночас, економічна безпека України зазнає відчутних трансформацій в умовах довготривалої війни. Пройшовши етап стабілізації та адаптації до перших шоків повномасштабного вторгнення, національний економічний механізм почав поступовий перехід до економіки воєнного часу, що підкреслює необхідність впровадження цифрових технологій для підтримки економічної стабільності. Це обумовлює як обережні оптимістичні прогнози експертів стосовно економічного відновлення, так і нові виклики та загрози економічній безпеці держави, які можуть бути мінімізовані завдяки ефективному використанню цифрових рішень в управлінні економікою.

У 2024 р. виклики і загрози економічній безпеці пов'язуються насамперед із безпосереднім деструктивним впливом воєнних дій для економічного розвитку (зокрема: фізичними руйнуваннями основних засобів та економічної інфраструктури, неможливістю здійснювати економічну діяльність в умовах воєнних дій на локальних напрямках; ракетно-дроновими атаками та ін.), нестачею кваліфікованої робочої сили, а також ймовірним збільшенням макроекономічних диспропорцій [2, с. 4]

Ступінь наукової розробки теми свідчить про значну увагу до проблематики цифрової економіки та її впливу на економічну безпеку в умовах

управління підприємствами, зокрема в контексті сучасних викликів, таких як військовий час та післявоєнна відбудова. Ретельний аналіз літератури дозволив виділити низку авторів, чиї роботи присвячені різноманітним аспектам цієї теми. Зокрема, Базілюк Я. Б. та Воронкова В. Г. досліджують проблеми цифровізації та автоматизації в управлінні підприємствами, визначаючи основні фактори, які забезпечують стійкість бізнесу в умовах економічної нестабільності. Гладких Д. М. та Котелевець Д. О. зосереджуються на впливі цифрових технологій на економічну безпеку підприємств, підкреслюючи важливість захисту інформаційних систем і адаптації до нових реалій. Кіндзерський Ю. В., Ліпич Л. Г. та Метеленко Н. Г. аналізують інструменти, що дозволяють підвищити ефективність виробничо-господарської діяльності за допомогою цифрових технологій, а також зменшити ризики для економічної безпеки в умовах кризових ситуацій. Піжук О. І. і Шостак Л. В. зосереджуються на впливі цифрових трансформацій на стратегії економічного розвитку підприємств в умовах невизначеності. Яковенко О. І. та інші дослідники вивчають питання інтеграції цифрових рішень у системи управління підприємствами з урахуванням специфіки післявоєнного відновлення економіки. Їхні праці становлять вагомий внесок у розвиток наукового розуміння того, як цифрова економіка може стати основою для забезпечення економічної безпеки та стійкості підприємств в умовах сучасних викликів. Проте, тема потребує подальших глибших досліджень, оскільки існуючі наукові розробки не завжди враховують усі аспекти впливу цифрових технологій на економічну безпеку підприємств у специфічних умовах військового часу та післявоєнної відбудови. Зокрема, необхідно більш детально вивчити інтеграцію цифрових рішень у процеси управління виробничо-господарською діяльністю в умовах значних геополітичних і економічних змін, а також розробити нові підходи до мінімізації ризиків кіберзагроз і забезпечення безпеки інформаційних систем на рівні окремих підприємств і національної економіки загалом. Окрім того, потребують подальшого вивчення специфічні механізми адаптації підприємств до умов постійно змінюваної економічної ситуації, пов'язаної з відновленням інфраструктури та реінтеграцією підприємств, зруйнованих під час війни. Зокрема, варто дослідити, як саме цифрові технології можуть сприяти створенню нових моделей бізнесу, спрямованих на ефективне відновлення та підтримку економічної безпеки в умовах післявоєнного періоду.

На тлі зазначених викликів та загроз, збереження прийнятного інноваційного й виробничого розвитку, залишаються важливими завданнями для мінімізації ризиків економічної безпеки України. У зв'язку з цим керівники підприємств змушені прискорити цифрову трансформацію

системи управління виробничо-господарською діяльністю з забезпеченням стабільного розвитку цифрової економіки та досліджувати інноваційні технологічні рішення інтегрованих комунікацій та їх інструментів. Крім того, керівники та працівники, повинні безперервно отримувати технологічні знання для постійної актуалізації ефективного інструментарію. Це може допомогти розв'язати безпрецедентні можливості та виклики, вдосконалити систему управління підприємством за рахунок підвищення ефективності, розширення сфери діяльності та впровадження інноваційних технологій.

В умовах швидкозмінної реальності, неочікувані та безпрецедентні виклики, що виникли внаслідок повномасштабної війни з росією, призвели до необхідності посилання динамізму бізнес-середовища з пошуку нових гнучких методів управління та організаційних структур виробничо-господарської діяльності підприємств [1, с. 64].

Інноваційна активність підприємства, його спроможність імплемувати в свою діяльність інформаційно-комунікаційні технології, схильність до впровадження інноваційних цифрових продуктів і діджиталізації процесів надання послуг споживачам визначають рівень конкурентоздатності підприємств на ринку, що в умовах глобалізації та швидких змін у технологічному середовищі є ключовим фактором для забезпечення стійкості та розвитку в довгостроковій перспективі. Крім того, ефективне використання цифрових технологій дозволяє не лише оптимізувати внутрішні бізнес-процеси, але й створювати нові бізнес-моделі, що сприяють розширенню ринкових можливостей та підвищенню фінансової стійкості підприємств у складних економічних умовах [4, с. 115].

Цифровізація приносить низку переваг для бізнесу: оптимізація витрат і роботи персоналу; розширення клієнтської бази; прискорення процесів надання послуг; підвищення рівня інформаційної безпеки підприємств і їх споживачів; збільшення обсягів і темпів передачі інформації.Цифрова епоха змінює метод наближення бізнесу та вимоги до використовуваних інформаційних технологій: системи маркетингу, продажів та обслуговування, системи управління документами та управління персоналом, бухгалтерських систем та інших бізнес-програм. Для забезпечення успішного розвитку цифрової економіки та звуження розриву із іншими країнами, Україні потрібна стратегія цифровізації економіки, яка враховуватиме значну структурну та технічну відсталість порівняно з розвиненими країнами [5].

Підводячи підсумок, зазначимо, що цифрова трансформація підприємств стала критичним фактором їх адаптації та виживання в умовах війни [6, с. 87]. Ті компанії, які впровадили цифрові технології, змогли

зберегти конкурентоспроможність та оперативно адаптуватися до нових умов. Цифровізація є безальтернативним шляхом розвитку бізнесу в умовах висококонкурентних ринків і воєнної агресії [3]. У зв'язку з цим, розгляд цифрової економіки та економічної безпеки в контексті управління підприємствами в умовах війни та післявоєнної відбудови є надзвичайно актуальним для забезпечення їх стійкості та розвитку.

Список використаних джерел:

1. Цифрова трансформація промислового менеджменту: теорія і практика : монографія / за ред. д. філософ. н., проф. В. Г. Воронкової, д. е. н., проф. Н. Г. Метеленко. Львів – Торунь : Liha-Pres, 2023. 816 с.
2. Діяльність вітчизняних підприємств під час війни в Україні: дослідження реального стану та потреб. Публікацію розроблено Центром ресурс ефективного та чистого виробництва за результатами опитування, виконаного у липні 2022 року. URL: http://www.recpc.org/wp-content/uploads/2022/11/National_businesses_during-war_2022.pdf.
3. Котелевець Д. О. Тенденції розвитку цифрової економіки в Україні. *Проблеми сучасних трансформацій. Серія: економіка та управління.* 2022. № 5. URL: https://doi.org/10.54929/2786-5738-2022-5-03- 01
4. Сергієнко Т. І., Крайнік О. М., Куріс Ю. В. Цифрова трансформація системи управління промислових підприємств. Цифрова трансформація промислового менеджменту: теорія і практика : монографія за ред. д. філософ. н., проф. В. Г. Воронкової, д. е. н., проф. Н. Г. Метеленко. Львів – Торунь : Liha-Pres, 2023. С. 111–172.
5. Цифрова адженда України – 2020. URL: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf.
6. Шостак Л. В., Ліпич Л. Г., Морохова В. О., Миронова Н. С. Особливості формування маркетингової стратегії розвитку підприємства в умовах цифрової трансформації, економіко-політичних змін та воєнного часу. *Трансформаційна економіка*. 2023. Випуск 4. С. 86–90.

УДК 334.012

ОГЛОБЛІНА ВІКТОРІЯ ОЛЕКСАНДРІВНА,
к.е.н., доцент, доцент кафедри інформаційної економіки,
підприємнитцва та фінансів
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: va.ogloblina@gmail.com
ORCID ID: http://orcid.org/0000-0001-6627-0255

ЗАГОРОДНІЙ СЕРГІЙ АНАТОЛІЙОВИЧ,
аспірант спеціальності 073 «Менеджмент»
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: zahorodnii@znuiepf.com.ua
ORCID ID: http://orcid.org/0009-0001-0848-7592

МАЗНЄВА ЄЛИЗАВЕТА СЕРГІЇВНА,
здобувач ступеня вищої освіти магістрського рівня, гр. 8.0723-удмф
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail:chernovol.0512@gmail.com

СТРАТЕГІЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ НА ШЛЯХУ ДО ЄС

Тема економічної безпеки України є надзвичайно актуальною в умовах воєнного стану. Економічна безпека – це стан національної економіки, який дає змогу зберігати стійкість до внутрішніх та зовнішніх загроз, забезпечувати високу конкурентоспроможність у світовому економічному середовищі і характеризує здатність національної економіки до сталого та збалансованого зростання. Економічна безпека надає можливість вчасно здійснювати державний контроль над потенційними загрозами економічних інтересів держави, що зміцнює стійкість національної економіки.

Конституція України зазначає: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу». Держава виступає головним суб'єктом національної економічної та інформаційної безпеки та забезпечує виконання покладених на неї функцій через органи законодавчої, виконавчої та судової влади [1].

Стратегія економічної безпеки України визначає шляхи досягнення цілей і реалізації пріоритетів національних інтересів у сфері забезпечення економічної безпеки. Національним інтересам України відповідає сталий розвиток національної економіки, інтеграція України в європейський економічний простір, розвиток рівноправного взаємовигідного економічного співробітництва з іншими державами [2].

Забезпечення національних економічних інтересів вимагає формування і реалізації стратегічного курсу у сфері забезпечення економічної безпеки, спрямованого як на стале нарощення конкурентоспроможності економіки України, так і на поступове зміцнення економічної стійкості та відповідно невразливості національної економіки до зовнішніх і внутрішніх загроз. Отже, стратегічний курс у сфері забезпечення економічної безпеки має два взаємопов'язаних напрями – напрям розвитку та безпековий напрям.

Важливе місце в безпековому напрямі займають виклики, пов'язані із збройною агресією Російської Федерації та тимчасовою окупацією частини території України. Руйнування економіки України є свідомою і цілеспрямованою дією Російської Федерації та одним з методів гібридної війни, оскільки зруйнована економіка продукує незадоволеність владою, трудову міграцію, соціальну напругу в суспільстві та підриває довіру до влади. При цьому широко використовуються економічні інструменти впливу, до яких, зокрема, відносяться санкції щодо українських товарів і послуг та використання впливу на інші держави з метою прийняття рішень, що суперечать основним національним економічним інтересам України [2].

Очікуваним результатом виконання Стратегії є забезпечення економічної безпеки держави як умови забезпечення національних економічних інтересів.

У контексті забезпечення національних економічних інтересів України реалізація Стратегії зорієнтована на:

– створення стійкої, конкурентоспроможної, соціально відповідальної ринкової економіки та умов для випереджаючого розвитку науково-технічного потенціалу країни, сталого нарощування національного багатства та факторів виробництва;

– досягнення Цілей сталого розвитку України на період до 2030 року, затверджених Указом Президента України від 30 вересня 2019 року № 722, рівня життя населення та соціально-політичної стабільності, притаманних економічно розвиненим країнам;

– зайняття Україною у світовому розподілі праці та міжнародних економічних відносинах місця, яке відповідає її природним, трудовим та інтелектуальним ресурсам, економічному та геополітичному потенціалу;

– забезпечення гарантованого захисту національної економіки в умовах виникнення або посилення внутрішніх та зовнішніх загроз [2].

Надзвичайно актуальною проблемою сьогодення в Україні є корупція, яка впливає на економічні та соціальні показники держави. Корупція – це використання публічним службовцем повноважень чи можливостей з метою одержання неправомірної вигоди, прийняття такої вигоди, прийняття обіцянки/пропозиції вигоди для себе чи інших осіб або обіцянка/пропозиція чи надання неправомірної вигоди публічному службовцю, або на його вимогу іншим фізичним чи юридичним особам з метою схилити цю особу до протиправного використання служебних повноважень чи пов'язаних з ними можливостей.

Спеціально уповноважені суб'єкти у сфері протидії корупції – органи прокуратури, Національної поліції, Національне антикорупційне бюро України, Національне агентство з питань запобігання корупції [3].

Політика, яку проводить держава у сфері протидії корупції, впливає на стан та динаміку корупції, що, в свою чергу, призводить до дисбалансу у соціальній, психологічній та економіко-правовій сферах відносин.

За даними соціологічних досліджень, 73 % громадян України вважають корупцію найбільшою проблемою нашої держави. Але реальна цифра українців, які стикаються з корупцією – 19 %. Ці цифри свідчить про жагу українського суспільства жити в державі без корупції.

За словами Голови НАЗК, це комплексна робота всіх державних інституцій щодо реформування сфер для усунення корупційних ризиків, цифровізація процесів для усунення людського фактору, розбудова доброчесного суспільства та адаптація законодавства до стандартів ЄС. Крім того, надзвичайно важливо залучати представників проактивного громадянського суспільства та журналістів.

За його словами, важливою є співпраця з міжнародними партнерами, зокрема з Організацією економічного співробітництва та розвитку (ОЕСР), яка об'єднує 38 найрозвиненіших країн світу. Завдяки цьому, ми отримуємо доступ до найкращих світових практик і інструментів для побудови системи доброчесного публічного управління. Україна стала першою країною не членом ОЕСР, яка долучиться до ініціативи «Індикатори публічної доброчесності».

НАЗК продовжує активну роботу в частині участі в переговорній процедурі між Україною та ЄС шляхом реалізації Антикорупційного мейнстріму, який є вимогою Єврокомісії та полягає в наявності блоку запобігання та боротьби з корупцією в кожному розділу переговорної процедури [4].

На зовнішньоекономічну безпеку України в умовах воєнного стану впливає участь держави у Міжнародних організаціях (МО). З початку повномасштабної військової агресії росії завдяки підтримці МВФ Україні вдалось забезпечити фінансову та макроекономічну стабільність.

Допомога надавалась у рамках різних інструментів (Інструмент швидкого фінансування (Rapid Financing Instrument – RFI) та Механізм розширеного фінансування (Extended Fund Facility – EFF), а також на пільговій та грантовій основі від міжнародних партнерів через спеціально створений Адміністративний рахунок МВФ [5].

Україна з 1994 р. активно співпрацює з МВФ, використовуючи його фінансові і технічні ресурси з метою досягнення макроекономічної стабілізації та створення необхідних передумов для проведення економічних реформ. Програми МВФ надавали можливість Україні забезпечити посилення фіскальної та фінансової стабільності, поступово запроваджувати структурні реформи та спрямувати Україну шляхом стабільного та збалансованого зростання [5].

Намагаючись посилити свої позиції у протистоянні з росією, Україна активно співпрацює з міжнародними організаціями (ООН, ЄС, НАТО, ОБСЄ, Радою Європи), які зробили низку солідарних кроків на підтримку Української держави.

За даними Міністерства закордонних справ (МЗС), станом на 1 січня 2022 року Україна є членом 81 міжнародної організації. У більшості з них (69 організацій) Україна має статус повноправного члена. Це дає нашій країні право брати участь у роботі МО на постійній основі, зокрема голосувати на засіданнях, формувати порядок денний, готувати стратегії розвитку, розробляти спільно з іншими учасниками організації міжнародні документи, імплементувати стандарти, розроблені в межах компетенції організації, тощо [6].

Отже, стратегія економічної безпеки України в умовах воєнного стану визначає шляхи досягнення цілей і реалізації пріоритетів національних інтересів у сфері забезпечення економічної безпеки. Національним інтересам України відповідає сталий розвиток національної економіки, інтеграція України в європейський економічний простір, розвиток рівноправного взаємовигідного економічного співробітництва з іншими державами

Список використаних джерел:

1. Метеленко Н. Г., Глущевський В. В., Клопов І. О., Оглобліна В. О., Нетяга А. В., Нетяга А. В. Ідентифікація фінансово-економічних ризиків та цифрова трансформація повоєнного відновлення промислових підприємств Запорізького регіоную. *Цифрова трансформація промислового менеджменту у контексті викликів, можливостей та змін* : монографія / за ред. д.філософ.н., проф В. Г. Воронкової, д.е.н., проф. Н. Г. Метеленко. Львів – Торунь : Liha-Pres, 2024. С. 198–249.

2. Указ президента України «Про рішення Ради національної безпеки і оборони України від 11 серпня 2021 року «Про Стратегію економічної безпеки України на період до 2025 року»» № 347/2021 від 11 серпня 2021 року. URL: https://zakon.rada.gov.ua/laws/show/347/2021#Text (дата звернення: 13.11.2024).

3. «Запобігання корупції». Національна соціальна сервісна служба України. URL: https://nssu.gov.ua/zapobigannya-korupciyi (дата звернення: 13.11.2024).
4. URL: https://nazk.gov.ua/uk/novyny/koruptsiya-ne-nash-spadok-tomu-maemo-vprovadyty-systemni-zminy-aby-ne-peredaty-yogo-nastupnym-pokolinnyam-golova-nazk/ (дата звернення: 13.11.2024).
5. «Співробітництво України з міжнародними фінансовими інституціями» – Міністерство закордонних справ України. URL: https://mfa.gov.ua/mizhnarodni-vidnosini/spivrobitnictvo-ukrayini-z-mizhnarodnimi-finansovimi-instituciyami (дата звернення: 14.11.2024).
6. Єдиний державний реєстр Міжнародних організацій, членом яких є Україна. URL: https://mfa.gov.ua/mizhnarodni-vidnosini/uchast-u-mizhnarodnih-organizaciyah (дата звернення: 14.11.2024).

УДК 338.2

ОГЛОБЛІНА ВІКТОРІЯ ОЛЕКСАНДРІВНА,
к.е.н., доцент, доцент кафедри інформаційної економіки,
підприємництва та фінансів
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: va.ogloblina@gmail.com
ORCID ID: http://orcid.org/0000-0001-6627-0255

МОРГУН КАТЕРИНА СЕРГІЇВНА,
бакалавр гр. 6.0721-фдпс
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: kataass03@gmail.com

БАЛХОВІТІН ВЛАДИСЛАВ ЕДУАРДОВИЧ,
магістр гр. 41МК
Таврійський державний агротехнологічний університет ім. Дмитра Моторного
(м. Запоріжжя, Україна)

ФІНАНСОВА БЕЗПЕКА УКРАЇНИ У ЦИФРОВОМУ ПРОСТОРІ В УМОВАХ ЄВРОІНТЕГРАЦІЙНИХ ПРОЦЕСІВ

У сучасному світі стрімка цифровізація торкається майже всіх сфер суспільного життя. Різні сектори, включаючи економічний, інформаційний, воєнний та енергетичний, інтегруються в цифровий простір, що

надає нові можливості, але водночас і відкриває численні ризики. Питання безпеки стають нагальною проблемою, оскільки кіберзагрози і атаки на критичну інфраструктуру можуть мати руйнівні наслідки для держави, бізнесу та громадян. В умовах війни суттєвою проблемою є необхідність збереження фінансово-економічної безпеки України.

Євроінтеграційні процеси стали ключовим фактором для України у визначенні її місця на світовій арені та забезпеченні її економічної безпеки. Відповідно до «Методики розрахунку рівня економічної безпеки України» складовими забезпечення економічної безпеки є: макроекономічна, фінансова, зовнішньоекономічна, інвестиційна, науково-технологічна, енергетична, виробнича, демографічна, соціальна, продовольча безпека [1].

Фінансова складова економічної безпеки дуже важлива для України серед інших складових, оскільки ринки Єврозони можуть вплинути на ще більше зниження темпів зростання ВВП, вплинути на монетарну та валютну безпеки держави. Як мінімум, девальвація євро проти основних валют (долар США, японська єна та швейцарський франк) означає, що українські експортери стануть менш конкурентоспроможними на європейському ринку. Навіть при збереженні природних обсягів продажів вони втратять у доларовому еквіваленті. Девальвація як фунту, так і євро негайно вплине на проблеми в банківському секторі, що вимагатиме значної рекапіталізації. За цих умов надзвичайно важливою є проблема захисту національних інтересів у фінансовому секторі та забезпечення фінансової безпеки держави [2].

Індикатори фінансової безпеки відображають специфіку певного рівня управління (громадян, домашніх господарств, підприємств, організацій і установ, галузі господарського комплексу, регіонів, банківської системи, фондового ринку, держави) або таких її складових, як безпека грошового обігу, інфляційна, валютна, бюджетна, боргова й інвестиційна безпека.

У Європейському Союзі існує система фінансових критеріїв (відповідно до Маастрихських угод), яким повинні відповідати країни учасниці та кандидати на вступ до ЄС.

Більшість показників фінансової безпеки у ЄС та України мають ідентичні критичні значення, що, з одного боку, сприяє можливій інтеграції України у європейське співтовариство, а з іншого, не враховує особливості вітчизняної економіки як перехідної та такої, що розвивається.

На основі багаторічного досвіду міжнародні інститути, зокрема МВФ, розробили систему показників, за допомогою яких оцінюють стан фінансової безпеки країни та прогнозують майбутній розвиток. Окрім загальноприйнятих, МВФ розраховує показник ВВП на душу населення, індекс

покриття експорту імпортом, індекс відкритості економіки та ін. показники фінансової безпеки.

Наприклад, до індикаторів фінансової безпеки за складовою «безпека банківського сектору» віднесено:

– частка іноземного банківського капіталу в загальному обсязі банківського капіталу, %;

– обсяг кредитування банками реального сектору економіки,% до ВВП.

Безпека банківської системи є насамперед складовою фінансової безпеки держави, яка визначається більшістю вчених як такий стан фінансової, грошово-кредитної, валютної, банківської, бюджетної, податкової систем, що характеризується збалансованістю, стійкістю до негативних впливів, спроможністю забезпечити ефективне функціонування національної економічної системи та її зростання.

Фінансово-економічна безпека включає захист національних і міжнародних фінансових систем від кіберзагроз. З розвитком електронної комерції, банківських операцій онлайн і цифрових валют, економічна система стала більш вразливою до хакерських атак і шахрайства. Основні механізми мінімізації ризиків у цій сфері включають:

– зміцнення кібербезпеки фінансових установ: банківські та фінансові організації повинні впроваджувати сучасні технології захисту даних, такі як багатофакторна автентифікація, шифрування і моніторинг транзакцій у режимі реального часу;

– використання штучного інтелекту для виявлення шахрайства: алгоритми штучного інтелекту дозволяють відстежувати підозрілі операції та реагувати на них швидше, ніж це можливо за допомогою традиційних методів контролю;

– підвищення обізнаності користувачів: фінансові установи повинні інформувати своїх клієнтів про можливі загрози та навчати безпечним методам ведення онлайн-фінансових операцій, щоб зменшити ризик соціальної інженерії та фішингових атак.

Ці заходи сприяють зменшенню ризику економічних втрат та забезпечують стабільність фінансової системи в умовах зростаючої цифровізації.

Євроінтеграційні процеси дозволяють Україні отримати доступ до європейських ринків та інвестицій. Це стимулює економічний зріст, сприяє розвитку підприємництва та підвищенню конкурентоспроможності українських компаній, що створює передумови для зростання ВВП та стійкості фінансово-економічного середовища. Крім того, євроінтеграція забезпечує Україні можливість використовувати європейські стандарти та норми, що сприяє модернізації галузей економіки та підвищенню їх якості. При вступі до Європейського Союзу Україна може отримати

доступ до додаткових фінансових ресурсів, технічної та експертної підтримки, що допоможе зменшити боргове навантаження та зміцнити фінансову систему [3].

Отже, фінансова безпека є однією з найважливіших складових економічної безпеки. Це своєрідний індикатор і критерій ефективності діяльності фінансової системи держави. Без забезпечення фінансової безпеки практично неможливо вирішити жодне із завдань, що стоять перед Україною.

Для досягнення високого рівня безпеки в умовах цифровізації важливо використовувати адаптивні механізми та поєднувати технічні, організаційні та просвітницькі підходи. Це дозволить знизити вразливість суспільства до ризиків цифрового простору і забезпечити стійкість критичних сфер національної безпеки та зміцнити стійкість держави до сучасних загроз у світі, де цифровий простір відіграє ключову роль у безпеці кожної країни.

Завершення війни та перемога у ній є критичними умовами для подальшого розвитку України як демократичної та економічно стабільної країни, готової до інтеграції зі світовим співтовариством, зокрема з Європейським Союзом.

Список використаних джерел:

1. Metelenko N. G., Klopov I. O., Ogloblina V. O. Instruments for ensuring the financial stability of the state during war. Science of XXI century: development, main theories and achievements : collection of scientific papers "SCIENTIA" with Proceedings of the VII International Scientific and Theoretical Conference, November 15, 2024. Helsinki, Republic of Finland: International Center of Scientific Research, 2024. 332 p. P. 30–33.

2. Пойда-Носик Н. Н. Фінансова безпека України в умовах Європейської інтеграції. *Науковий вісник Полісся*. 2017. № 1(9) (дата звернення: 17.11.2024).

3. Метеленко Н. Г., Глущевський В. В.,Клопов І. О., Оглобліна В. О., Нетяга А. В., Нетяга А. В. Ідентифікація фінансово-економічних ризиків та цифрова трансформація повоєнного відновлення промислових підприємств Запорізького регіону. *Цифрова трансформація промислового менеджменту у контексті викликів, можливостей та змін* : монографія / за ред. д.філософ.н., проф В. Г. Воронкової, д.е.н., проф. Н. Г. Метеленко. Львів – Торунь : Liha-Pres, 2024. 592 с. С. 198–249.

УДК 004.9:330.34:336.02(477)

ОГЛОБЛІНА ВІКТОРІЯ ОЛЕКСАНДРІВНА,
к.е.н., доцент, доцент кафедри інформаційної економіки,
підприємнитцва та фінансів
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: va.ogloblina@gmail.com
ORCID ID: http: orcid.org/0000-0001-6627-0255

МЕТЕЛЕНКО НАТАЛЯ ГЕОРГІЇВНА,
д.е.н., проф., директор
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: natalia.metelenko@gmail.com
ORCID ID: http: orcid.org/0000-0002-6757-3124

БУЦ ОЛЕКСІЙ ВАДИМОВИЧ,
здобувач вищої освіти спеціальності 072, другий освітній рівень «магістр»,
кафедра ІЕПФ
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)

ЦИФРОВА ТРАНСФОРМАЦІЯ ЕКОНОМІКИ ЯК ІНСТРУМЕНТАРІЙ ФІНАНСОВОЇ СТІЙКОСТІ ДЕРЖАВИ

Цифрова трансформація економіки продовжує відігравати критично важливу роль в інтеграції України до європейського цифрового простору, у впровадженні інноваційних технологій під час війни та підвищенні стійкості держави. Серед важливих подій цифрової трансформації економіки в поточному 2024 році варто виділити такі: інтеграція України до європейського цифрового простору; міжнародна підтримка України під час повномасштабної війни; посилення уваги до штучного інтелекту; розвиток статистичних спостережень.

Так, Україна досягла вагомих результатів у впровадженні європейських цифрових стандартів; отримала максимальні оцінки за імплементацію Європейської рамки взаємодії (European Interoperability Framework) про що свідчить Digital Public Administration factsheets – 2024. Одним із ключових пріоритетів України є взаємне визнання електронних довірчих послуг між Україною та ЄС, для чого проведені необхідні законодавчі зміни і Європейський Союз високо оцінив відповідність України

реформам у цій сфері. Водночас слід зауважити, що право ЄС динамічно розвивається і відображення цих змін в українському законодавстві є необхідною умовою подальшої інтеграції у європейський цифровий простір. До планів на найближчі роки щодо доступності державних послуг віднесено процеси відновлення та модернізація центрів надання адміністративних послуг (ЦНАП), які були зруйновані чи пошкоджені внаслідок війни, а також перетворення їх на інклюзивні та цифрові офіси для забезпечення рівного доступу для всіх громадян. Запровадження таких заходів поліпшить надання електронних послуг і забезпечить повну взаємодію з цифровими системами ЄС [1].

Також, досягнуто значного прогресу в упровадженні е-довірчого списку послуг між Україною та ЄС [2]. Ці послуги спрощують створення, перевірку й валідацію електронних підписів і цифрових сертифікатів з країн Європейського Союзу та додають іноземних провайдерів до списку довірених осіб Центрального засвідчувального органу України. Проте визнання іноземних сертифікатів відкритих ключів, електронних підписів, а також їх використання під час взаємодії між суб'єктами різних держав потребує нових інноваційних рішень щодо інтеграції України у світовий цифровий інформаційний простір. Україна активно рухається у напрямі повної цифровізації державних послуг, що сприяє інтеграції до цифрового простору ЄС, зміцнює економічний потенціал через взаємне визнання електронних довірчих послуг між Україною та ЄС. Наша держава приєдналася до консорціуму Potential, який працює над розробкою європейського гаманця цифрової ідентичності (European Digital Identity Wallet, EUDI).

Впровадження законодавчих змін у сфері зміцнення економічного потенціалу та правових основ функціонування електронної комунікаційної мережі з використанням інноваційних технологій потребує координації заходів і приведення їх у відповідність до норм, передбачених Законом України «Про електронні комунікації» [3]. Розробка програмних інтерфейсів для електронної інформаційної взаємодії з державними органами дозволить здійснювати передбачені чинним законодавством верифікацію та підтвердження даних пільгових категорій громадян, актуалізацію адресної інформації й надання даних про осіб з інвалідністю тощо. Для відновлення телекомунікаційного сектора, який зазнав мільярдних збитків від початку повномасштабного вторгнення, поліпшення якості мобільного зв'язку, збільшення покриття фіксованим і мобільним інтернетом в Україні Міжнародна фінансова корпорація (IFC) і ЄБРР за підтримки Європейської комісії та уряду Франції 10 жовтня 2024 р. підписали договір про спільне фінансування в розмірі 435 млн дол. США. Також у жовтні місяці поточного 2024 року на засіданні Українсько-швейцарського

спільного економічного комітету розглядалися актуальні питання залучення стратегічних інвестицій у реалізацію спільних українсько-швейцарських проєктів, розвиток інновацій та спільні ініціативи для відбудови України; обговорювалися можливості співпраці в інженерії та виробництві напівпровідників, у галузі автономних транспортних засобів на наступні п'ять років і можливості в IT-індустрії, пов'язані з розвитком Глобальної інноваційної візії України. На цифровізацію публічного управління та розвиток регіонів України уряд Швейцарії планує виділити 58,7 млн швейцарських франків, зокрема, на цифрову трансформацію соціально важливих сфер державної політики й цифровий розвиток громад протягом 2024–2028 рр. Проєкти реалізовуватимуться у межах програми «Електронне урядування задля підзвітності влади та участі громади» (далі – Програма EGAP), що виконується Фондом Східна Європа [4]. Слід зазначити, що це вже третій проєкт, який Україна реалізовує за підтримки уряду Швейцарії в рамках підписаного меморандуму; Програма EGAP бере початок у 2015 році, і за весь час швейцарський уряд виділив понад 30 млн франків. Зокрема, меморандум передбачає реалізацію реформ у сфері охорони здоров'я, соціальній політиці, освіті, гуманітарному розмінуванні, житлово-комунальних послугах, державній статистиці та реформі державного управління. Завдяки цифровій трансформації громадяни України отримують публічні послуги швидко, прозоро й безпечно. Цифровізація стала важливим каталізатором реформ, які необхідні для відновлення, відбудови й сталого розвитку України. Крім того, у фокусі взаємодії в рамках Програми EGAP – цифровий розвиток та підвищення стійкості громад. Так, у межах меморандуму Швейцарія підтримуватиме місцеве самоврядування в 9 областях України: Чернігівській, Дніпропетровській, Херсонській, Хмельницькій, Луганській, Одеській, Сумській, Вінницькій, Волинській, а регіони отримають цифрові інструменти та знання, необхідні для покращення надання послуг. Також Програма EGAP спрямована на підтримку українців, які постраждали внаслідок повномасштабного вторгнення, зокрема, ВПО, осіб з інвалідністю і жителів раніше окупованих територій. Передбачається відновлення цифрової інфраструктури та створення доступного й енергонезалежного середовища для надання публічних послуг. Такий комплексний підхід є важливим для відновлення й розвитку громад, а також забезпечення інклюзивного цифрового доступу.

У межах реалізації проєкту EU4DigitalUA Міністерство цифрової трансформації України оприлюднило документ «Права людини в епоху штучного інтелекту: виклики та правове регулювання» [5], що містить рекомендації для бізнесу та державних органів під час застосування ШІ, а також аналіз регулювання ШІ в ЄС та США. Документ «Права людини

в епоху штучного інтелекту: виклики та правове регулювання» є методичним документом, у якому йдеться про вплив передових технологій ШІ та підходи до його правового регулювання; у ньому також надаються рекомендації щодо управління інтелектуальною системою відповідно до національного законодавства та міжнародних стандартів.

В документі зазначається, що сьогодні штучний інтелект використовується практично у всіх сферах людської діяльності. Передові технології можуть виконувати різноманітні завдання: керувати транспортними засобами, виробничими процесами на підприємствах, генерувати текст, музику, розпізнавати обличчя та голоси, виступати персональними помічниками на смартфоні та багато іншого. Вони інтегровані в різні пристрої, які щодня використовуються в уряді, в політиці, в міській інфраструктурі, бізнесі або просто в повсякденному житті. Незважаючи на широкі суспільні перспективи, які можуть створити інтелектуальні системи, увага також повинна бути спрямована на етичні та правові аспекти їх використання, зокрема вплив на права і свободи людини. Розуміння принципів, якими повинні керуватися розробники й компанії, що працюють із ШІ, важливі для побудови довіри до електронних сервісів в Україні. Рекомендації у сфері захисту персональних даних допоможуть зміцнити поінформованість та запобігти порушенням права на приватність. Ці настанови представляють собою наступний крок до комплексного регулювання штучного інтелекту в Україні.

Учасники Програми EU4Digital оцінили українську платформу Цифрової екосистеми для підзвітного управління відновленням (DREAM) і виявили, що вона ефективно підтримує потреби громад у реконструкції. Також EU4Digital підготувала «дорожню карту» для вдосконалення платформи DREAM, яка є ключовим компонентом цифрової трансформації для підтримки довіри та підзвітності під час реконструкції та відновлення України. Успішна оцінка платформи DREAM свідчить про ширшу відданість просуванню цифрового управління та кібербезпеки в Україні. Очікується, що DREAM, як прозора та безпечна система, відіграватиме важливу роль у поточних зусиллях із відновлення країни, надаватиме можливість громадам ефективно відновлюватися та дозволятиме міжнародним донорам впевнено розподіляти ресурси. Крім того, методології та рамки цифрової довіри, застосовані в оцінці DREAM, можуть слугувати моделлю для інших систем управління державними фінансами в Україні, що сприятиме ширшій інтеграції країни в європейську цифрову екосистему [6].

15 жовтня 2024 р. Кабінет Міністрів України затвердив план державних статистичних спостережень на 2025 р. [7], зокрема щодо використання інформаційно-комунікаційних технологій (ІКТ) на підприємствах, що

сприятиме формуванню інформації про впровадження підприємствами цифрових технологій для інформаційного забезпечення аналізу розвитку ІКТ та електронної торгівлі. Такі заходи є незмінним поступом України до імплементації законодавства ЄС, обміну даними на основі європейської методології [8] та затвердженого для України переліку показників Індексу цифрової економіки й суспільства (DESI) [9]. Так, у Європейській статистичній системі (ESS) Vision 2020 зазначено, що дані слід використовувати в усіх статистичних сферах для кращого аналізу нових явищ (наприклад, глобалізації) і для кращого обслуговування політики Союзу, яка має великий вплив. Вихідні дані повинні ґрунтуватися на ефективних та надійних статистичних процесах ESS. Ширший обсяг загальної правової бази для бізнес-статистики повинен забезпечити інтеграцію взаємозалежних виробничих процесів із використанням багатьох джерел [10].

Висновки та рекомендації. Цифрова трансформація економіки України впродовж 2024 р. набула подальшого розвитку щодо впровадження європейських цифрових стандартів та цифрових технологій у всіх сферах економіки. Бізнес та урядові структури здійснюють заходи щодо імплементації й узгодженості процесів інтеграції України до цифрового простору ЄС. Вищеокреслені зміни демонструють стратегічну важливість цифрової трансформації економіки для забезпечення стійкості, підтримки та взаємодії з цифровими системами ЄС в умовах війни й повоєнного відновлення; спрямовані на розвиток онлайн-послуг, інструментів електронної демократії та цифровізація регіонів.

Список використаних джерел:

1. Переговори щодо вступу України в ЄС: Україна зустрілась з Європейською Комісією. URL: https://thedigital.gov.ua/news/peregovori-shchodo-vstupu-ukraini-v-es-ukraina-zustrilas-z-evropeyskoyu-komisieyu (дата звернення: 19.11.2024).

2. Кабмін ухвалив постанову про е-довірчий список послуг між Україною та ЄС. URL: https://jurliga.ligazakon.net/news/230912_kabmn-ukhvaliv-postanovu-pro-e-dovrchiy-spisok-poslug-mzh-ukranoyu-ta-s (дата звернення: 02.10.2024).

3. Про електронні комунікації. Закон України від 01.07.2024 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 02.10.2024).

4. Швейцарія виділяє 58,7 млн франків на цифровізацію публічного управління та розвиток регіонів України: Мінцифра й Уряд Швейцарії підписали меморандум. URL: https://www.eda.admin.ch/countries/ukraine/fr/home/actualite/nouveautes.html/content/countries/ukraine/uk/meta/news/2024/september/Switzerland-signed-a-memorandum-with-the-Ministry-of-Digital-Transformation-of-Ukraine (дата звернення: 07.10.2024).

5. Права людини у сфері штучного інтелекту: виклики та правове регулювання. URL: https://eufordigital.eu/uk/library/human-rights-in-the-area-of-artificial-intelligence-challenges-and-legal-regulation/ (дата звернення: 02.10.2024).

6. Побудова цифрової довіри у відновленні України: оцінка платформи DREAM Програмою EU4Digital. URL: https://eufordigital.eu/uk/building-digital-trust-in-ukraines-recovery-eu4digital-dream-platform-assessment/ (дата звернення: 19.10.2024).

7. Про затвердження плану державних статистичних спостережень на 2025 рік : Розпорядження Кабінету Міністрів України від 15.10.2024 № 1003-р. URL: https://www.ukrstat.gov.ua/norm_doc/proekt/proekt_23.05.2024/plan.pdf

8. Regulation (EU) 2019/2152 of the European Parliament and of the Council of 27 November 2019 on European business statistics, repealing 10 legal acts in the field of business statistics (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2019/2152/oj (дата звернення):

9. Про затвердження переліку показників Індексу цифрової економіки та суспільства (DESI) : Розпорядження Кабінету Міністрів України від 05.09.2023 № 774-р. URL: https://zakon.rada.gov.ua/laws/show/774-2023-%D1%80#Text (дата звернення: 10.10.2024).

10. Регламент (ЄС) 2019/2152 Європейського Парламенту та Ради від 27 листопада 2019 року про європейську бізнес-статистику, що скасовує 10 правових актів у сфері бізнес-статистики (текст стосується ЄЕЗ). URL: https://eur-lex.europa.eu/eli/reg/2019/2152/oj (дата звернення: 10.10.2024).

УДК 330.34

ПАРШИН ЮРІЙ ІВАНОВИЧ,
д.е.н., проф. кафедри інформаційної економіки, підприємництва та фінансів
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: parshin22@ukr.net
ORCID ID: http: orcid.org/0000-0002-8650-5303

ОЛЄНІЧЕНКО ВОЛОДИМИР ПЕТРОВИЧ,
аспірант кафедри інформаційної економіки, підприємництва та фінансів
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)

КОРПОРАТИВНЕ УПРАВЛІННЯ ПРОМИСЛОВИМ ПІДПРИЄМСТВОМ У ЦИФРОВІЙ ЕКОНОМІЦІ

Під корпоративним управлінням розуміють таке управління бізнес-діяльністю коли здійснюється грамотний розподіл результатів цієї діяльності між усіма заінтересованими сторонами. Основна мета

ефективного корпоративного управління – підвищення інвестиційної привабливості підприємства та, відповідно, зростання капіталізації. У разі ефективного корпоративного управління акціонери можуть здійснювати необхідний моніторинг за діяльністю менеджменту, що передбачає опрацювання та впровадження нових внутрішніх процедур управління та застосування зовнішніх правових та регуляторних інструментів. Також акціонери вважають за краще мати повну та достовірну інформацію про розподіл відповідальності топ-менеджерів за діяльність підприємства. Одночасно з цим особам, які фінансують бізнес-діяльність, важливою є можливість участі у прийнятті стратегічних рішень. Моніторингові процеси добре здійснювати у разі коли інформація про діяльність організації, її показники, відображаються у цифровому форматі. Отже, відцифрувати всю інформацію для прийняття будь-яких рішень є питанням і задачею досить актуальною.

Корпоративне управління групами бізнес-систем визначає різні аспекти відносин, що виникають між великими економічними об'єктами у процесі розподілу ринкових зон впливу та зон відповідальності за менеджмент. Такі дії унеможливлюють конфлікт інтересів бізнес-систем, які здійснюють господарську діяльність у складі загальної корпорації.

Теоретичним та методологічним аспектам впровадження цифрових технологій в організаціях присвячено наукові роботи Мокера М., Молоні К., Росса Дж. та інших. Використання цифрових технологій в менеджменті розглядали такі науковці як Баранов В. В., Коляденко С. В., Калетнік Г. М., Гунько І. В., Жуковська В. М. та інші. Поряд з цим окремі питання цифровізації групи бізнес-систем залишаються не достатньо дослідженими.

Метою дослідження є розгляд задач організації корпоративного управління групами бізнес-систем, які здійснюють промислову діяльність у парадигмі індустрії 4.0 та орієнтованих на один сегмент ринку в контексті цифровізації бізнес-процесів.

Ускладнення економічних процесів і сучасний стан економічної системи збільшує актуальність вдосконалення корпоративного управління, переведення процесів управління на цифрову основу та цифровий формат.

На сучасному етапі багато відомих економістів дійшли висновку, що керівництву корпорацій, або інших великих організаційних утворень, необхідно не тільки розвивати ризик-менеджмент та забезпечувати ефективний контроль за управлінням ризиками, а й підвищувати конкурентні переваги своїх компаній, для чого необхідно своєчасно впроваджувати кардинальні цифрові інновації. Це, у свою чергу, змінює самий стиль роботи вищого керівництва корпорацій та підприємств реального сектору економіки. Широкий комплекс інноваційних та інвестиційних проблем,

що пов'язані з реалізацією таких рішень проблем ризику, змушує вище керівництво розробляти та застосовувати принципово нові стандарти співробітництва метою яких є підвищення ефективності загального результату їх роботи [2].

Вченні та економісти-практики виділяють кілька відмінних характеристик, властивих системам корпоративного управління, серед них [1]:

– поєднання власника об'єкта та управління однією особою;

– слабкі механізми контролю за діяльністю організації (найманий керівник підпорядковується, зазвичай, лише провідному акціонеру, а не всім акціонерам);

– низька прозорість операцій, складність в отриманні інформації про реальний фінансовий стан компанії, власників, угод тощо;

– використання незаконних або неетичних методів роботи, серед яких маніпуляції з акціями, недопущення акціонерів на збори, відведення активів тощо.

Зазначимо, що багатьом компаніям також невигідно підвищувати прозорість, оскільки це робить їх уразливими перед контролюючими органами та силовими структурами, незважаючи на те, що існує багато органів які повинні подолати таку ситуацію. Все ще високий рівень корупції зберігає ризик для акціонерів втратити власність через втручання чиновників. Також спостерігається великий розрив між рівнем життя заможних і малозабезпечених людей, звідси – різниця у цінностях та ставлення до цілей компанії.

Також проблемою є дефіцит досвідчених менеджерів. На практиці керівництво організацією часто здійснюють акціонери, які можуть діяти практично безконтрольно, проводити угоди в особистих інтересах, нехтувати фінансовою політикою компанії в цілому, спускати великі обсяги роботи на підлеглих [3].

Зазначимо, що проблеми корпоративного управління пов'язують із відокремленням прав власності від прав управління в умовах розпорошених прав власності між багатьма акціонерами. Корпоративне управління націлене на вирішення таких питань, як:

– представництво інтересів акціонерів;
– надання інформації акціонерам про дії менеджерів;
– розподіл прав між менеджерами та акціонерами;
– застосування механізмів корпоративного контролю.

Слід також звернути увагу на те, що проблема корпоративного управління зводиться до створення механізмів, які забезпечували дотримання інтересів акціонерів, які є власниками корпорації в умовах, коли значуща для прийняття рішень (як поточних, так і стратегічних) інформація

розподілена асиметрично на користь менеджерів, і які часто мають на увазі власні інтереси. А отже, цифровізація інформаційних потоків дозволить оптимізувати виробничі процеси, зробити їх більш відкритими для акціонерів та надасть можливість активного залучення акціонерів до моніторингових процесів. Також зазначимо, що корпоративне управління включає розгляд двох основних питань – це внутрішнє функціонування організації та взаємодія корпорації із зовнішнім середовищем.

До внутрішнього життя корпорації відноситься її створення, ліквідація, права акціонерів, а також компетенції органів управління. Під взаємодією корпорації із зовнішнім середовищем розуміється у першу чергу випуск акцій, облігацій, умови придбання великих пакетів акцій тощо.

У сучасному менеджменті можна виокремити кілька ключових моделей корпоративного управління, серед яких: англо-американська, німецька та японська моделі. Основний момент відмінностей полягає в тому, як побудовано розподіл функцій між радою директорів та виконавчими органами. Крім того, відрізняється і ступінь залучення до управління різних зацікавлених осіб. Формування моделі також багато в чому залежить від особливостей загальної економічної ситуації в країні.

Отже корпоративне управління – це важливий параметр діяльності будь-якої організації, що забезпечує можливість підвищення її ефективності. Це система продуктивної взаємодії вищого управління компанії, ради директорів та стейкхолдерів. Якщо корпоративне управління організовано досить ефективно, воно повною мірою дозволить керівництву компанії визначити механізми формування ключових цілей діяльності організації, тактики їх досягнення та механізмів ефективного контролю. Цифровізація процесів дозволить більш динамічно та ефективно впливати на прийняття рішень та унеможливлює використання спотвореної інформації між всіма учасниками.

Список використаних джерел:

1. Зуб П., Калач Г. Цифровізація бізнес-процесів промислових підприємств. *Економіка та суспільство*, № 26. 2021. URL: https://economyandsociety.in.ua/index.php/journal/article/view/385

2. Обидєннова Т., Васильєв В. Цифрові технології в управлінні підприємством: теоретичний аспект. *Адаптивне управління: теорія і практика.* № 15(30). 2023. URL: https://amtp.org.ua/index.php/journal2/article/view/541

3. Панкратова О. М. Цифровізація як сучасний тренд розвитку менеджменту. *Економіка та суспільство*. № 33. 2021. С. 1–5.

УДК 658.8:004.9

РЕКОТОВ ПЕТРО ВАЛЕНТИНОВИЧ,
к.ю.н., доцент, доцент кафедри інформаційної економіки,
підприємництва та фінансів
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: recotov@meta.ua
ORCID ID: https://orcid.org/ 0000-0002-0378-378X

САВЧЕНКО ДАНИЛО В'ЯЧЕСЛАВОВИЧ,
магістр
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: meelike@ukr.net

ІННОВАЦІЙНА ДІЯЛЬНІСТЬ У СФЕРІ МАЛОГО БІЗНЕСУ В УКРАЇНІ: ПРАВОВІ АСПЕКТИ

Інноваційна діяльність є ключовим фактором економічного розвитку, що стимулює зростання малого бізнесу в Україні. Вона полягає у впровадженні нових або значно покращених продуктів, послуг чи процесів з метою підвищення конкурентоспроможності підприємств. Проте, інноваційна діяльність малого бізнесу має свої особливості, які часто визначаються особливостями правового регулювання.

Законодавство України дає наступне визначення інноваційної діяльності: «діяльність, що спрямована на використання і комерціалізацію результатів наукових досліджень та розробок і зумовлює випуск на ринок нових конкурентоздатних товарів і послуг» [1]. Її результатом є інновації. Науковці по різному трактують зміст терміну «інновація» – від теоретичних до прикладних підходів. В цілому ці підходи варто умовно поділити на дві групи. Одна включає ряд вчених, які розглядають інновацію саме як«процес упровадження нових виробів, технологій, методів організації виробництва і праці та методів управління. Інша група передбачає дослідження інновації як продукту – результату процесів упровадження нової техніки, технології, нового методу [2, с. 10].

Правове регулювання інноваційної діяльності розглядається як комплексна система правових засобів, що регулюють здійснення інноваційної діяльності в Україні. Фундаментальним нормативним документом виступає Закон України «Про інноваційну діяльність», який встановлює базові дефініції, фундаментальні принципи, визначає суб'єктний та об'єктний

склад інноваційної діяльності, а також закріплює правові засади формування інноваційної інфраструктури, включаючи технологічні парки та бізнес-інкубатори [1].

У сфері податкового регулювання запроваджено систему преференцій для суб'єктів господарювання, що провадять інноваційну діяльність, зокрема передбачено звільнення від оподаткування прибутку, отриманого внаслідок реалізації інноваційних проектів, що створює сприятливі умови для активізації інноваційної діяльності малого підприємництва. Законом України «Про державну підтримку малого підприємництва» регламентовано механізми надання державної підтримки суб'єктам малого підприємництва, що здійснюють інноваційну діяльність, через інструменти фінансового забезпечення та сприяння залученню інвестиційних ресурсів [3].

Актуальні проблеми та виклики у сфері інноваційної діяльності малого підприємництва характеризуються комплексом взаємопов'язаних факторів. Першочергову значущість має проблематика недостатності фінансового забезпечення інноваційних проектів. Незважаючи на наявність державних програм підтримки, суб'єкти малого підприємництва в Україні стикаються з суттєвими перешкодами у процесі залучення фінансових ресурсів для реалізації інноваційних ініціатив. Фінансово-кредитні установи демонструють низьку готовність до інвестування в інноваційні проекти через підвищений рівень ризиковості таких вкладень.

Стратегічні напрями розвитку малого підприємництва з урахуванням правового регулювання передбачають імплементацію комплексу взаємопов'язаних заходів. Пріоритетним напрямом визначено формування локальних інформаційно-консультативних центрів підтримки малого підприємництва, функціональне призначення яких полягає у забезпеченні суб'єктів господарювання актуальною інформацією щодо кон'юнктурних параметрів місцевих ринків, доступності матеріально-технічних об'єктів для орендного використання, наявності науково-технічних розробок та інноваційних рішень.

Окрім того, важливим рушієм розвитку малого бізнесу є цифровізація його діяльності, що не може не відобразитись позитивно і на рівні інноваційності економіки в цілому [4, с. 330].

Виходячи із вищезазначеного, на сьогоднішній день актуалізується необхідність активізації впровадження інноваційних технологій, зокрема цифровізації малого бізнесу, через застосування правових інструментів стимулювання, податкового преференціювання та грантового фінансування, що забезпечуватиме розширення можливостей малого підприємництва щодо інноваційного розвитку. Державою запропоновано реалізацію програми формування регіональних ринків інтелектуальної власності з визначенням організаційно-правових механізмів

комерціалізації результатів інтелектуальної діяльності у секторі малого підприємництва, включаючи спрощення процедур патентування, реєстрації торговельних марок та ліцензування технологічних рішень тощо.

Список використаних джерел:

1. Про інноваційну діяльність : Закон України від 04.07.2002 № 40-IV. *Відомості Верховної Ради.* України (ВВР), 2002, № 36, ст. 266. URL: https://iplex360.com.ua/npa.php?code=40-15 (дата звернення: 17.11.2024).

2. Харів П. С. Інноваційна діяльність підприємства та економічна оцінка інноваційних процесів. Тернопіль : Економічна думка, 2003. 326 с.

3. Про державну підтримку малого підприємництва: Закон України. від 19.10.2000 р. № 2063-III. *Відомості Верховної Ради України (ВВР).* 2000. № 51–52. Ст. 447. URL: https://zakon.rada.gov.ua/laws/show/2063-14#Text (дата звернення: 17.11.2024).

4. Церковна А. В., Карелова К. С. Вплив цифровізації на розвиток малого і середнього бізнесу в Україні. *Ринкова економіка: сучасна теорія і практика управління.* 2020. Том 19. Випуск 2(45). С. 328–339. DOI: file:///C:/Users/user/Downloads/201486-Текст%20статті-453750-1-10-20200511%20(1).pdf (дата звернення: 17.11.2024).

УДК 658.8:004.9

РЕКОТОВ ПЕТРО ВАЛЕНТИНОВИЧ,
к.ю.н., доцент, доцент кафедри інформаційної економіки,
підприємництва та фінансів
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: recotov@meta.ua
ORCID ID: https://orcid.org/ 0000-0002-0378-378X

ДЕБЕЛИЙ ВЛАДИСЛАВ СЕРГІЙОВИЧ,
магістр
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: vladdebeluy@dmail.com

ОСОБЛИВОСТІ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ РОЗВИТКУ ПІДПРИЄМНИЦТВА В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

Розвиток підприємництва є ключовим фактором економічного зростання та соціальної стабільності в будь-якій країні. В Україні

ж становлення та функціонування підприємницької діяльності зіткнулося зі значними викликами, які лише посилилися з початком повномасштабної військової агресії з боку Росії. Запровадження воєнного стану, пошкодження інфраструктури, порушення ланцюгів постачання, втрата ринків збуту та інші негативні фактори суттєво ускладнили можливість ведення бізнесу. За таких обставин державі вкрай важливо створити сприятливі правові умови, які допоможуть зберегти та відродити підприємницьку діяльність [1, с. 3].

Огляд нормативно-правових актів, прийнятих в Україні після 24 лютого 2022 року, свідчить про зусилля уряду, спрямовані на підтримку бізнесу в умовах війни, заходи включають спрощення процедур реєстрації бізнесу, надання податкових пільг, запровадження кредитних та грантових програм, а також започаткування проекту з переміщення бізнесу із зон конфлікту. Незважаючи на ці кроки, багато правових питань, пов'язаних з веденням бізнесу в умовах воєнного стану, залишаються невирішеними. Чинне законодавство все ще містить численні прогалини та суперечності, особливо щодо форс-мажорних обставин, статусу раніше укладених контрактів, процедур банкрутства та захисту прав інвесторів. Відсутність чітких правових механізмів створює ризики для бізнесу та перешкоджає залученню інвестицій. Крім того, відновлення ділової активності на деокупованих територіях залишається недостатньо врегульованим. Компанії стикаються з такими проблемами, як необхідність відновлення прав власності, компенсації збитків, кадрове забезпечення та доступ до фінансування. Уряд має розробити ефективні правові інструменти для стимулювання економічної активності в цих регіонах, оскільки оподаткування також створює численні проблеми для бізнесу. Незважаючи на деякі податкові послаблення, загальний фіскальний тягар залишається високим [2, с. 17].

Невизначеність щодо майбутньої податкової політики та непередбачуваність законодавчих змін негативно впливають на довгострокове бізнес-планування. Потрібні більш гнучкі та стимулюючі механізми оподаткування, особливо для малих та середніх підприємств. Крім того, недостатніми є правові інструменти захисту прав суб'єктів господарювання. В умовах дестабілізації верховенства права загострилися такі проблеми, як рейдерство, незаконне втручання контролюючих органів, недобросовісна конкуренція. Держава має забезпечити відповідальність за порушення у сфері підприємницької діяльності, що потребуватиме вдосконалення інституційної інфраструктури підтримки бізнесу. Наразі підприємці змушені орієнтуватися у взаємодії з численними державними органами, де процедури часто забюрократизовані та непрозорі. Існує потреба у впровадженні цифрових інструментів для полегшення взаємодії між бізнесом

і державою та створенні єдиних онлайн-платформ для доступу до послуг і консультацій [3, с. 151].

Таким чином, попри певні позитивні зрушення, правове забезпечення розвитку підприємництва в Україні в умовах воєнного стану залишається недосконалим та фрагментарним. Для подолання наявних проблем необхідно реалізувати комплекс правових заходів, спрямованих на створення сприятливого бізнес-середовища, зниження адміністративних бар'єрів, захист прав інвесторів, стимулювання підприємницької ініціативи.

Вдосконалення правового регулювання підприємницької діяльності в умовах воєнного стану потребує комплексного підходу, який охоплює кілька ключових напрямів. Перш за все, необхідним кроком є усунення прогалин та суперечностей у чинному законодавстві. Наявні законодавчі акти часто не враховують специфіку ведення бізнесу в умовах кризи, тому виникає потреба в ухваленні спеціальних законів, що регулюватимуть особливості підприємницької діяльності в умовах воєнного стану. Наступним важливим напрямком є розробка та реалізація державних програм, спрямованих на відновлення бізнесу на деокупованих територіях. Відновлення економіки в цих регіонах повинно стати пріоритетом державної політики, що вимагає надання цільової фінансової та організаційної підтримки. Державні програми мають включати як довгострокові заходи для стимулювання інвестицій, так і короткострокові заходи, спрямовані на підтримку підприємців, що відновлюють свою діяльність у цих регіонах [2, с. 64].

Важливим аспектом економічної реформи є лібералізація податкової системи, зокрема, запровадження стимулів, які сприятимуть зростанню бізнесу. Однією з таких пропозицій є запровадження «податкових канікул» для новостворених підприємств, захід полегшить фінансове навантаження на компанії на ранніх стадіях їхнього розвитку, сприятиме створенню нових робочих місць та розширенню бізнесу. Податкова лібералізація є життєво важливим кроком для пожвавлення економіки, оскільки вона створює сприятливі умови для інвестицій та розвитку бізнесу.

На додаток до податкових реформ необхідне вдосконалення правового регулювання, особливо в частині посилення відповідальності за порушення прав бізнесу. Забезпечення захисту прав підприємців має важливе значення для ринкової стабільності, особливо у воєнний час, коли багато підприємств стикаються з нерівною конкуренцією та корупцією. Боротьба з корупцією та забезпечення рівних умов для всіх учасників ринку є ключовими для забезпечення сталого економічного зростання. Іншим важливим фактором є діджиталізація адміністративних процедур. Створення онлайн-платформ для комунікації між бізнесом та владою, а також для

надання державних послуг дозволить значно скоротити час, необхідний для вирішення адміністративних питань, та мінімізувати корупційні ризики, що особливо актуально в умовах воєнного стану, коли традиційні способи комунікації можуть бути ускладнені, освітні та консультаційні програми для підприємців мають вирішальне значення для підвищення їхньої правової обізнаності. Підприємці з належними правовими знаннями будуть краще підготовлені до управління своїм бізнесом та уникнення ризиків, пов'язаних з правовою невизначеністю програми повинні охоплювати як загальні правові норми, так і специфічні виклики, з якими стикаються у воєнний час. Комплексне вдосконалення нормативно-правової бази, що регулює підприємницьку діяльність, сприятиме створенню сприятливого середовища для розвитку бізнесу, наданню правової підтримки та стимулюванню економічної активності.

Окрім того, втілення в життя змісту Доктрини інформаційної безпеки від 25 лютого 2017 року та програм «Цифрова Європа» (2021–2027) і «Україна 2030 – країна з розвинутою цифровою економікою» дасть можливість на рівні державних програм інтенсифікувати процеси цифровізації, що виключно позитивно впливають на розвиток та підтримку економічної сфери держави.

Реалізація цих заходів покращить правовий клімат для ведення бізнесу, стимулюватиме економічну активність та прискорить післявоєнну відбудову України. Держава має відігравати ключову роль у цих процесах, створюючи надійну правову базу та інституційні механізми підтримки бізнесу. Водночас, побудова сильної легальної економіки вимагає об'єднання зусиль держави, бізнесу та громадянського суспільства заради спільного майбутнього.

Список використаних джерел:

1. Гонтарева І. В., Євтушенко В. А., Михайленко Д. Г. Особливості розвитку підприємництва в умовах військових дій та повоєнного відновлення України. *Проблеми сучасних трансформацій. Серія: економіка та управління,* 2023. № 7. URL: https://doi.org/10.54929/2786-5738-2023-7-03-04 (дата звернення: 16.11.2024).

2. Експрес-оцінка впливу війни на мікро-, малі та середні підприємства в Україні. Аналітичний звіт. Київ : Програма розвитку ООН в Україні, 2022. 77 с.

3. Намлієва Н. Особливості підприємницької діяльності в умовах воєнного стану в Україні. *Сталий розвиток економіки*. 2023. № 2(47). С. 150–157. 185 с. URL: https://doi.org/10.32782/2308-1988/2023-47-22 (дата звернення: 16.11.2024).

УДК 351.75:324:342.9(477)

РЕКОТОВ ПЕТРО ВАЛЕНТИНОВИЧ,
к.ю.н., доцент, доцент кафедри інформаційної економіки,
підприємництва та фінансів
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: recotov@meta.ua
ORCID ID: https://orcid.org/ 0000-0002-0378-378X

КРОЛЬ БОГДАН ОЛЕКСІЙОВИЧ,
студент
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: krolbohdan1@gmail.com

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

Штучний інтелект (ШІ) став одним із найважливіших інструментів цифрової трансформації, який сьогодні впливає на всі сфери суспільних відносин, у тому числі і на правоохоронну діяльність. Його впровадження відкриває нові можливості у боротьбі зі злочинністю, забезпеченні безпеки громадян та захисті правопорядку. Завдяки своїм широким можливостям, ШІ дозволяє швидко аналізувати великі обсяги даних, виявляти закономірності, які важко визначити людині, оперативно розпізнавати та реагувати на потенційні загрози.

Прикадом можуть послужити алгоритми розпізнавання облич, які використовуються у правоохоронних органах США, Великої Британії та Китаю, забезпечуючи пошук підозрюваних на основі записів з камер спостереження. В Індії створена система прогнозування злочинів, що аналізує місця підвищеної кримінальної активності для ефективного розподілу поліцейських ресурсів. У Європейському Союзі використовуються технології аналізу великих даних для боротьби з кіберзлочинністю та відмиванням грошей.

Водночас, сучасні виклики, такі, як загроза тероризму, гібридні війни та зростання кіберзлочинності, вимагають більш широкого використання цифрових технологій в діяльності правоохоронних органів нашої держави. Особливе значення має використання ШІ в умовах російської агресії, коли

аналіз розвідувальних даних, моніторинг кіберпростору та прогнозування поведінки ворога стають важливими елементами національної безпеки.

Однією з ключових пробем використання ШІ в правоохоронній діяльності є його недостатня врегульованість. Наразі відсутня досконала законодавча база, яка б регламентувала застосування алгоритмів ШІ у роботі правоохоронних органів. Це створює ризики зловживань, пов'язаних з незаконним моніторингом громадян без їхньої згоди, проблемами легітимності отриманих таким чином доказів у судових процесах. Наприклад, дані із соціальних мереж часто залишаються спірним доказовим матеріалом через недосконалість нормативних актів, які регулюють їх використання.

Етичні питання є важливою складовою проблем використання штучного інтелекту. Досвід США показує, що алгоритми розпізнавання облич можуть демонструвати несправедливу упередженість щодо расових або етнічних груп, що ставить під сумнів об'єктивність його роботи. В Україні ця проблема може ускладнитися через низьку якість локалізації програмного забезпечення, що призводить до помилок у розпізнаванні осіб або неправильної інтерпретації даних [1]. Виникає потреба у створенні етичних стандартів для використання ШІ, які б гарантували дотримання прав людини.

Коло проблем доповнюють технологічні виклики. Інфраструктура для інтеграції ШІ в правоохоронну діяльність в Україні знаходиться на початковому етапі розвитку. Наприклад, система «Безпечне місто», яка включає камери спостереження та аналітичні алгоритми, наразі діє лише у великих обласних центрах, залишаючи менші населені пункти поза увагою [2]. Крім того, бракує інтеграції між різними базами даних, що ускладнює обмін інформацією між відомствами [3].

Попри зазначене, перспективи використання ШІ у правоохоронній діяльності залишаються значними. Україна може скористатися міжнародним досвідом для вдосконалення своїх систем. У Сінгапурі, наприклад, реалізовано систему Predictive Policing, яка аналізує поведінкові моделі підозрюваних і прогнозує ймовірність вчинення ними злочинів.Такі технології могли б стати ефективним інструментом для зниження рівня злочинності в Україні.

Ще одним перспективним напрямом є розвиток національних систем, які інтегрують інформацію з камер спостереження, дронів та інших пристроїв. Це дозволить автоматизувати виявлення загроз, таких як несанкціоноване використання зброї, переміщення вибухових речовин чи підозріла активність. Подібні системи можуть значно підвищити ефективність розслідувань і знизити ризики злочинів.

У 2023 році наша держава значно покращила свої позиції з кібербезпеки для протидії російським кіберзагрозам. Використовуючи передові

алгоритми, Україна успішно запобігла понад 150 DDoS-атак, спрямованих на дезорганізацію роботи державних органів та критичної інфраструктури. Ці дії були частиною ширшої національної ініціативи щодо зміцнення систем захисту від ескалації кіберзагроз, які створює російська тактика гібридної війни. Захист критичної інфраструктури країни, включно з енергетичними системами, значно підвищився, що допомогло пом'якшити наслідки ворожих кібератак [4].

З огляду на ескалацію гібридної війни з боку Російської Федерації, важливо врахувати рекомендації НАТО щодо адаптації національного законодавства до нових кіберзагроз. Це передбачає створення більш гнучких механізмів протидії атакам на критичну інфраструктуру, розробку системи раннього виявлення загроз та посилення міжнародного співробітництва у цій сфері [5].

Пріоритетом є фізична безпека. У 2022 році в Києві створено Центр моніторингу безпеки, який активно використовує дрони й аналітичні системи у тому числі і для виявлення диверсійних груп [6]. Ця ініціатива демонструє ефективність інтеграції сучасних технологій у забезпечення безпеки громадян. Проте, задля підвищення національної безпеки, такі центри необхідно впроваджувати в інших регіонах, зокрема в прикордонних та прифронтових зонах, де загрози є найбільш актуальними.

Важливим напрямом залишається реформування діяльності правоохоронних органів. Умови воєнного стану вимагають адаптації системи управління кримінальними розслідуваннями. Це включає спрощення доступу до цифрових доказів, впровадження аналітичних платформ для обробки великих обсягів даних та покращення координації між різними правоохоронними підрозділами. Застосування штучного інтелекту для аналізу цифрових матеріалів, виявлення злочинних схем і прогнозування поведінки підозрюваних може значно підвищити ефективність правоохоронної діяльності.

Таким чином, використання сучасних технологій, зокрема штучного інтелекту, у забезпеченні безпеки України має значний потенціал. Інтеграція цих рішень потребує оновлення законодавчої бази, розвитку інфраструктури кіберзахисту та міжнародного співробітництва. У той же час, необхідно враховувати етичні аспекти та забезпечувати прозорість процесів, що гарантуватиме безпеку громадян та ефективний захист національних інтересів.

Список використаних джерел:

1. Етичні основи правоохоронної діяльності : навчально-методичні рекомендації для студ. юридичного факультету / Юрій Богданович Гофман. Луцьк : Волин. нац. ун-т ім. Лесі Українки, 2022. 36 с. URL: https://evnuir.vnu.edu.ua/bitstream/123456789/21219/3/Etychni%20osnovy.pdf (дата звернення: 17.11.2024).

2. Використання «Безпечного міста» URL: https://dc.org.ua/news/regulyuvannya-shi-v-ukrayini-golovni-tendenciyi-ta-vyklyky (дата звернення: 17.11.2024).

3. ШІ в Україні – як не зарегулювати, захищаючись від ризиків. URL: https://www.dw.com/uk/si-v-ukraini-ak-ne-zareguluvati-ale-zahistitis-vid-rizikiv/a-67288026 (дата звернення: 17.11.2024).

4. Російські хакери координують дії з військовими та посилюють атаки напередодні зими. Як Україна протистоїть кібератакам на енергосистему? URL: https://forbes.ua/company/rosiyski-khakeri-koordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberatakam-na-energosistemu-08112023-17242 (дата звернення: 17.11.2024).

5. Стандарти НАТО: механізм і темпи впровадження, адаптація до українських реалій. URL: https://armyinform.com.ua/2021/02/12/standarty-nato-mehanizm-i-tempy-vprovadzhennya-adaptacziya-do-ukrayinskyh-realij/ (дата звернення: 17.11.2024).

6. Київська міська рада:Створення Центру моніторингу безпеки в Києві. URL: https://kyivcity.gov.ua (дата звернення: 17.11.2024).

УДК 338.45

СЕРГІЄНКО ТЕТЯНА ІВАНІВНА,
Національний університет «Запорізька політехніка» (м. Запоріжжя, Україна)
E-mail: sergienko7921@gmail.com
ORCID ID: http://orcid.org/ 0000-0002-4654-9248

ЛОБАНЬ СЕРГІЙ ІВАНОВИЧ,
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: loban.s1973@gmail.com
ORCID ID: http://orcid.org/0009-0004-2079-3025

МЕХАНІЗМИ МІНІМІЗАЦІЇ РИЗИКІВ ПРОМИСЛОВОГО ПІДПРИЄМСТВА У ЦИФРОВОМУ ПРОСТОРІ ТА ЇХ ВПЛИВ НА КОНКУРЕНТОСПРОМОЖНІСТЬ

Актуальність теми обумовлена стрімким розвитком цифрових технологій, які все активніше інтегруються в усі сфери економіки, зокрема в промисловості. Цифровізація відкриває нові можливості для оптимізації виробничих процесів, підвищення ефективності та зниження витрат, однак вона також супроводжується суттєвими ризиками. Серед них – кіберзагрози, витоки даних, технічні неполадки та інші небезпеки, що можуть

виникнути в результаті інтеграції інформаційно-комунікаційних технологій у виробничі процеси. Промислові підприємства, які активно застосовують цифрові інструменти, стають вразливими до кібернападів і збоїв в інформаційних системах, що може призвести до значних фінансових і репутаційних втрат. У цьому контексті питання мінімізації ризиків у цифровому просторі набуває надзвичайної важливості, оскільки забезпечення безпеки виробничих процесів і стабільності підприємства є критично важливим для його ефективного функціонування [3, с. 163]. Розробка та впровадження ефективних механізмів для мінімізації цих ризиків не лише забезпечує стійкість підприємства, а й підтримує його конкурентоспроможність в умовах швидких технологічних змін та глобалізації.

Розвиток економіки в умовах цифрових трансформацій та інформаційного суспільства є активно досліджуваною темою в сучасній науці. Закордонні вчені, такі як Х. Альбах, Д. Белл, Дж. Гелбрейт, М. Кастельс, Т. Месенбург, Х. Мефферат, Н. Негропонте, А. Пінкварт, Р. Рейхвальд, Д. Тапскотт та Е. Тоффлер, значною мірою сприяли формуванню теоретичних засад дослідження економічних перетворень в умовах цифровізації та створення інформаційного суспільства. Вони розглядали процеси, пов'язані з інтеграцією цифрових технологій у економіку, а також вивчали соціальні, економічні та культурні зміни, що виникають через глобальну цифрову трансформацію.

Вітчизняні науковці також зробили вагомий внесок у вивчення цих процесів, зокрема В. Апалькова, С. Апальков, О. Воскобоєва, М. Глутковський, Н. Демчишак, О. Джусов, М. Дубина, Г. І. Жекало, Н. Іванова, Г. Карчева, С. Коляденко, О. Ромащенко, М. Руденко та інші. Вони зосереджуються на адаптації економіки України до умов цифрової трансформації, зокрема на аналізі процесів впровадження цифрових технологій у різних галузях. Окремо варто виокремити дослідження, присвячені цифровізації промислових підприємств, які є важливим аспектом економічної трансформації. Роботи О. Амоші, Н. Брюховецької, В. Вишневського, В. Воронкової, А. Грищенка, С. Давимуки, Л. Дейнеко, Л. Збаразської, Б. Кваснюка, Ю. Кіндзерського, С. Князєва, О. Ляха, В. Ляшенка, В. Сіденка, В. Тарасевича, Л. Федулової та інших українських дослідників дозволяють глибше зрозуміти, як цифровізація впливає на управління виробничими процесами та ризиками, підвищення ефективності підприємств і мінімізацію ризиків. Таким чином, наукова розробка обраної теми перебуває на стадії активного розвитку, охоплюючи широкий спектр аспектів, таких як кібербезпека, управління ризиками в умовах цифрових трансформацій, а також захист інформаційних систем і даних. На основі теоретичних досліджень та практичних підходів сформовано чимало механізмів і стратегій для

мінімізації ризиків, пов'язаних із впровадженням цифрових технологій у промисловості. Проте, питання, пов'язані з удосконаленням методів управління цифровими ризиками в контексті постійно змінюваного технологічного середовища, залишаються актуальними.

Продовження досліджень цієї теми потребує глибшого аналізу нових загроз і викликів, що виникають у результаті інтенсивної цифровізації виробничих процесів, а також розробки більш ефективних механізмів реагування на них. Необхідно враховувати не лише технологічні, але й організаційні, правові та соціальні аспекти, які можуть значно вплинути на ефективність мінімізації ризиків у цифровому просторі промислових підприємств.

Для того, щоб дослідити механізми мінімізації ризиків промислових підприємств у цифровому просторі, важливо не тільки визначити ключові терміни та поняття, а й зрозуміти, як ці поняття взаємодіють між собою, впливають на процеси управління та цифровізації на підприємстві. Зв'язок між необхідністю дослідження цієї теми та вивченням понятійно-категоріального апарату допоможе забезпечити чітке розуміння основних концепцій, які є основою для формування ефективних механізмів управління ризиками в умовах цифрової трансформації.

Зважаючи на це, представимо таблицю, яка допоможе наочно пов'язати необхідність дослідження цієї теми з основними поняттями та категоріями (див. табл. 1).

Таблиця 1 – **Понятійно-категоріальний апарат досліджуваної теми**

Поняття	**Опис поняття**	**Зв'язок з темою дослідження**
1	2	3
Механізми мінімізації ризиків	Заходи, стратегії, інструменти для зниження ймовірності негативних подій чи їхніх наслідків.	Залучення до дослідження допоможе розробити інструменти для зменшення ризиків у цифровому середовищі промислових підприємств.
Ризики промислового підприємства	Ймовірні загрози, які можуть вплинути на підприємство, включаючи фінансові, технічні, організаційні й цифрові.	Вивчення ризиків дозволяє точно ідентифікувати цифрові загрози для підприємств та розробити стратегії їх мінімізації.
Цифровий простір	Інфраструктура та технології, що забезпечують обробку, передачу та збереження інформації в цифровому вигляді.	Цифровий простір є основним середовищем, де виникають ризики, які потребують мінімізації через механізми управління ризиками.

Продовження таблиці 1

1	2	3
Цифровізація підприємства	Впровадження інформаційно-комунікаційних технологій в усі аспекти діяльності підприємства для оптимізації процесів.	Цифровізація підприємства відкриває нові можливості для зниження ризиків, але також створює нові загрози для інформаційної безпеки.
Кіберризики	Ризики, що пов'язані з кібербезпекою, включаючи атаки, зловмисне втручання, витік даних і порушення роботи IT-систем.	Розгляд кіберризиків є невід'ємною частиною мінімізації ризиків у цифровому просторі, оскільки вони становлять найбільшу загрозу для підприємств.
Інформаційна безпека	Система заходів, спрямованих на захист інформаційних ресурсів від несанкціонованого доступу, використання або змін.	Захист інформаційних ресурсів є критично важливим елементом механізмів мінімізації ризиків у цифровому середовищі підприємства.
Цифрові інструменти для управління ризиками	Спеціалізовані програмні та технологічні рішення для моніторингу, аналізу та управління ризиками в цифровому середовищі.	Використання таких інструментів дозволяє зменшити ймовірність виникнення ризиків та швидко реагувати на зміни в цифровому середовищі.
Ризик-менеджмент	Процес і стратегія управління ризиками, включаючи їх ідентифікацію, оцінку, контролювання та мінімізацію.	Ризик-менеджмент є основою для розробки механізмів мінімізації ризиків і є ключовим інструментом для управління ризиками в цифровому просторі.
Кризовий менеджмент	Система заходів, спрямованих на управління кризовими ситуаціями, що виникають у результаті кризових ризиків.	Кризовий менеджмент важливий для оперативної реакції на ризики, що виникають в умовах цифрової трансформації.

Отже, вивчення понятійно-категоріального апарату обраної теми дозволяє чітко визначити основні концепції та терміни, що є фундаментом для розробки ефективних механізмів управління ризиками [2]. Кожне з визначених понять – від ризиків підприємства до інструментів для їх мінімізації – взаємопов'язане та необхідне для глибокого розуміння процесів, які протікають в цифровому середовищі підприємства. Водночас інтенсивна цифровізація промислових підприємств створює значні

можливості для оптимізації виробничих процесів, підвищення ефективності, зниження витрат та покращення якості продукції [1]. Однак з цими перевагами також виникають нові загрози і виклики, які потребують особливої уваги, зокрема в контексті управління ризиками. Ці нові загрози вимагають застосування адекватних механізмів для їх мінімізації, які базуються на знаннях з понятійного апарату теми. За допомогою таблиці, систематизуємо основні механізми мінімізації ризиків промислового підприємства у цифровому просторі (див. табл. 2).

Таблиця 2 – **Основні механізми мінімізації ризиків промислового підприємства у цифровому просторі**

Тип механізму	**Механізм мінімізації ризиків**	**Опис**
1	2	3
Технічні механізми	Кібербезпека	Впровадження антивірусів, фаєрволів, систем виявлення вторгнень, шифрування даних, багатофакторної аутентифікації для захисту IT-систем від несанкціонованого доступу.
	Інтеграція систем резервного копіювання	Регулярне створення резервних копій важливих даних для забезпечення їх відновлення у разі втрати чи зламу.
	Використання технологій блокчейн	Забезпечення прозорості та незмінності даних, що дозволяє захищати бізнес-процеси від маніпуляцій або шахрайства.
	Автоматизація та моніторинг	Впровадження автоматизованих систем для виявлення й аналізу загроз у реальному часі, що дозволяє оперативно реагувати на інциденти.
Організаційні механізми	Політика кібербезпеки	Розробка стандартів і процедур для захисту даних та управління доступом до цифрових ресурсів підприємства.
	Навчання персоналу	Постійне підвищення кваліфікації співробітників з питань кібербезпеки, проведення тренінгів та навчання щодо захисту інформаційних систем.
	Інцидент-менеджмент	Розробка процедур для оперативного реагування на інциденти безпеки: виявлення, аналіз і відновлення після атак.
Правові механізми	Законодавчі норми та регулювання	Відповідність міжнародним і національним стандартам кібербезпеки, таким як GDPR, закони про захист даних та інформації.
	Юридична відповідальність	Визначення правових наслідків для осіб, відповідальних за порушення стандартів безпеки або виток даних.

Продовження таблиці 2

1	2	3
Соціальні механізми	Підвищення обізнаності серед співробітників	Формування корпоративної культури безпеки, підвищення обізнаності співробітників щодо кіберзагроз і захисту даних.
	Створення довіри серед партнерів і споживачів	Забезпечення прозорості у використанні даних та технологій для зменшення ризиків втрати довіри серед клієнтів і бізнес-партнерів.
Економічні механізми	Оцінка фінансових ризиків	Аналіз потенційних збитків від кіберзагроз і визначення оптимальних витрат на заходи безпеки та відновлення після інцидентів.
	Страхування кіберризиків	Впровадження політик кіберстрахування для зменшення фінансових втрат у разі кібератак, витоків даних чи інших кіберінцидентів.

Щодо визначення механізмів мінімізації ризиків промислового підприємства у цифровому просторі, то це сукупність дій, інструментів та стратегій, спрямованих на зниження ймовірності виникнення небажаних подій, а також на пом'якшення їх наслідків, які можуть виникнути в результаті цифрових трансформацій та інтеграції інформаційно-комунікаційних технологій (ІКТ) у виробничі процеси підприємства [4, с. 15]. Вони охоплюють як технічні, так і організаційні заходи, що дозволяють забезпечити безпеку підприємства в умовах постійно зростаючих цифрових загроз, гарантуючи таким чином стабільність його діяльності і мінімізацію ризиків, пов'язаних з кіберзагрозами та іншими небезпеками цифрового середовища.

Отже, аналіз механізмів мінімізації ризиків у цифровому просторі для промислових підприємств, систематизований у таблиці, дозволяє чітко визначити, як кожен механізм сприяє зниженню потенційних загроз і підвищенню безпеки підприємства в умовах цифрової трансформації. Комплексний підхід до вирішення проблем цифрових ризиків, який охоплює технологічні, організаційні, правові та соціальні аспекти, є необхідним для забезпечення стійкості та конкурентоспроможності підприємства в умовах швидко змінюваного цифрового середовища. Врахування всіх цих факторів дозволяє не лише знизити ризики, а й створити умови для сталого розвитку підприємства, забезпечити його інноваційне зростання та зберегти конкурентні переваги. Це, в свою чергу, сприяє довгостроковій стабільності і ефективності підприємства в умовах цифрової економіки.

Список використаних джерел:

1. Касич А. О., Семенюк В. С. Конкурентоспроможність підприємства в реаліях цифрової економіки. URL: http://www.repository.hneu.edu.ua/bitstream/123456789/27449/1 (дата звернення: 12.11.24).
2. Пархуць Є. Д. Цифрова трансформація та її вплив на конкурентоспроможність міжнародних компаній. URL: http://bses.in.ua/journals/2024/87_2024/14.pdf (дата звернення: 12.11.24).
3. Сергієнко Т. І., Крайнік О. М., Куріс Ю. В. Цифрова трансформація системи управління промислових підприємств. Цифрова трансформація промислового менеджменту: теорія і практика: монографія за ред. д. філософ. н., проф. В. Г. Воронкової, д. е. н., проф. Н. Г. Метеленко. Львів – Торунь : Liha-Pres, 2023. С. 111–172.
4. Цифрова трансформація промислового менеджменту: теорія і практика: монографія за ред. д. філософ. н., проф. В. Г. Воронкової, д. е. н., проф. Н. Г. Метеленко. Львів – Торунь : Liha-Pres, 2023. 816 с.

УДК 005.322:005.93

СІРКО ДМИТРО СЕРГІЙОВИЧ,
магістрант спеціальності 073 «Менеджмент»
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
Науковий керівник: д.філос.н., проф. **Нікітенко В. О.**

УДОСКОНАЛЕННЯ ЛІДЕРСЬКИХ ЯКОСТЕЙ КЕРІВНИКА ТА ЙОГО КОМАНДИ В УМОВАХ КРИЗИ

Поняття лідерства у менеджменті є комплексним та не до кінця вивченим, серед експертів досі точаться дискусії щодо природи його виникнення та фундаментальної сутності його природи.

На даний момент існує декілька взаємовиключних теорій появи лідерства, але ми сконцентруємося на наборі характеристик поняття лідерства, шо визнаються всіма цими теоріями та вивчимо взаємодію поняття з принципами антикризового менеджменту для розробки локальної концепції покращення лідерських якостей керівника та його команди.

До основних характеристик та безпосередніх функцій лідерства як явища віднесено прояв ініціативності, вміння налагоджувати функціональну комунікацію у робочому колективі, підтримка високої вмотивованості та морально-психологічного духу підлеглих, профілактика та вирішення конфліктів у середовищі, вміння проявляти емпатію до підлеглих та

адаптивність, можливість радикально змінювати характеристики та стиль діяльності свої, та своєї команди. Також ми вивчимо взаємодію понять лідерства та антикризового менеджменту.

Одним з основоположників ідей антикризового менеджменту як окремої дисципліни був соціолог Чарльз Перроу, він вивчив взаємодію структури лідерства із ефективністю виявлення та ліквідації проблем у системах різного розміру та будови[1, с. 208–210]. Надалі поняття та механізми антикризового менеджменту багато разів переглядалися та змінювалися його сучасниками та наступниками.

На жаль у відкритому доступі нема досліджень, що чітко б демонстрували приклади застосування методики удосконалення лідерських якостей та на практиці б доводили її ефективність. Для цього необхідно було б після імплементації такої програми поспостерігати за виходом компанії з кризи, у натуральних, а не лабораторних умовах, та чітко визначити що саме завдяки застосуванню впровадженої методики була досягнута ефективність лідерства та антикризового менеджменту.

Натоміть нами буде проаналізований задокументований випадок застосування керівником компанії своїх лідерських якостей у сукупності зі стратегіями та інструментами антикризового менеджменту для подолання серйозної кризи що загрожувала існуванню компанії.

Йдеться про інцидент спалаху інфекції кишкової палички та вірусу Норуок у мережі фаст-фуд ресторанів Chipotle Mexican Grill у Сполучених Штатах Америки в 2015 році. Сам спалах був викликаний системними проблемами у апараті контроля якості Chipotle на всіх рівнях, включно з: механізмом підбору та навчання нових кадрів, механізмом підбору та сертифікації постачальників сировини, механізмом вертикальної взаємодії між структурними підрозділами та механізму контролю якості виробництва безпосередньо на місцях [2, с. 49–54].

Цей спалах спричинив масштабну економічну та репутаційну кризу, вихід та відновлення після якої зайняло компанії більше 2 років. Завдяки лідерству керівника та засновника Chipotle Стіва Еллса компанія впровадили 2 паралельні антикризові програми- усунення проблем у контролі якості через реформи системи, та масштабну PR-акцію, з метою відновлення іміджу і довіри клієнтів.

Основними елементами реформ контролю якості стали введення планових корпоративних перевірок, зміни системи підбору та контролю постачальників, нові міри перевірки та контролю якості продуктів, та нові методи навчання робітників. PR кампанія включала в себе відкритий лист керівника інвесторам із вибаченням, та визнанням провини, висококласний рекламний фільм у документальному стилі, та серія рекламних

епізодів що демонстрували впровадження та ефективність реформ контролю якості.

Дослідження цієї теми є актуальним через потенціал негативного впливу, що нестача лідерства може мати на ефективність антикризових заходів компанії.

Далі ми вивчимо проблематику лідерства як механізму управління та проблеми проведення заходів з удосконалення лідерських якостей керівника в умовах кризи, щоб зрозуміти як боротися з ними при складанні нашої концепції.

До проблем застосування лідерства можна віднести неготовність керівника адаптувати свій стиль управління відповідно до потреб антикризового менеджменту, проблемі у комунікаційному апараті компанії [3], недієва система профілактики та вирішення конфліктних ситуацій робочої середи та негативний вплив зовнішніх факторів.

До проблем проведення заходів з удосконалення лідерських якостей включають неготовність до адаптації компаній- тобто багаторівневий супротив реформуванню підходів управління та організації праці, структурний спротив- специфіку побудови праці та розподілення повноважень, що запобігає ефективному використанню керівником інструментів кризового менеджменту та його лідерських якостей.

Проаналізувавши ці аспекти задачі ми можемо підійти до формування концепції вдосконалення лідерських якостей керівника та його команди в умовах кризи з розумінням теми та проблем, з якими ми можемо зіткнутися, що дозволить нам досягти більшої ефективності результуючої концепції.

Список використаних джерел:

1. Riggio R. E., Newstead T. Crisis Leadership. *Annual Review of Organizational Psychology and Organizational Behavior*. 2022. 244 с. URL: https://www.annualreviews.org/content/journals/10.1146/annurev-orgpsych-120920-044838 (дата звернення: 06.12.2024)

2. J. Cha, R. F. Cichy. Lessons from Chipotle Mexican Grill's Foodborne Illness Outbreaks. *Journal of Hospitality & Tourism Cases.* 2016. 54 с. URL: https://www.chrie.org/assets/docs/JHTC-case-notes/JHTC-vol-6/JHTC_Vol6Issue4_Cha_case.pdf (дата звернення: 06.12.2024)

3. V. Soela, A. Moreira de Carvalho Neto, F. Versiani, D. Martins Diniz. The practice of experienced CEOs: Relational leaders challenging crisis situations. *Contextus – Revista Contemporânea de Economia e Gestão*. 2024. URL: https://www.redalyc.org/journal/5707/570776479001/html/ (дата звернення: 06.12.2024).

4. Цифрова трансформація промислового менеджменту: теорія і практика : монографія / за ред. д.філософ.н., проф. В. Г. Воронкової, д.е.н., проф. Н. Г. Метеленко. Львів – Торунь : Liha-Pres, 2023. 816 с.

5. Цифрова трансформація промислового менеджменту у контексті викликів, можливостей та змін : колективна монографія / за ред. д.філософ.н., проф. В. Г. Воронкової, д.е.н., проф. Н. Г. Метеленко. Львів – Торунь : Liha-Pres, 2024. 592 с.

УДК 330.345

ТКАЧЕНКО ЄЛИЗАВЕТА ЮРІЇВНА,
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: lizahouse@ukr.net
ORCID ID: https://orcid.org/0000-0003-1377-362X

МУРАВЧЕНКО ЄВГЕН КОСТЯНТИНОВИЧ,
магістр, спеціальність 072 «Фінанси, банківська справа, страхування
та фондовий ринок», ОПП «Управління державними та місцевими фінансами»
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: muravchenko.yevhen @gmail.com

УДОСКОНАЛЕННЯ БЮДЖЕТНОЇ ПОЛІТИКИ НА ЗАСАДАХ ПРІОРИТЕТНОСТІ РОЗВИТКУ ОБОРОННОЇ ГАЛУЗІ

У сучасному світі немає жодної країни, яка б у певні періоди своєї історії не стикалася з війнами, кризами, боротьбою чи внутрішніми конфліктами. А рівень бюджетних витрат на оборону є одним із найважливіших показників безпеки будь-якої країни. Таким чином, в умовах зовнішніх загроз фінансове забезпечення, стабілізація та розвиток Збройних Сил України набувають великого значення, а збільшення військових витрат відіграє важливу роль у збереженні територіальної цілісності країни, захисті її суверенітету та формуванні ефективна ринкова модель національної економіки.

Завдання, пов'язані з національною безпекою покладаються в першу чергу на державу. До основних показників, які відображають прагнення держави забезпечити розвиток збройних сил та інших військових формувань, належать видатки державних коштів на оборонну сферу.

Законодавством встановлено, що видатки на фінансування сектору безпеки та оборони мають становити не менше 5 % валового внутрішнього продукту, з яких не менше 3 % має бути спрямовано на фінансування сил оборони. Домінуючу роль у фінансовому забезпеченні відіграють кошти

державного бюджету України, проте допускається і використання інших джерел, які не заборонені законодавством.

Основними критеріями для зміни чисельності сектору безпеки та оборони є зміни безпекового середовища, а також фінансові можливості держави [1].

Повномасштабна війна, яку Росія розв'язала у 2022 році, змусила Україну суттєво переглянути оборонний бюджет. Заплановані на 2022 рік витрати на національну безпеку і оборону у розмірі 323 млрд грн, або 6 % ВВП, були рекордними, але недостатніми для війни такого масштабу. У результаті у 2022 році ці витрати становили 1 трлн 536,6 млрд грн, що становить 32,5 % ВВП.

У 2023 році з державного бюджету на національну безпеку і оборону було спрямовано 1 трлн 141 млрд грн, або 18,2 % ВВП. Зокрема, фінансове забезпечення сил оборони становило 13,85 % ВВП. З усіх видатків держбюджету на оборону припадало 43,4 %. Водночас прогнозувалося, що дефіцит бюджету перевищить 20 % ВВП.

У держбюджеті на 2024 рік на національну безпеку і оборону було закладено майже половину всіх видатків – 1 трлн 692 млрд грн, або 21,6 % ВВП. Ця сума майже на пів трильйона гривень перевищила рівень 2023 р. На фінансування виробництва зброї та боєприпасів спрямовано 51 млрд грн, що в 4,2 рази більше, ніж у попередньому році. На закупівлю дронів виділили 43,3 млрд грн. Очікувалось, що дефіцит бюджету становитиме 614,5 млрд грн.

Заплановані доходи державного бюджету України на 2025 рік без урахування трансфертів становитимуть приблизно 2,34 трлн грн, у тому числі доходи загального фонду – 2,15 трлн грн, доходи спеціального фонду – 193,87 млрд грн.

Заплановані видатки бюджету становитимуть 3,94 трлн грн, у тому числі видатки загального фонду – 3,69 трлн грн, видатки спеціального фонду – 247,43 млрд грн. Зокрема, витрати на оборону плануються у розмірі 2,22 трлн грн.

У бюджеті-2025 видатки на оборону заклали 2 трлн 223 млрд грн (26,3 % прогнозного ВВП). Ця сума більш ніж на півтрильйона перевищує витрати 2024 року. Запланований дефіцит становитиме 1,6 трильйона гривень, або 19,4 % ВВП[2].

У 2023 році Міністерство оборони отримало 857,9 млрд грн. З них 494,1 млрд грн спрямовано на підтримку Збройних Сил України, зокрема на підготовку військових, медичне обслуговування та соціальні виплати ветеранам. На закупівлю та модернізацію озброєнь і техніки було спрямовано понад 350 млрд грн. На житло для армії виділено 136,1 млн грн [2].

У 2024 році бюджет Міноборони зріс до 1 трлн 164 млрд грн, що на 306,1 млрд грн більше попереднього. З них 882,8 млрд грн спрямовано на підтримку Збройних Сил України. Оборонні закупівлі склали приблизно 265 млрд грн. На житлове будівництво спрямовано 100,7 млн грн.

У 2025 році фінансування Міністерства оборони зросте до 1 трлн 530 млрд грн (+366 млрд грн до 2024 року). На Збройні сили України передбачено трохи більше ніж 1 трлн грн. На закупівлю та модернізацію озброєння і техніки спрямовано 455,8 млрд грн. Крім того, 54,5 млрд грн буде спрямовано на розвиток ОПК – на 3,5 млрд грн більше, ніж у 2024 році. Держава виділить 500 млн грн на підтримку програми доступних кредитів для ОПК. У 2025 році до Головного управління розвідки Міноборони має бути перераховано 24,9 млрд грн, що на 6,8 млрд грн більше, ніж у бюджеті на 2024 рік (18,1 млрд грн) і на 13,4 млрд грн більше, ніж у 2023 році (11,5 млрд грн).

До основних проблем, наявних в Україні, у сфері фінансування ЗСУ, належать такі: бюджет України не є бюджетом розвитку; залежність обсягів видатків від благодійної, гуманітарної та міжнародної технічної допомоги, що надається іноземними державами; неефективна структура видатків оборонного бюджету; відсутність об'єктивних можливостей зростання власних доходних джерел та ін.

Для України є вкрай важливою і необхідною співпраця в рамках Європейської політики безпеки і оборони та військове двостороннє співробітництво з країнами-членами ЄС, що є також одним із зобов'язань, які Україна взяла на себе відповідно до Угоди про асоціацію з ЄС [3].

Крім фінансування сектору безпеки й оборони, ЗСУ, як під час війни, так і після неї Україна потребуватиме великих за обсягом фінансових ресурсів для відбудови житла, соціальної інфраструктури, відновлення виробничих активів, промисловості, досягнути яких самостійно в нинішніх реаліях неможливо. однакові видатки зазначені на житло в трьох бюджетах – по 150 млн грн кожен [3].

Список використаних джерел:

1. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. Дата оновлення: 24.10.2020. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 12.11.2024).

2. Гроші для сильних: як змінювався оборонний бюджет України від початку війни. ЗМІ. https://www.rbc.ua/rus/news/groshi-silnih-k-zminyuvavsya-oboronniy-byudzhet-1732120941.html (дата звернення: 12.11.2024).

3. Солдатенко О. В. Фінансування збройних сил України в умовах воєнного стану: євроінтеграційний вектор. *Науковий вісник Ужгородського університету. Серія: Право.* Ужгород, 2023. Т. 1. Вип. 80. С. 576–581. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/297184/290100 (дата звернення: 12.11.2024).

УДК 33.1:004.42

ХОРОШУН ВІКТОРІЯ ВАСИЛІВНА,
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: vixhoroshun@gmail.com
ORCID ID: https://orcid.org/0000-0002-7757-8041

ДЄВІН ВІТАЛІЙ ГЕННАДІЙОВИЧ,
магістр, спеціальність 051 «Економіка», ОПП «Інформаційна економіка»
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
E-mail: vitaliy.devin@gmail.com
ORCID ID: https://orcid.org/0009-0001-3205-8608

ПЕРСПЕКТИВИ РОЗВИТКУ АДАПТИВНИХ МЕХАНІЗМІВ ЕКОНОМІЧНОЇ БЕЗПЕКИ У ЦИФРОВОМУ ПРОСТОРІ

Цифровізація є невід'ємною частиною сучасного економічного розвитку, що охоплює широкий спектр сфер – від електронної комерції до використання великих даних для оптимізації виробничих процесів. Цифровий простір відкриває нові можливості для ефективного управління ресурсами, зниження витрат та підвищення конкурентоспроможності підприємств. Однак разом з перевагами цифровізації зростають і нові загрози, що стосуються інформаційної безпеки, захисту фінансових потоків та захисту персональних даних. У зв'язку з цим важливим аспектом для будь-якої держави та організацій стає забезпечення економічної безпеки в умовах цифрової економіки. Адаптивні механізми мінімізації ризиків в цифровому просторі є основними інструментами для забезпечення стійкості економічної системи до нових викликів.

Економічна безпека традиційно визначається як здатність національної економіки підтримувати стійке функціонування, мінімізувати внутрішні та зовнішні загрози, а також зберігати конкурентоспроможність у глобальному економічному середовищі. Проте з розвитком цифрових технологій поняття економічної безпеки набуло нових вимірів. У цифровому просторі акцент переноситься на забезпечення безпеки інформаційних технологій, захист даних, кібербезпеку та підтримку безперервності цифрових операцій.

Захист економічної безпеки в умовах цифровізації стає складним завданням, оскільки цифрові технології створюють нові можливості для

кібератак, маніпуляцій з інформацією, а також для шахрайства в різних сферах – від фінансів до логістики. Тому економічна безпека в цифровому просторі охоплює не лише захист традиційних економічних систем, а й захист від кіберзагроз, ризиків втрати інформації, а також зловживань з боку учасників цифрових ринків. Розглянемо ризики та загрози цифрової економіки. Цифрові технології створюють нові економічні можливості, але також несуть і суттєві загрози, які можуть завдати шкоди економічній безпеці. Ключовими загрозами є:

1. Кіберзагрози. З переходом до цифрових форматів ведення бізнесу зростає кількість кіберзлочинів. Хакерські атаки можуть призвести до великих фінансових втрат, витоку конфіденційної інформації або збоїв у роботі критично важливих інфраструктур. Наприклад, атакуючи фінансові платформи чи державні органи, зловмисники можуть викрасти мільйони доларів або дестабілізувати економічну ситуацію.

2. Інформаційні маніпуляції та фальсифікація даних. Завдяки розвитку технологій обробки великих даних та поширенню соціальних мереж значно підвищується ймовірність маніпуляцій з інформацією, що може призвести до зміщення ринкових цін, маніпуляцій політичними рішеннями та спотворення публічного уявлення про реальну ситуацію в економіці.

3. Шахрайство у фінансовій сфері. Оскільки більшість фінансових операцій сьогодні здійснюється в онлайн-просторі, шахраї мають доступ до значних обсягів капіталу та персональних даних. Виникає проблема захисту електронних платіжних систем від несанкціонованих транзакцій, а також управління фінансовими потоками на основі ненадійних або підроблених даних.

4. Незахищеність приватних даних. Персональні дані стають важливим економічним активом, який можна використовувати для маніпуляцій на ринку. Недостатня захищеність даних клієнтів або співробітників може призвести до втрати довіри до компанії, судових позовів і фінансових втрат [1, с. 81–122].

Адаптивні механізми мінімізації ризиків є гнучкими інструментами, здатними ефективно реагувати на постійно змінювані загрози в цифровому просторі. Основними аспектами таких механізмів є:

– *розвиток інфраструктури кібербезпеки.* Для захисту економічних операцій у цифровому середовищі необхідно створити багаторівневу систему кібербезпеки. Вона має включати використання криптографії для захисту конфіденційних даних, інтеграцію антивірусних систем і фаєрволів для блокування несанкціонованого доступу, а також впровадження систем виявлення та реагування на інциденти (IDS/IPS), здатних виявляти й блокувати атаки в реальному часі;

– *використання штучного інтелекту (ШІ) та машинного навчання.* Адаптивні алгоритми на основі ШІ здатні виявляти аномалії в поведінці користувачів або фінансових потоках, що дозволяє своєчасно реагувати на потенційні загрози. Наприклад, за допомогою машинного навчання можна передбачити й заблокувати шахрайські транзакції або атаки на платформи;

– *впровадження технології блокчейн.* Одним із найефективніших способів боротьби з фінансовими шахрайствами та зловживаннями є блокчейн. Ця технологія забезпечує прозорість і незмінність даних, що особливо важливо для запобігання маніпуляціям з інформацією, а також для забезпечення безпеки фінансових операцій. Блокчейн забезпечує контроль за транзакціями, знижуючи ймовірність підробки інформації та фінансових маніпуляцій;

– *дотримання нормативно-правових стандартів.* Адаптивна модель безпеки повинна відповідати постійно змінюваним нормативним вимогам. Це включає в себе дотримання стандартів кібербезпеки, таких як GDPR для захисту персональних даних, а також міжнародних стандартів у галузі фінансової безпеки (наприклад, PCI DSS для платіжних систем);

– *інноваційні фінансові технології.* Використання інноваційних платіжних систем, таких як мобільні гаманці та цифрові валютні платформи, дозволяє знижувати ризики, пов'язані з несанкціонованими фінансовими операціями, оскільки більшість з цих систем мають вбудовані механізми захисту даних і двофакторної аутентифікації [2].

Держава відіграє ключову роль у забезпеченні економічної безпеки в цифровому просторі. Це передбачає створення нормативно-правової бази, що регулює питання кібербезпеки, захисту даних та боротьби з фінансовими злочинами в інтернеті. Окрім національних заходів, важливою є міжнародна співпраця в області цифрової економіки. Лише завдяки глобальним зусиллям можна ефективно протидіяти міжнародним кіберзагрозам, стандартизувати правила захисту даних та забезпечити безпечне функціонування глобальних цифрових платформ. У майбутньому адаптивні механізми мінімізації ризиків у цифровому просторі будуть ставати ще більш інтелектуальними та автоматизованими. Прогнози розвитку технологій штучного інтелекту, квантових обчислень, а також дистрибутивних реєстрів відкривають нові можливості для боротьби з цифровими загрозами та покращення економічної безпеки. Важливими напрямками також є розвиток інфраструктури для захисту критичних цифрових ресурсів та вдосконалення міжнародних стандартів цифрової безпеки. Таким чином, цифровізація економіки має величезний потенціал для розвитку, однак вона також приносить нові виклики для забезпечення економічної

безпеки. Адаптивні механізми мінімізації ризиків у цифровому просторі є важливим інструментом для збереження стабільності економічних процесів у цих умовах. Вони повинні включати комплексний підхід, що поєднує новітні технології, правове регулювання та міжнародну співпрацю для забезпечення стійкості економічних систем до нових загроз.

Список використаних джерел:

1. Економіка в умовах цифрової трансформації: перспективи розвитку в XXI столітті [Електронний ресурс] : тези доп. Міжнар. наук.-практ. інтернет-конф. (Київ, 16 трав. 2024 р.) / відп. ред. Ю. М. Уманців. Київ : Держ. торг.-екон. ун-т, 2024. 390 с.

2. Чубукова О. Ю., Ольшанська О. В. Адаптація системи управління економічної безпеки підприємства. URL: http://www.economy.nayka.com.ua/?op=1&z=3765

УДК 331

ЦИКІН ДМИТРО СЕРГІЙОВИЧ,
здобувач третього рівня вищої освіти ступеня доктора філософії
Запорізький національний університет (м. Запоріжжя, Україна)

ХОРУНЖИЙ АРТЕМ ВІКТОРОВИЧ,
магістрант спеціальності 281 «Публічне управління та адміністрування»
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)

АЖАЖА МАРИНА АНДРІЇВНА,
д.н.держ.упр., проф. кафедри управління та адміністрування
Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Запорізького національного університету (м. Запоріжжя, Україна)
ORCID ID: https://orcid.org/0000-0003-3549-7718

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ СОЦІАЛЬНОГО ЗАХИСТУ В УМОВАХ ВОЄННОГО СТАНУ

Повномасштабне вторгнення російської федерації в Україну стало серйозним викликом для всіх напрямків державної політики, зокрема соціальної, яка зосереджена на підтримці малозабезпечених і соціально вразливих категорій населення. У зв'язку з активними бойовими діями та запровадженням воєнного стану на території України було внесено низку

змін до законодавства у сфері соціального забезпечення, які стосуються військовослужбовців та внутрішньо переміщених осіб. Ці зміни суттєво вплинули на зміст та обсяг їх прав і обов'язків.

Незважаючи на воєнний стан, Україна продовжує реалізовувати державну соціальну політику, спрямовану на забезпечення соціальних прав своїх громадян. Відповідно до Конституції України, закріплено такі основоположні принципи: Україна є соціальною і правовою державою (ст. 1); людина, її життя, здоров'я, честь, гідність, недоторканість і безпека визнаються найвищою соціальною цінністю (ст. 3); забезпечення прав і свобод людини є головним обов'язком держави (ст. 3); права і свободи є невідчужуваними та непорушними (ст. 21); вони гарантуються Конституцією і не можуть бути скасовані, а зміни до законодавства не повинні звужувати змісту та обсягу цих прав (ст. 22) [1]. Конституція також визначає основні соціальні права громадян, серед яких:

- право на працю та належні, безпечні й здорові умови праці, а також заробітну плату, не нижчу від визначеної законом (ст. 43);
- право на соціальний захист у разі повної або часткової втрати працездатності, втрати годувальника, безробіття з незалежних від особи обставин, у старості та в інших випадках, передбачених законом (ст. 46);
- право на житло (ст. 47);
- право на достатній життєвий рівень для себе і своєї сім'ї (ст. 48);
- право на охорону здоров'я, медичну допомогу та медичне страхування (ст. 49);
- право дітей-сиріт і дітей, позбавлених батьківського піклування, на державне утримання та виховання (ст. 52);
- право на доступну та безоплатну освіту у державних і комунальних навчальних закладах (ст. 53).

Особливе значення має право на соціальний захист, яке закріплене в статті 46 Конституції України. Воно охоплює матеріальне забезпечення, підтримку та соціальні послуги у разі настання соціальних ризиків. Термін «соціальний захист» у вітчизняному та зарубіжному законодавстві використовується у різних аспектах [1]:

– у широкому значенні – як система економічних, юридичних і організаційних заходів для забезпечення основних соціальних прав людини;

– у вузькому значенні – як діяльність держави, спрямована на захист населення від негативних наслідків соціальних ризиків;

– спеціальний соціальний захист – як захист, що має особливі умови для певних категорій осіб, визначених законом;

– додатковий соціальний захист – як надання пільг, наприклад, у сфері працевлаштування або житлово-комунальних послуг.

Основним законодавчим актом, що кодифікує принципи соціального захисту учасників бойових дій, є Конституція України. Зокрема, стаття 17 визначає, що держава забезпечує соціальний захист громадян України, які проходять військову службу у Збройних Силах України та інших військових формуваннях, а також членів їхніх сімей [1]. Це положення є базисом для інших законів і підзаконних актів, які деталізують різні аспекти соціального забезпечення цієї категорії населення.

Конституція підкреслює важливість державної підтримки учасників бойових дій та їх родин, що узгоджується з міжнародними стандартами соціального захисту, закріпленими у Загальній декларації прав людини, Європейській соціальній хартії та інших міжнародних документах.

Таким чином, у сучасних умовах соціальний захист залишається фундаментальним правом громадян України, яке держава забезпечує навіть у кризових умовах воєнного стану.

До категорії нормативно-правових актів, що регулюють соціальний захист у різних сферах, належать також кодекси України. Зокрема: Податковий кодекс України – визначає податкові пільги для учасників бойових дій [2]; Житловий кодекс України – регулює питання надання житла учасникам бойових дій [3]; Земельний кодекс України – передбачає виділення земельних ділянок для цієї категорії громадян [4].

Нормативно-правове забезпечення соціального захисту під час воєнного стану в Україні є основою для ефективного функціонування системи соціального забезпечення у складних умовах. Воно охоплює як конституційні гарантії, так і спеціальні закони та підзаконні акти, які регулюють заходи підтримки населення в умовах війни.

Закон України «Про правовий режим воєнного стану» «визначає зміст правового режиму воєнного стану, порядок його введення та скасування, правові засади діяльності органів державної влади, військового командування, військових адміністрацій, органів місцевого самоврядування, підприємств, установ та організацій в умовах воєнного стану, гарантії прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб» [5]; визначає основи діяльності державних органів та місцевого самоврядування в умовах воєнного стану; регламентує порядок евакуації населення, забезпечення гуманітарної допомоги та функціонування критичної інфраструктури.

Закон України «Про соціальні послуги» «визначає основні організаційні та правові засади надання соціальних послуг, спрямованих на профілактику складних життєвих обставин, подолання або мінімізацію їх негативних наслідків, особам/сім'ям, які перебувають у складних життєвих обставинах» [6]; містить положення про надання соціальних послуг

вразливим категоріям населення, зокрема внутрішньо переміщеним особам (ВПО) та постраждалим від воєнних дій; регулює діяльність організацій, які надають соціальну допомогу. Надання соціальних послуг здійснюється на принципах [6]:

1) дотримання прав людини, прав дитини та прав осіб з інвалідністю;
2) гуманізму;
3) забезпечення рівних прав та можливостей жінок і чоловіків;
4) поваги до честі та гідності;
5) толерантності;
6) законності;
7) соціальної справедливості;
8) доступності та відкритості;
9) неупередженості та безпечності;
10) добровільності;
11) індивідуального підходу;
12) комплексності;
13) конфіденційності;
14) максимальної ефективності та прозорості використання надавачами соціальних послуг бюджетних та інших коштів;
15) забезпечення високого рівня якості соціальних послуг.

Закон України «Про статус ветеранів війни, гарантії їх соціального захисту» «визначає правовий статус ветеранів війни, забезпечує створення належних умов для їх життєзабезпечення, сприяє формуванню в суспільстві шанобливого ставлення до них»; передбачає комплекс заходів підтримки для учасників бойових дій, членів їхніх сімей, а також сімей загиблих військовослужбовців; включає право на безкоштовне медичне обслуговування, пільги на житло, комунальні послуги та інші форми допомоги. Закон «спрямований на захист ветеранів війни шляхом: створення належних умов для підтримання здоров'я та активного довголіття; організації соціального та інших видів обслуговування, зміцнення матеріально-технічної бази створених для цієї мети закладів і служб та підготовки відповідних спеціалістів; виконання цільових програм соціального і правового захисту ветеранів війни; надання пільг, переваг та соціальних гарантій у процесі трудової діяльності відповідно до професійної підготовки і з урахуванням стану здоров'я» [7]. «Державна політика у сфері соціального захисту ветеранів війни та членів їх сімей, членів сімей загиблих (померлих) ветеранів війни, членів сімей загиблих (померлих) Захисників та Захисниць України формується та реалізується на принципах соціальної справедливості під час встановлення обсягу пільг та гарантій, комплексності під час формування та реалізації заходів адаптації

ветеранів війни до мирного життя, належного фінансового забезпечення передбачених законом пільг та гарантій зазначеній категорії громадян, відкритості та рівного доступу до інформації про державні пільги та гарантії, механізми їх реалізації, доступу до реалізації права на отримання всіх пільг та гарантій, прозорості та підзвітності діяльності органів державної влади, їх посадових осіб у сфері соціального захисту ветеранів війни та членів їх сімей, членів сімей загиблих (померлих) ветеранів війни, членів сімей загиблих (померлих) Захисників та Захисниць України» [7].

Закон України «Про статус ветеранів війни, гарантії їх соціального захисту» закріплює систему державних гарантій, передбачає значний перелік пільг та послуг для ветеранів війни (понад двадцять), серед яких: право на безкоштовне отримання рецептів, лікарських і медичних засобів; виплата допомоги по тимчасовій непрацездатності у повному розмірі незалежно від стажу роботи; збереження робочого місця у разі скорочення чисельності працівників; право на отримання спеціального житла, земельних ділянок для забудови, садівництва чи городництва; ремонт житлового приміщення і пільги на пальне. Закон також закладає правові основи для розвитку соціального партнерства у сфері захисту прав учасників бойових дій.

Закон України «Про соціальний і правовий захист військовослужбовців та членів їх сімей» [8] «визначає основні засади державної політики у сфері соціального захисту військовослужбовців та членів їх сімей, встановлює єдину систему їх соціального та правового захисту, гарантує військовослужбовцям та членам їх сімей в економічній, соціальній, політичній сферах сприятливі умови для реалізації їх конституційного обов'язку щодо захисту Вітчизни та регулює відносини у цій галузі.»; створює єдину систему соціально-правового забезпечення військовослужбовців, спрямовану на створення сприятливих умов для виконання ними свого конституційного обов'язку щодо захисту держави.

Закон визначає: розмір одноразової грошової допомоги для мобілізованих військовослужбовців, яка виплачується в день демобілізації (пункт 2 статті 15); право на отримання одноразової виплати у разі загибелі військовослужбовця чи втрати працездатності. Розмір таких виплат не залежить від військового звання, окладу або стажу служби.

Значущою складовою законодавчої системи України є низка нормативно-правових актів, які прямо або опосередковано стосуються соціального захисту учасників бойових дій. Зокрема, положення Закону України «Про реабілітацію осіб з інвалідністю в Україні» [9] відповідають принципам міжнародних документів у цій сфері.

Закон України «Про реабілітацію осіб з інвалідністю в Україні» визначає основні засади створення правових, соціально-економічних,

організаційних умов для усунення або компенсації наслідків, спричинених стійким порушенням здоров'я, функціонування системи підтримання особами з інвалідністю фізичного, психічного, соціального благополуччя, сприяння їм у досягненні соціальної та матеріальної незалежності [9].

Основними завданнями законодавства України з питань реабілітації осіб з інвалідністю є [9]:

– створення умов для усунення обмежень життєдіяльності осіб з інвалідністю, відновлення і компенсації їх порушених або втрачених здатностей до побутової, професійної, суспільної діяльності;

– визначення основних завдань системи реабілітації осіб з інвалідністю, видів і форм реабілітаційних заходів;

– розмежування повноважень між центральними і місцевими органами виконавчої влади, органами місцевого самоврядування;

– регламентування матеріально-технічного, кадрового, фінансового, наукового забезпечення системи реабілітації осіб з інвалідністю;

– структурно-організаційне забезпечення державної соціальної політики по відношенню до осіб з інвалідністю і дітей з інвалідністю;

– сприяння залученню громадських організацій осіб з інвалідністю до реалізації державної політики у цій сфері.

Фінансове забезпечення соціального захисту учасників бойових дій регулюється положеннями Бюджетного кодексу України [10] та Законом України «Про Державний бюджет України на 2024 рік». Фінансування відповідних програм здійснюється через централізовані та місцеві органи влади, які відповідають за реалізацію заходів у цій сфері.

Разом з тим, деякі вітчизняні та міжнародні експерти наголошують, що окремі положення зазначених законів залишаються декларативними. Зокрема, потребують змін підходи до забезпечення та документування прав осіб з інвалідністю, включно з учасниками бойових дій, які отримали поранення внаслідок війни. Особливо важливими є: доступність послуг; забезпечення рівних можливостей, враховуючи індивідуальні потреби; вирішення проблем працевлаштування; сприяння повноцінній участі осіб з інвалідністю у суспільному житті.

Окрім цього, законодавство передбачає право осіб з інвалідністю на отримання державної допомоги, що стало результатом багатьох факторів, зокрема зростання фізичного та психологічного навантаження, пов'язаного з виконанням професійних обов'язків. Відповідно до Закону України «Про статус ветеранів військової служби, ветеранів органів внутрішніх справ, ветеранів Національної поліції та інших осіб та їх соціальний захист», ветерани з інвалідністю I та II груп мають право на особливий соціальний захист [11].

Законодавство також враховує травми, поранення, каліцтва чи захворювання, отримані під час виконання службових обов'язків, зокрема:

- під час військової служби або перебування у військовому резерві;
- при участі в антитерористичних операціях, заходах з безпеки, відсічі або стримуванні збройної агресії;
- у процесі ліквідації надзвичайних ситуацій чи охорони громадського порядку.

Ці положення формують комплексну систему підтримки для осіб, які постраждали під час виконання службових обов'язків або внаслідок бойових дій, спрямовану на їх реабілітацію та інтеграцію в суспільство.

В Україні функціонує значна кількість закладів різних форм власності, які надають реабілітаційні послуги для осіб з інвалідністю. Ці послуги спрямовані на сприяння інтеграції таких осіб у суспільство. Науковці зазначають, що завдяки мультидисциплінарному підходу такі заклади пропонують широкий спектр реабілітаційних послуг, адаптованих до індивідуальних потреб, віку, статі та характеру захворювань [12].

Однак в Україні наразі відсутня комплексна та системна інфраструктура реабілітації, яка могла б забезпечити доступні, якісні й ефективні послуги, пристосовані до потреб часу, зокрема до викликів, що виникли через військові дії. Тимчасова окупація територій зовнішнім агресором спричиняє втрату значної частини інфраструктури, необхідної для відновлення. У зв'язку з цим набуває особливого значення розвиток військово-медичної реабілітації та відповідної інфраструктури, оскільки кількість осіб із інвалідністю внаслідок бойових дій продовжує зростати. За цих умов державі необхідно значно збільшити інвестиції у створення сучасних реабілітаційних закладів, а органам місцевого самоврядування слід активно шукати додаткові інвестиції у цю сферу з боку інших суб'єктів.

Для вдосконалення нормативно-правової бази важливим напрямком є створення механізмів допомоги та солідарної відповідальності держави й органів місцевого самоврядування щодо страхування життя учасників бойових дій. Це вимагає науково обґрунтованого підходу до розрахунку необхідних фінансових ресурсів у бюджетах різних рівнів. У сучасній Україні вже існують приклади впровадження таких підходів: неприватні страхові компанії укладають договори страхування життя військовослужбовців (як тих, хто перебуває на службі, так і потенційних учасників конфлікту). Крім того, місцева влада впроваджує елементи муніципальної моделі страхування для цієї категорії осіб.

Удосконалення нормативно-правових механізмів державного управління у сфері соціального захисту учасників бойових дій також вимагає залучення громадських і ветеранських організацій, профільних об'єднань

та інших соціальних партнерів до процесу законотворчої діяльності. Досвід свідчить, що такі організації добре обізнані з проблемними аспектами соціального захисту військових і здатні запропонувати інноваційні підходи до вирішення цих питань.

Таким чином, система нормативно-правових актів, зокрема Конституція України, кодекси та спеціальні закони, створює комплексну основу для реалізації державної політики соціального захисту учасників бойових дій та військовослужбовців. Вона враховує як матеріальні, так і правові аспекти підтримки цієї демографічної групи, забезпечуючи їхні права та потреби у складних умовах. Поряд із національними нормативними актами, важливу роль відіграють міжнародні договори, ратифіковані Україною, зокрема документи ООН, Ради Європи та інших організацій, які стосуються прав людини та соціального забезпечення.

Список використаних джерел:

1. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text
2. Податковий кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2755-17#Text
3. Житловий Кодекс України. URL: https://zakon.rada.gov.ua/laws/show/5464-10#Text
4. Земельний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2768-14#Text
5. Закон України «Про правовий режим воєнного стану». URL: https://zakon.rada.gov.ua/laws/show/389-19#Text
6. Закон України «Про соціальні послуги». URL: https://zakon.rada.gov.ua/laws/show/2671-19#Text.
7. Закон України «Про статус ветеранів війни, гарантії їх соціального захисту». URL: https://zakon.rada.gov.ua/laws/show/3551-12#Text
8. Закон України «Про соціальний і правовий захист військовослужбовців та членів їх сімей». URL: https://zakon.rada.gov.ua/laws/show/2011-12#Text
9. Закон України «Про реабілітацію осіб з інвалідністю в Україні». URL: https://zakon.rada.gov.ua/laws/show/2961-15#Text
10. Бюджетний кодекс України: Кодекс України від 08.07.2010 р. № 2456-VI. URL: https://zakon.rada.gov. ua/laws/show/ 2456-17#Text.
11. Закон України «Про статус ветеранів військової служби, ветеранів органів внутрішніх справ, ветеранів Національної поліції і деяких інших осіб та їх соціальний захист». URL: https://zakon.rada.gov.ua/laws/show/203/98-%D0%B2%D1%80#Text
12. Івчук Ю. Ю. Соціальний захист окремих категорій громадян в умовах воєнного стану: законодавчі новели та проблемні аспекти. *Актуальні проблеми права: теорія і практика.* № 2(46), 2023. DOI https://doi.org/10.33216/2218-5461/2023-46-2-101-111
13. Кононець В. П. Актуальні питання соціального захисту та надання послуг військовослужбовцям та внутрішньо переміщеним особам. Юридичний науковий електронний журнал. № 3/2024. http://www.lsej.org.ua/3_2024/75.pdf