УДК 355.451:004.7
JEL: E44; G28; H79
DOI: https://doi.org/10.32983/2222-4459-2024-6-64-79

КІБЕРБЕЗПЕКА ЕКОНОМІКИ ТА ДЕРЖАВНИХ ФІНАНСІВ: ІСТОРІОГРАФІЯ ТА ПОВОЄННА ТРАЄКТОРІЯ РОЗВИТКУ

©2024 ПЕТРУХА Н. М., ПЕТРУХА С. В., ЖМАЄВ А. Ю., СИНКЕВИЧ М. Е.

УДК 355.451:004.7
JEL: E44; G28; H79

Петруха Н. М., Петруха С. В., Жмаєв А. Ю., Синкевич М. Е. Кібербезпека економіки та державних фінансів: історіографія та повоєнна траєкторія розвитку

У статті досліджено еволюцію парадигми кібербезпеки в контексті онтогенезу економіки та державних фінансів з акцентом на тригерах довоєнної та воєннoорієнтованої інституційної пам'яті, а також викликів у повоєнному відновленні України. Наукова новизна полягає в комплексному дослідженні історіографічних процесів у кібербезпеці та їх впливу на динамічні зрушення в економіці та державних фінансах з урахуванням ендо- й екзогенних кібервикликів та сформованих новою економічною реальністю можливостей щодо цифрової трансформації та всеохопної цифровізації. Виявлено, що поява та посилення ролі штучного інтелекту дозволяє сформувати більш тісний рівень кореляції між тенденціями в розвитку економіки та державних фінансах шляхом додавання до прогностичних моделей нових даних, доведення їх до рівня великих даних, виявлення загроз і ризиків у них для вироблення адаптивних антикризовозабарвлених регуляторних поведінкових моделей для державних регуляторів, у тому числі в частині створення формальних і неформальних інституційних правил для протидії кіберзагрозам. На основі цього були сформовані спрямовані на практику рекомендації щодо підвищення ефективності та продуктивності рівня кібербезпеки, які відповідають наявному стратегічному документу в означеній сфері – Стратегії кібербезпеки України, яка зшиває нішові стратегічні документи (якими є План для Ukraine Facility, Стратегія реформування системи управління державними фінансами на 2022–2025 роки) єдиною системою кіберзахисту.

Ключові слова: *кіберзагрози, кібербезпека, національна економіка, державні фінанси, повоєнне відновлення, реконструкція, фінансово-економічна безпека, цифровізація.*
Рис.: *6.* ***Табл.:*** *2.* ***Бібл.:*** *40.*

Петруха Ніна Миколаївна *– кандидат економічних наук, доцент, доцент кафедри менеджменту в будівництві, Київський національний університет будівництва і архітектури (просп. Повітряних Сил, 31, Київ, 03680, Україна)*
E-mail: *nninna1983@gmail.com*
ORCID: *https://orcid.org/0000-0002-3805-2215*
Researcher ID: *https://www.webofscience.com/wos/author/record/2411439*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=58000960900*
Петруха Сергій Валерійович *– кандидат економічних наук, доцент, доцент кафедри менеджменту в будівництві, Київський національний університет будівництва і архітектури (просп. Повітряних Сил, 31, Київ, 03680, Україна)*
E-mail: *psv03051984@gmail.com*
ORCID: *https://orcid.org/0000-0002-8859-0724*
Researcher ID: *https://www.webofscience.com/wos/author/record/2411435*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57006812300*
Жмаєв Анатолій Юрійович *– незалежний дослідник (Київ)*
ORCID: *https://orcid.org/0000-0002-4776-2526*
Синкевич Максим Едуардович *– незалежний дослідник (Київ)*
ORCID: *https://orcid.org/0009-0009-0625-104X*

UDC 355.451:004.7
JEL: E44; G28; H79

Petrukha N. M., Petrukha S. V., Zhmaiev A. Yu., Synkevych M. E. Cyber Security of the Economy and Public Finances: Historiography and Post-War Trajectory of Development

The article examines the evolution of the cyber security paradigm in the context of the ontogenesis of the economy and public finances with an emphasis on the triggers of pre-war and war-oriented institutional memory and challenges in the post-war reconstruction of Ukraine. The scientific novelty consists in a comprehensive study of historiographical processes in cyber security and their impact on dynamic shifts in the economy and public finances, considering endo- and exogenous cyber challenges and opportunities for digital transformation and all-encompassing digitalization formed by the new economic reality. It was found that the emergence and strengthening of the role of artificial intelligence allows for a closer level of correlation between trends in the development of the economy and public finances by adding new data to predictive models, bringing them to the level of big data, identifying threats and risks in them for the development of adaptive anti-crisis-colored regulatory behavioral models for the State regulators, including in terms of creating formal and informal institutional rules for countering cyber threats. On the basis of this, practical recommendations on increasing the efficiency and productivity of the level of cyber security were formed, which correspond to the existing strategic document in this area – the Cyber Security Strategy of Ukraine, which stitches together niche strategic documents (such as the Plan for the Ukraine Facility, the Strategy for the Reform of the State Finance Management System for 2022–2025) by a single cyber defense system.

Keywords: *cyber threats, cyber security, national economy, public finances, post-war recovery, reconstruction, financial and economic security, digitalization.*
Fig.: *6.* ***Tabl.:*** *2.* ***Bibl.:*** *40.*

Petrukha Nina M. *– PhD (Economics), Associate Professor, Associate Professor of the Department of Management in Construction, Kyiv National University of Construction and Architecture (31 Povitryanykh Syl Ave., Kyiv, 03680, Ukraine)*
E-mail: *nninna1983@gmail.com*
ORCID: *https://orcid.org/0000-0002-3805-2215*
Researcher ID: *https://www.webofscience.com/wos/author/record/2411439*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=58000960900*
Petrukha Serhii V. *– PhD (Economics), Associate Professor, Associate Professor of the Department of Management in Construction, Kyiv National University of Construction and Architecture (31 Povitryanykh Syl Ave., Kyiv, 03680, Ukraine)*
E-mail: *psv03051984@gmail.com*
ORCID: *https://orcid.org/0000-0002-8859-0724*
Researcher ID: *https://www.webofscience.com/wos/author/record/2411435*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57006812300*
Zhmaiev Anatolii Yu. *– Independent Researcher (Kyiv)*
ORCID: *https://orcid.org/0000-0002-4776-2526*
Synkevych Maksym E. *– Independent Researcher (Kyiv)*
ORCID: *https://orcid.org/0009-0009-0625-104X*

У сучасному світі, де цифрові технології стають невід'ємною частиною економічних і фінансових систем, питання кібербезпеки набуває особливої актуальності. З розвитком інформаційних технологій і нарощенням обсягів цифрових даних зростає і кількість загроз, що впливають на стабільність і безпеку економічних і фінансових систем, систем управління державними фінансами. І саме кібератаки, зловмисні програми, фішинг та інші форми кіберзлочинності становлять серйозну загрозу не лише для окремих суб'єктів господарювання, але й для державних фінансів та економіки загалом. Майбутня повоєнна модерно-парадигмальна траєкторія розвитку України ще більш ускладнює проблему кібербезпеки, оскільки в цей період країна зіштовхнеться з новими викликами, такими як необхідність відновлення енергетичної інфраструктури, «зшиття» стратегій реконструкції економіки країни зі стійкістю державних фінансів, і за таких умов, без перебільшення іменованих невизначеністю, кібербезпека стає критично важливою для забезпечення національної безпеки, всеохопного цифрового розвитку, цифрової трансформації та цифровізації країни.

Поточне дослідження аналізує еволюцію кібербезпеки в контексті національної економіки та державних фінансів, а також вивчає повоєнні виклики з урахуванням безпоковоорієнтованих поступів та перспектив розвитку цифрової економіки та суспільства. Важливість даної теми також додатково підкреслюється наявною нормативною, інституціональною та регуляторною невизначеністю щодо повоєнної спрямованості нішових і секторальних стратегій (програм) цифрових поступів і забезпечення кібербезпеки відповідно до концептуальних засад розвитку цифрової економіки та суспільства України на 2018–2020 роки [1], які де-юре є чинними й нині. Таким чином, наше дослідження не лише має теоретичне значення, але й володіє високою практичною цінністю, описуючи чинники, які здатні провокувати (виступати в ролі подразника або агента) додаткову стійкість і безпечність національних економічних і фінансових систем, систем управління державними фінансами в сучасному мілітарноорієнтованому світогляді.

Дослідження кібербезпеки економіки та державних фінансів доцільно умовно розділити на два періоди. Перший період – після 2021 р., коли було прийнято рішення Ради національної безпеки і оборони України щодо схвалення Стратегії кібербезпеки України [2]. Зазначений програмно-стратегічний документ сформував новий ландшафт для стратегування систем кібербезпеки економіки та державних фінансів, і в цьому ж році було прийнято Стратегію здійснення цифрового розвитку, цифрових трансформацій і цифровізації Системи управління державними фінансами до 2025 р. [3]. Їм передувала Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки [1], яка ознаменувала другий період досліджень та сформувала «місток» переходу від домінуючого розвитку цифрової економіки та кіберзахисту фінансової системи до аналогічних процесів усередині системи управління державними фінансами (до прикладу, на виконання Концепції створення інтегрованої інформаційно-аналітичної системи «Прозорий бюджет» [4] були розроблені платформа відкритих даних Є-data та ІАС «LOGICA» з однією з найкращих систем кіберзахисту в країні).

Вперше вплив процесів цифровізації економіки та державних фінансів, систем їх кіберзахисту в умовах сучасного соціально-економічного життя населення більшої частини нашої планети та парадигм економічного, фінансового, соціального й інформаційно-технологічного роз-

витку дослідила група провідних вчених світу під керівництвом нобелівських лауреатів з економіки Д. Стігліца й А. Сена [5]. Вона надала поштовх до подальших прикладних досліджень у сфері цифрової економіки [6–9], а також їх перетікання до сфери управління державними фінансами [10–13]. Окремо необхідно виокремити дослідження, присвячені питанням кібербезпеки, які за цей період еволюціонували в напрямі фінансово-економічної безпеки, фінансової стабільності (стійкості) та сучасних фінансових рішень, таких як FinTech тощо [14–16].

Україна не стоїть осторонь фінансово-технологічних процесів, і вже в липні 2020 р. Національний банк України затвердив Стратегію розвитку фінтеху в Україні до 2025 р. [17], яка була після повномасштабного вторгнення рф переглянута в напрямі посилення кібербезпеки [18].

Паралельно цьому в Україні також велися дослідження питань цифрової економіки, процесів цифровізації державних фінансів, їх кіберзахисту в епоху четвертої промислової революції – Індустрії 4.0. Серед цих досліджень варто виокремити роботи В. Вишневського та ін. [19], Ю. Когута [20], В. Міщенка [21], Л. Мельника та ін. [22], С. Криниці [23], О. Парубця [24], Т. Палійчук [25], К. Клименко [26; 27], О. Шубалого [28] та інших [29] визначних учених.

Не применшуючи цінності, важливості та значення результатів згаданих досліджень, варто наголосити, що проблематика кібербезпеки економіки та державних фінансів в умовах воєнного стану та повоєнного відновлення України як підойми до виконання заходів, передбачених Планом для Ukraine Facility та Програмою в рамках Механізму розширеного фінансування для України, залишається нерозв'язаною.

Метою статті є дослідження розвитку кібербезпеки економічних і фінансових систем, державних фінансів України, окреслення основних історичних етапів та сучасних викликів у цій царині, а також розробка рекомендацій для підвищення рівня кібербезпеки як за сучасних умов, так і за умов повоєнного відновлення.

Завдання дослідження:

- визначити основні етапи онтогенезу кібербезпеки з урахуванням розвитку мережі «Інтернет» та інформаційно-телекомунікаційних технологій;
- оцінити ефективність різних методів захисту від кіберзагроз і стан їх упровадження в систему управління державними фінансами;
- визначити особливі виклики кібербезпеці, з якими Україна зіштовхується на сучасному етапі воєнної економіки та державних фінансів, а також, імовірно, зіштовхнеться в повоєнний період;
- надати рекомендації щодо вдосконалення Стратегії кібербезпеки України з урахуванням інерції довоєнної та воєнної інституціональної пам'яті у сфері цифрового розвитку, цифрових трансформацій і цифровізації національної економіки та державних фінансів.

Нарощення інвестицій в Інтернет речей, робототехніку, технології блокчейн і віртуальну реальність змінюють структуру економіки та систему управління державними фінансами. Так, на другому році російсько-української війни частка експорту українських ІТ-послуг у ВВП становить 4%, невпинно нарощується порівняно з іншими галузями економіки, зберігаючи висхідний тренд (*рис. 1*). Це дещо менше, ніж показник 2022 р. – 4,6%, проте значно більше, ніж докризовий рівень 2013 р. – 0,7%. Для порівняння: цей самий показник в аналогічний період в Індії складає 2,8%, у Чехії – 1,8%, у Польщі – 1,8%, у Бразилії – 0,2% [30], підтверджуючи спрямованість економічної політики України як в умовах війни, так і повоєнного відновлення на створення умов для розвитку знаннєвої економіки, просякнуту духом цифрової економіки та цифрових фінансів.

Державні фінанси, з одного боку, налаштовуються на цифровізацію та кіберзахист національної економіки, зокрема шляхом формування механізмів використання коштів, передбачених у державному бюджеті за програмою «Електронне урядування» (КПКВК 2901030). Чинним порядком використання коштів [32] головним їх розпорядником і відповідальним виконавцем цієї бюджетної програми визначено Мінцифри, а одним із провідних одержувачів коштів спеціального фонду державного бюджету – державне підприємство «ДІЯ». Динаміка налаштованості державних фінансів (з акцентованістю на позабюджетні джерела) на процеси цифровізації національної економіки загалом і процеси ІТ-розвитку електронного урядування зокрема наведено на *рис. 2.* З даних цього рисунку видно, що, незважаючи на правовий режим воєнного стану та консолідацію бюджетних видатків, особливо видатків розвитку, Україна продовжує адаптацію державних фінансів до забезпечення невпинних цифрових поступів національної економіки в напрямі укорінення повоєнної модельності цифрової економіки. Це, безумовно, досягається завдяки підтримці партнерів з розвитку таких цифрових поступів із віднесенням даних джерел до позабюджетних, які апріорі не можуть бути секвестровані.

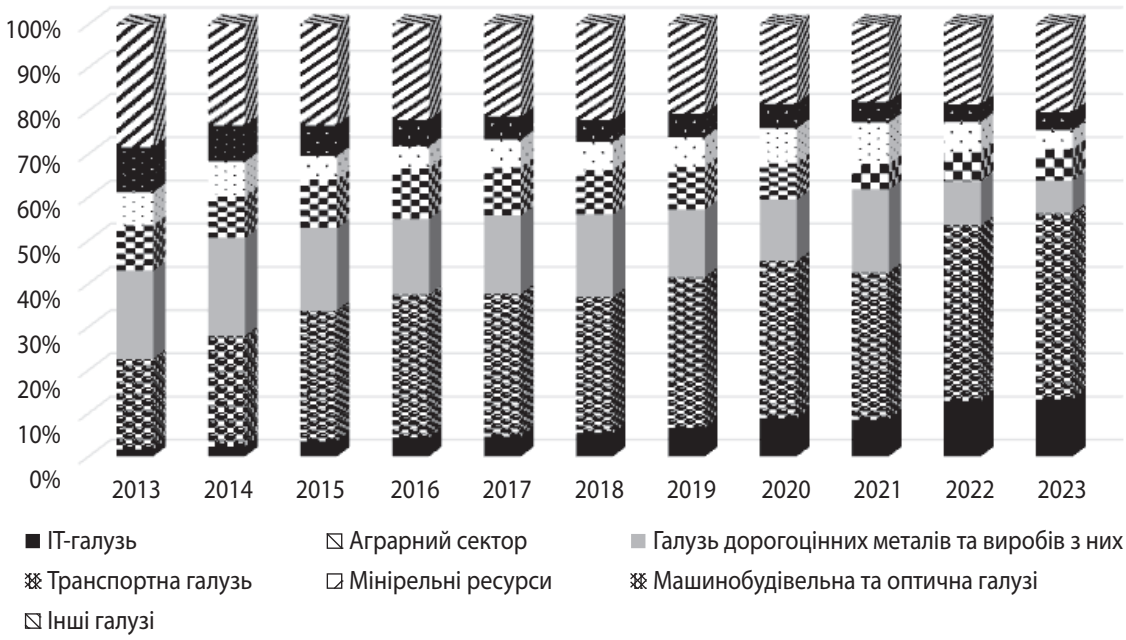

Рис. 1. Динаміка структури експорту товарів (робіт, послуг) національною економікою

Джерело: сформовано авторами за даними [30; 31].

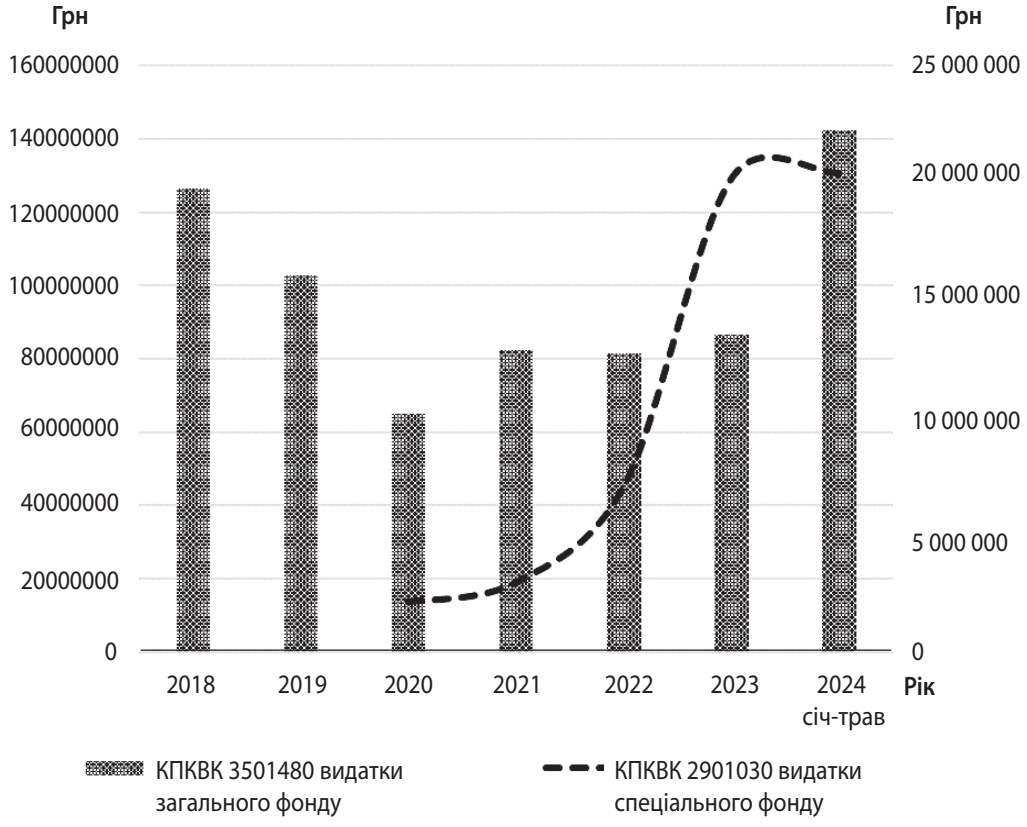

Рис. 2. Налаштованість державних фінансів на власну цифровізацію та формування цифрової економіки України

Джерело: сформовано авторами за даними [33].

З іншого боку, державні фінанси під впливом всеохопного процесу цифровізації економіки також неухильно та стійко вмонтовуються в значені процеси. Для цього Мінфін наказом від 30.01.2017 р. № 18 створив державну установу «Відкриті публічні фінанси», яка має забезпечува-

ти ефективне супроводження ІТ-проєктів у сфері відкритих публічних фінансів. Динаміка фінансування діяльності цієї установи за бюджетної програмою за КПКВК 3501480 «Інформаційне забезпечення системи управління державними фінансами та електронної верифікації і моніторингу» наведено на рис. 2. Згідно з даними цього рисунку спостерігається висхідна тенденція в бюджетних асигнуваннях починаючи із 2022 р., тобто фактично в умовах правового режиму воєнного стану. Однак їх співвідношення (спрямування видатків на цифрові державні фінанси через реалізацію трьох проєктів: єдиний вебпортал використання публічних коштів, бюджет для громадян і портал реєстру проєктів МФО) із видатками на формування цифрової економіки складає 1 : 6.

Таким чином, функціонування системи управління державними фінансами України залежить від ендо- та екзогенних факторів і передумов для повоєнного відновлення національної економіки, її фінансової системи. Серед останніх причин, які виступили каталізатором прискорення процесу цифровізації, – російсько-українська війна та пандемія коронавірусної інфекції COVID-19. Проте ці ж каталізатори виступають також і в ролі активаторів нових кіберзагроз воєнній економіці та державних фінансів.

Загалом концепт кібербезпеки виник у середині XX ст. з розвитком інформаційно-телекомунікаційних технологій та інтернету, і вже перші кіберзагрози з'явилися паралельно зі створенням першого програмного забезпечення. Виникнення хакерства в 1960-х роках, коли ентузіасти розпочали зламувати комп'ютерні системи задля випробування їх можливостей, ознаменувало початок нової епохи в історії національної безпеки. Так, вже у 80-х роках XX ст., коли інтернет розпочав набувати широкої популярності, питання захисту інформаційних систем стало надзвичайно актуальним. Перші віруси, такі як Brain і Morris Worm, продемонстрували уразливість комп'ютерних систем і необхідність захисту даних. Відповідно феномен кібербезпеки має таку етапізацію власного онтогенезу [2; 12; 34]:

- *перший етап (1960–1980-ті рр.)* характеризується тим, що відбулося становлення основних принципів кібербезпеки. Перші кроки в захисті інформаційних систем були спрямовані на захист від фізичного доступу до комп'ютерів та обмеження доступу до даних шляхом використання паролів;
- *другий етап (1990-ті рр.)* обумовлений розширенням мережі «Інтернет», яка спричинила збільшення кількості загроз і спровокувала появу перших комп'ютерних вірусів, комп'ютерних хробаків, троянських і шкідливих програм. У відповідь на ці кіберзагрози розпочався процес створення антивірусних програм і мережевих фаєрволів, започаткувався процес створення перших стандартів кібербезпеки, таких як ISO/IEC 27001;
- *третій етап (2000-ті рр.)* ознаменувався зростанням фізичної кількості користувачів інтернету та розвитком електронної комерції, які спровокували збільшення кіберзлочинності. У цей період з'являються більш складні кіберзагрози, такі як фішинг, DDoS-атаки, також активно розвиваються технології шифрування даних і багатофакторної автентифікації;
- *четвертий етап (2010-ті рр. – наш час)* вирізняється появою технологій Інтернету речей, мобільних пристроїв та хмарних технологій, які породжують нові виклики для кібербезпеки. Кібератаки стають усе більш організованими, стрімко розпочинають розвиватися технології штучного інтелекту для виявлення та запобігання кіберзагрозам, з'являються нові стандарти та регламенти протидії їм, такі як GDPR.

У XXI ст. змінився характер використання фінансів, власне сам перехід у цифрову сферу дозволив державам різного геополітичного рівня, організаціям різного масштабу та окремим фізичним особам завдавати відчутних ударів своїм противникам, і критична неможливість точного відстеження ініціатора фінансового удару дозволяє їм почуватися безкарними. Слід пам'ятати, що за кожною штучно створеною фінансовою кризою, за кожним соціальним, економічним чи фінансовим шоком настає довгостроковий спад якості життя населення, руйнування наявної моделі економічного розвитку, дестабілізація державних фінансів. Таким чином, забезпечення фінансово-економічної безпеки держави – комплексне завдання, вирішення якого лежить в площині злагоджених дій уряду, фізичних та юридичних осіб. Уряд має забезпечувати якісне нормативно-правове підґрунтя модернізації національної економіки та державних фінансів у напрямі їх цифровізації, сформувати нову поведінково-цифрову потребу для учасників економічних відносин, водночас і самі інститути державного регулювання мають продовжувати та посилювати роботу з поінформованості фізичних і юридичних осіб щодо загроз у кіберпросторі [8]. Так, з боку юридичних осіб необхідний відкритий діалог з професійними ІТ-компаніями зі сфери кібербезпеки,

що дозволяє сформувати нові якісні інструменти як боротьби з наслідками від кібератак, так і прогнозування, перехоплення та відбиття кібератак на національну економіку та державні фінанси.

Процеси євроінтеграції загалом та імплементація цілепокладань Цифрової стратегії ЄС формує дедалі більшу залежність суб'єктів державних фінансів і економічних агентів від цифрових технологій та електронних транзакцій, роблячи їх усе більш вразливими до різноманітних кіберзагроз, які можуть мати серйозні наслідки для економічної стійкості, фінансової стабільності та фінансово-економічної безпеки.

Враховуючи це, виокремимо особливості кіберзагроз для системи управління державними фінансами з урахуванням інституційної довоєнної інерції їх регуляції та воєнної адаптації [1; 15; 26, 35]:

1) *масштабність і комплексність системи управління державними фінансами*. Вказана система охоплює широкий спектр суб'єктів, яких об'єднує бюджетний процес, учасниками якого є всі органи державної влади, органи місцевої влади та місцевого самоврядування, бюджетні установи, організації, інші юридичні особи, що беруть участь у бюджетній діяльності. Вона здійснюється через автоматизовану інформаційну систему ведення державного бюджету «Програмний комплекс для ГРК», а відповідно, значна кількість учасників бюджетного процесу створює певну кількість точок входу в програмний комплекс, загострюючи проблему з його кіберзахистом. Станом на зараз вказаний процес унормовує Порядок обміну електронними документами між Мінфіном та учасниками бюджетного процесу на рівні державного бюджету із застосуванням автоматизованої інформаційної системи онлайн-взаємодії з розпорядниками коштів державного бюджету, затверджений наказом Мінфіна від 27.03.2024 р. № 150;
2) *чутливість даних*, яка проявляється в тому, що різні рівні системи управління державними фінансами є володарями соціальної, економічної та фінансової інформації, обробляють значні масиви конфіденційної інформації, включно з персональними даними громадян, їх фінансовими транзакціями та транзакціями учасників бюджетного процесу, військово-обліковими даними українців тощо. Незаконне заволодіння такою інформацією може призвести до руйнування, а можливо, і краху системи управління державними фінансами, до неправомірного використання бюджетних ресурсів (їх нецільового, нерезультативного та неефективного використання) та порушення конфіденційності й інституціональної довіри до системи управління нею;
3) *зовнішні загрози*. Кіберзагрози в переважній більшості не обмежуються країновими кордонами, а отже, як система управління державними фінансами, так і її суб'єкти можуть стати ціллю кібератак, у тому числі з боку країни-агресора – рф, організованих злочинних угруповань або окремих хакерів, що можуть також діяти в колаборації з різних країн світу;
4) *технологічна складність*, у тому числі ІАС «Прозорий бюджет», «Місцевий бюджет», «LOGICA» тощо. Багаторівневі системи ідентифікації, збору та аналізу даних, верифікації суб'єктів бюджетного процесу, їх імовірне відставання від кращих практик, які використовують суб'єкти корпоративного сектора національної економіки, Національний банк України тощо, разом із російсько-українською війною, що продовжується, створюють нові види кіберзагроз, зокрема через застосування кібератак на основі штучного інтелекту, квантових комп'ютерів для зламування шифрів та інших передових методів, вимагаючи від володаря ІАС у сфері управління державними фінансами постійного вдосконалення систем кіберзахисту.

На цій основі ми можемо виділити найбільш небезпечні кіберзагрози для системи управління державними фінансами та сформувати відповідні проєкції (у формі відкликів на відповідні предиктори) на національну економіку (*табл. 1*).

Кібератаки на державні фінанси можуть мати різні форми та спричиняти різноманітні наслідки, зокрема [36]:

1. *DDoS-атаки (Distributed Denial of Service)* – спрямовані на перевантаження серверів установ (організацій), які забезпечуються ІТ-супровід системи управління державними фінансами – ДУ «Відкриті публічні фінанси», що спричинить тимчасове припинення обслуговування розпорядників бюджетних коштів. Окрім того, можливі сценарії унеможливлення підготовки бюджетних запитів головними розпорядниками бюджетних коштів та розпорядниками нижчого рівня через дестабілізацію роботи ІТ-системи бюджетного планування та моніторингу – АІС

Таблиця 1

Типологія кіберзагроз національній економіці та системі управління державними фінансами в умовах російсько-української війни

Найменування кіберзагрози	Характеристика кіберзагрози
1	2
1. Хакерські атаки (у всіх можливих формах прояву), у тому числі спонсором яких виступає країна-агресор – рф	*Цілі кіберзагрози* – втручання в систему управління державними фінансами (передусім неможливість проведення транзакцій для потреб сил безпеки і оборони), інформаційно-комунікаційні системи підтримки суб'єктів національної економіки задля створення зон кризогенності в їх функціонуванні, дестабілізації діяльності найбільших фінансових інститутів держави та/або отримання контролю над ними. *Об'єкти кіберзагрози* – інформаційні системи управління державними фінансами, у тому числі ІАС «Прозорий бюджет», «Місцевий бюджет», «LOGICA», СДО «Клієнт Казначейства – Казначейство» тощо, Національний банк, системно важливі банки, фондові біржі, фінансові Data-центри, майнінгові ферми тощо. *Особливості кіберзагрози* – найвища кваліфікація хакерів, інфраструктурна підтримка кібератак за допомогою військової інфраструктури ініціатора атаки (рф), масштабність і системність характеру кібератаки
2. Фінансові диверсії всередині системи управління державними фінансами та на фінансовому ринку, ініційовані найбільшими фінансовими корпораціями, у тому числі кінцевим бенефіціарним власником яких є представник рф	*Цілі кіберзагрози* – формування всередині системи управління державними фінансами (передусім у системі казначейського обслуговування) та на фінансових ринках панічних настроїв, зниження вартості або виключення з котирувань окремих цінних паперів, ОВДП через технологію дезінформації (фейкових новин, інформації, що паплюжить честь і гідність керівництва держави, державних службовців категорії А, ділової репутації суб'єктів державного сектора економіки та фінансових компаній), контрольований виток інсайдерської інформації, хакерські атаки, організацію штучних збоїв або аварій усередині інформаційно-керівних систем. *Об'єкти кіберзагрози* – державні цінні папери, цінні папери суб'єктів державного та корпоративного секторів національної економіки, а також втручання у процеси залучення міжнародної технічної допомоги, іноземних інвестицій, програм державно-приватного партнерства (переважно у сфері потреб сил безпеки і оборони та розвитку оборонно-промислового комплексу та енергетики). *Особливості кіберзагрози* – штучне погіршення рейтингування державних цінних паперів, цінних паперів суб'єктів господарювання, зниження інвестиційної привабливості суб'єктів державного сектора економіки, створення штучних бар'єрів на ринках капіталів для оборонно-промислового комплексу та енергетики
3. Архітектування та застосування соціоінженерних троянів, їх адаптація до прогресу розвитку систем управління державними фінансами	*Цілі кіберзагрози* – отримання через акаунти приватних і публічних осіб – клієнтів банків, органів державного казначейства доступу до всієї фінансової інфраструктури з подальшою ініціацією втрати контролю над нею, а також незаконного заволодіння інформацією з обмеженим доступом, у тому числі видатками бюджету для потреб сектора безпеки і оборони, персональними даними представників суб'єктів, які є учасниками бюджетного процесу. *Об'єкти кіберзагрози* – програмні модулі соціальних мереж, акаунти в інтернет-банкінгу, СДО «Клієнт Казначейства – Казначейство», файлові менеджери власників банківських карток тощо. *Особливості кіберзагрози* – доступ до критичної банківської та казначейської інфраструктури зловмисники (хакери) отримують через менш захищені приватні та публічні акаунти, які знаходяться за межами основної інфраструктури банків та органів державного казначейства, а отже, мають більш високу вразливість
4. Інфраструктурні атаки на IoT-мережі (Інтернет речей)	*Цілі кіберзагрози* – отримання контролю над бізнес-процесами суб'єктів корпоративного та державного секторів національної економіки, а також завдання їм прямої та/або непрямої (опосередкованої) шкоди (збитків), формування нових фіскальних ризиків для державних фінансів.

Закінчення табл. 1

1	2
	Об'єкти кіберзагрози – інформаційні системи управління державними фінансами, надання соціальних послуг, надання медичних послуг, системи банківської та/або казначейської взаємодії із клієнтами. *Особливості кіберзагрози* – через викрадення чи злам акаунта або елементів ІТ-інфраструктури хакери отримують можливість впливати на інфраструктуру користувача, конструюючи фінансово-економічний і соціальний хаос або техногенні загрози
5. Провайдинг хакерського інструментарію засобами відкритого коду	*Цілі кіберзагрози* – залучення до числа зловмисників (хакерів) громадян, які схильні до колаборації із країною-агресором або до порушення законодавства, зокрема через вмотивованість до помсти чи суспільного (фахового) визнання шляхом передачі їм хакерського інструментарію (програмного забезпечення) з відкритим кодом. *Об'єкти кіберзагрози* – переважно атаки спрямовані на швидкий доступ до коштів об'єктів атаки, якими є суб'єкти бюджетного процесу, учасники казначейського та банківського обслуговування, акаунти інтернет-банкінгу та СДО «Клієнт Казначейства – Казначейство» тощо. *Особливості кіберзагрози* – шляхом застосування програмного забезпечення з відкритим кодом зловмисники (хакери) здійснюють множинну атаку на систему управління державними фінансами або суб'єктів національної економіки з безлічі географічно віддалених точок доступу, унеможливлюючи (суттєво ускладнюючи) розкриття учасників кібератаки

Джерело: сформовано авторами за даними [3; 16; 17].

«ГРК-ВЕБ», а також покриття негайних потреб сил безпеки і оборони. У даній системі станом на перший квартал 2024 р. створено 1209 облікових записів, з яких 83 належать головним розпорядникам коштів і 1126 – розпорядникам нижчого рівня.

2. *Фішинг і соціальна інженерія* – застосовується для отримання доступу до конфіденційної інформації шляхом обману працівників розпорядників бюджетних коштів, які модерують електронні кабінети в АІС «ГРК-ВЕБ» та/або відповідають за функціонування чи створення запитів (зокрема, платіжних інструкцій) у СДО «Клієнт Казначейства – Казначейство».
3. *Шкідливе програмне забезпечення* (*malicious software*) – може бути використане для викрадення даних, дестабілізації роботи систем управління державними фінансами, зокрема кібератака вірусами «Petya», «Petya/Mischa» та «NotPetya» паралізувала доступ до СДО «Клієнт Казначейства – Казначейство», системи внутрішнього моніторингу між головними розпорядниками бюджетних коштів та розпорядниками нижчого рівня, зачепивши також діяльність Національного банку України та комерційних банків.

Кібербезпека державних фінансів є критично важливою для виконання державою взятих на себе зобов'язань щодо підтримки суб'єктів господарювання, проведення економічних реформ, забезпечення функціонування економічних агентів у межах наявного парадигмального напряму розвитку економіки України. Водночас чим вищий ступінь впровадження ІТ-сервісів у систему управління державними фінансами та доступність державних вебсайтів, тим більший ступінь ризику для кібератаки на них. Так, під час російсько-української війни значно зросла кількість кібератак на об'єкти зв'язку, системи управління силами безпеки і оборони, критичну інфраструктуру та фінансовий сектор (*рис. 3*).

З даних рис. 3 спостерігається високий рівень кореляції між ступенем відкритості вебсайтів органів державної влади та кількістю кіберзагроз суб'єктам національної економіки і державних фінансів. Така тенденція обумовлена необхідністю приведення ступеня відкритості вебсайтів до ДСТУ EN 301 549:2022 «Інформаційні технології. Вимоги щодо доступності продуктів та послуг ІКТ», тобто фактично це є спробою сформувати цифрову інклюзію в системі управління соціально-економічними процесами та державними фінансами, що наближає України до кіберкультури провідних європейських країн.

Подальше балансування між відкритістю та каберзахистом вебсайтів органів державної влади лежить у площині політичного підтексту кіберзагроз, кількість яких невпинно зростає. Так, відповідно до даних European Repository

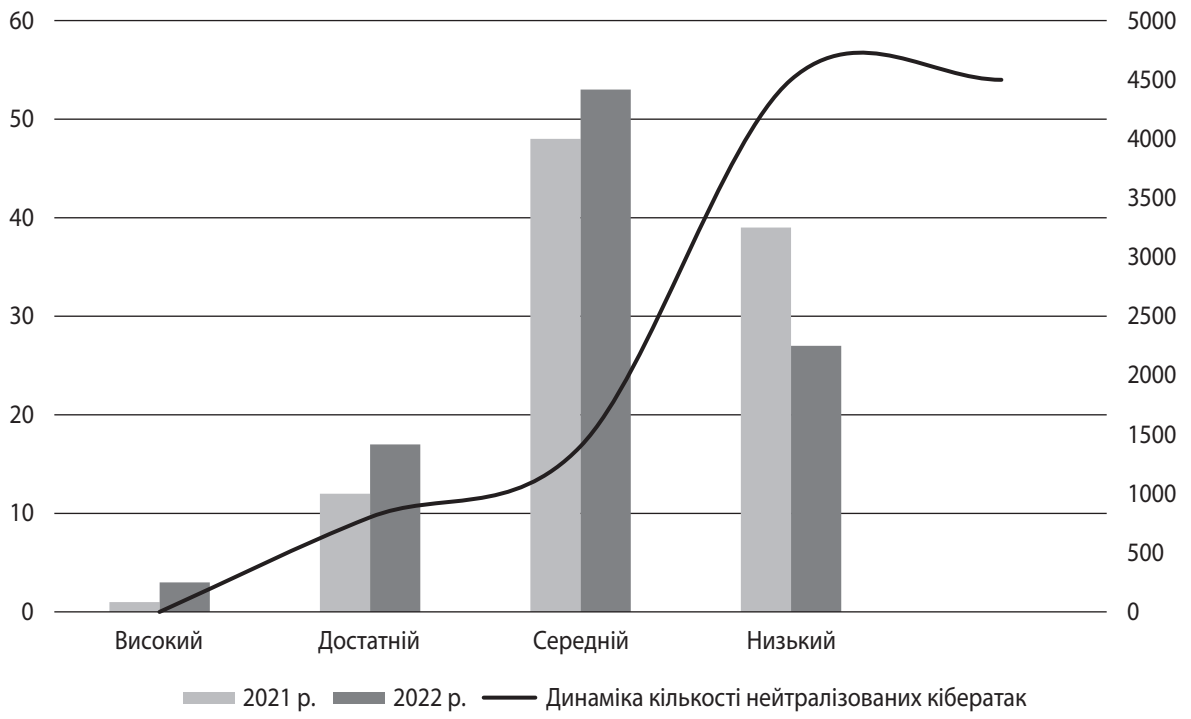

Рис. 3. Співвідношення рівня відкритості вебсайтів органів державної влади та кіберзагроз суб'єктам національної економіки і державних фінансів

Джерело: сформовано авторами за даними [5; 37].

of Cyber Incidents [38], за майже чверть століття хакери здійснили біля 2700 кібератак, майже половина з яких (1110 од.) відбулася в останні три роки. Найбільша частка політично вмотивованих кібератак відбувається з КНДР – майже 12%, за якою слідує рф з часткою 11,6% та Іран – 5,3%, які прямо чи опосередковано підтримують країну-агресора в російсько-українській війні. Водночас наголосимо, що у 45% випадків країну походження кібератаки на економічних агентів чи суб'єктів державних фінансів ідентифікувати неможливо (*рис. 4*).

В умовах воєнної економіки та формування контурів повоєнного відновлення, у тому числі шляхом реалізації заходів, передбачених Планом для Ukraine Facility, від рівня протистояння суб'єктами системи управління державними фінансами кібератакам залежить фактично швидкість покриття негайних потреб сил безпеки і оборони, потреб у релокації бізнесу та підтримки соціально незахищених верств населення, передусім ВПО. Для цього необхідно стратегувати заходи протистояння таким кіберзагрозам на коротко- та середньострокову перспективу (*табл. 2*).

Повоєнний період для будь-якої країни є часом відновлення та реконструкції. Тож для України, яка продовжує зазнавати значних втрат (збитків) під час війни, особливо важливо звернути увагу на кібербезпеку економіки та державних фінансів, налаштовуючи первинний модуль – моніторингову систему для збору емпіричної інформації та поведінкових моделей діяльності користувачів в АІС «ГРК-ВЕБ» та СДО «Клієнт Казначейства – Казначейство». На *рис. 5* візуалізовано елементи контуру формування, забезпечення, а також взаємозв'язку складових у системі моніторингу кіберсередовища функціонування державних фінансів у повоєнний період.

Моніторинг кількісних характеристик кіберзагроз системі управління державними фінансами включає постійне відстеження рівня певних індикаторів з метою прогнозування їх ступеня та антикризового управління [39], що включає застосування набору превентивних заходів, спрямованих на нейтралізацію та зниження кіберризиків. Для цього необхідно в короткостроковій перспективі запровадити в систему управління державними фінансами сучасну композицію відповідних кіберзаходів для протистояння кіберзагрозам (*рис. 6*).

Їх впровадження додатково актуалізується наявністю щільної кореляції між кількісно-якісною параметризацією кіберзагроз системі управління державними фінансами та стійкістю структурних зрушень у національній економіці [40], зокрема швидкістю її адаптації спочатку до умов ведення воєнної економіки, а згодом і до процесів повоєнного відновлення, уречевлених, серед іншого,

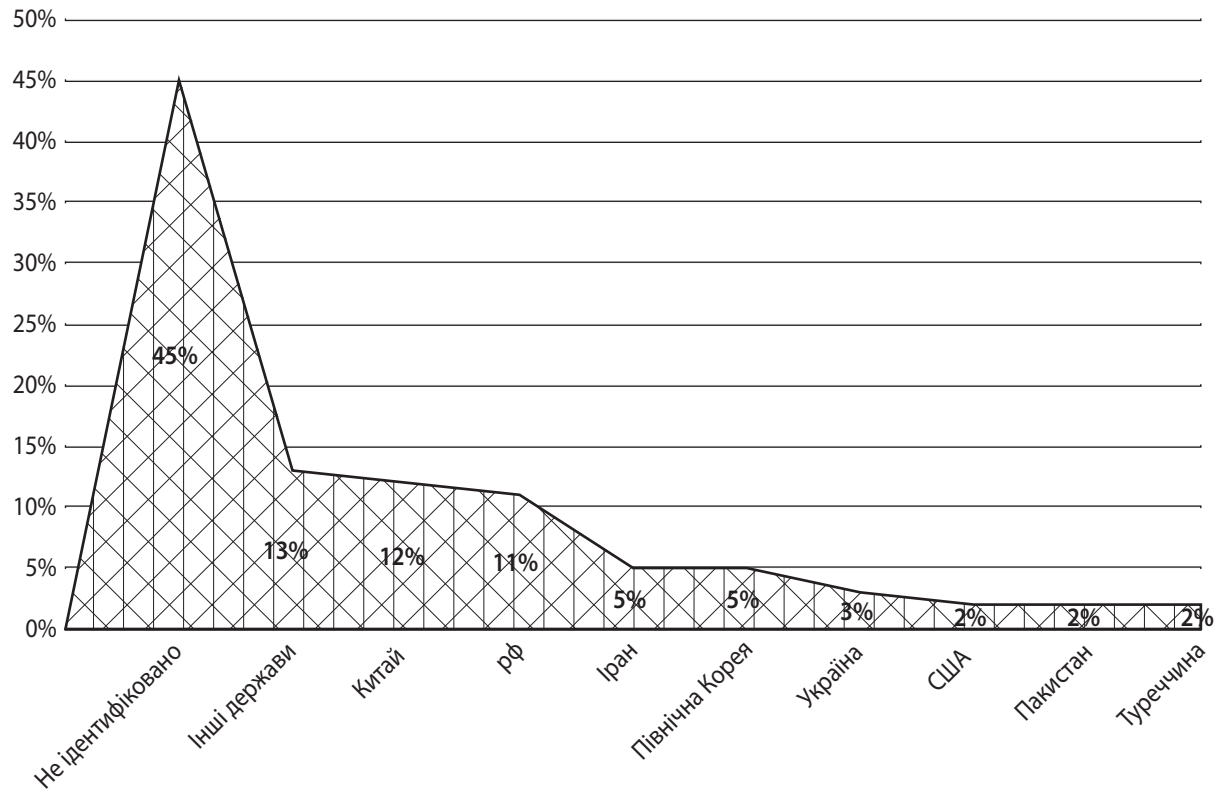

Рис. 4. Країни походження політично заангажованих кіберзагроз

Джерело: сформовано авторами за даними [38].

Таблиця 2

Перспективні налаштування системи управління державними фінансами задля протидії кіберзагрозам

Захисні чи адаптаційні стратегічні рішення	Характеристика	Застосовувані технології	Тактичні заходи щодо впровадження	Переваги
1	2	3	4	5
Підвищення рівня кібербезпеки	Посилення кібербезпеки на всіх рівнях системи управління державними фінансами	Мультифакторна аутентифікація, шифрування даних, розробка спеціалізованого й оновлення наявного програмного забезпечення	Регулярні аудити кібербезпеки та тестування на наявність несанкціонованого доступу до ІТ-систем	Виявлення й усунення вразливих сторін у функціонуванні АІС «ГРК-ВЕБ» та СДО «Клієнт Казначейства – Казначейство»
Підвищення рівня цифрових компетенцій користувачів АІС «ГРК-ВЕБ» та СДО «Клієнт Казначейства – Казначейство»	Короткострокові навчальні заходи та пілотування практичних ситуацій з виявлення й реагування на кібератаки, побудована базових поведінкових моделей користувачів	Програми тематичних короткострокових навчально-комунікаційних заходів, створення симуляторів кіберзагроз, які враховують особливості функціонування систем	Розширення спеціалізованим контентом вебпорталу управління знаннями НАДС, формування нормативної частини тематичного насичення відповідних тренінгових курсів для державних службовців та представників органів місцевого самоврядування	Підвищення рівня обізнаності та швидкості реагування уповноважених представників на виявлені кібератаки

Закінчення табл. 2

1	2	3	4	5
Колаборація з партнерами з розвитку	Співпраця з визнаними міжнародними організаціями у сфері кіберзахисту	Обмін досвідом, новітні технології, імплементація кращих ІТ-рішень та безпекових практик	Участь у міжнародних угодах та ініціативах	Доступ до новітніх ІТ-рішень та координація дій у сфері кібербезпеки
Удосконалення положень Стратегії кібербезпеки України	Внесення окремого розділу до Стратегії кібербезпеки України, присвяченого особливостям функціонування державних фінансів в умовах правового режиму воєнного стану	Захист критичної інфраструктури в системі управління державними фінансами, координування дій стейкхолдерів задля швидкого реагування на кіберзагрози	Формування робочої групи з питань адаптації державних фінансів до кіберзагроз, зокрема породжених особливостями функціонування економічних агентів в умовах воєнної економіки	Комплексний підхід до кіберзбезпеки системи управління державними фінансами
Використання штучного інтелекту та машинного навчання	Використання новітніх технологій для виявлення та запобігання кібератакам	Штучний інтелект, машинне навчання, аналіз великих даних	Автоматизований аналіз великих даних і прогнозування кіберзагроз	Підвищення ефективності кіберзахисту системи управління державними фінансами

Джерело: авторська розробка.

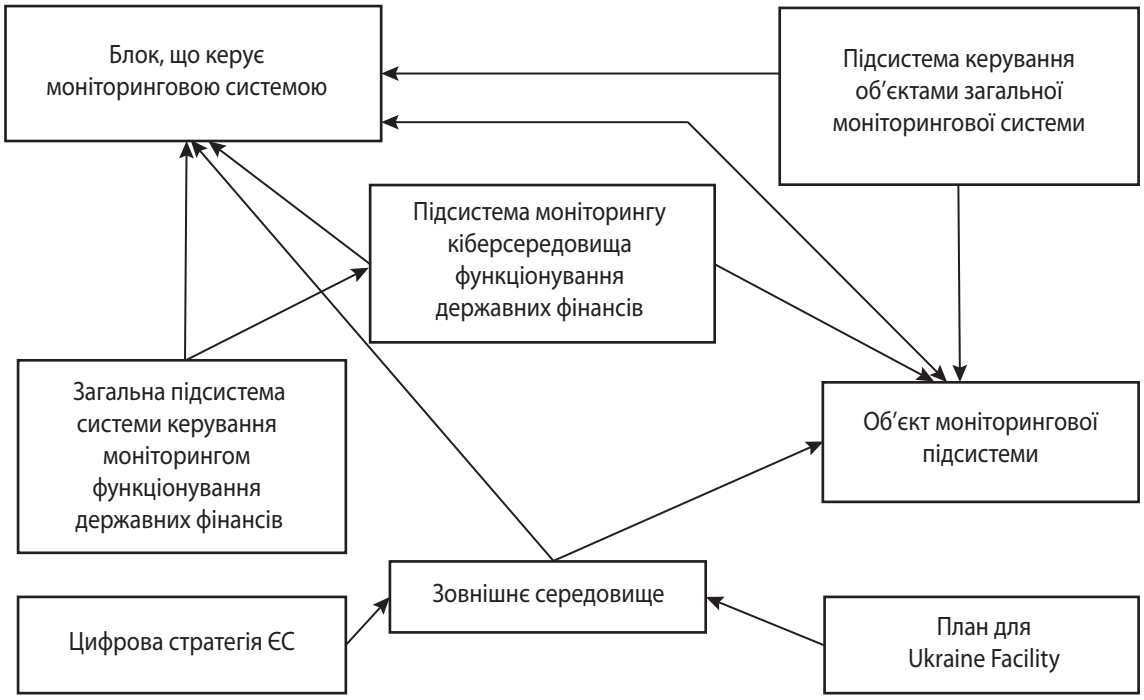

Рис. 5. Візуалізація елементної будови системи кібермоніторингу функціонування державних фінансів

Джерело: авторська розробка.

в необхідності виконання заходів, передбачених Планом для Ukraine Facility.

ВИСНОВКИ

Економіка воєнного часу, традиційні воєнні дії, які відбуваються вже третій рік поспіль на понад 3,5 тис. км по лінії зіткнення з рф, переносять загрози у формі кібератак ще й на системи, які ресурсно забезпечують потреби сил безпеки і оборони та економічних агентів національної економіки. Фактично на кіберарені питання кібербезпеки державних фінансів заміщується категорією

Рис. 6. Перспективні напрями забезпечення кібербезпеки системи управління державними фінансами в умовах правового режиму воєнного стану та формування підходів до повоєнного відновлення

Джерело: авторська розробка.

«кібервійна», яку невпинно провокує країна-агресор – рф. Від того, як ми стабілізуємо ІТ-фронт, залежить і те, як швидко ми переможемо в кібервійні з рф, а відповідно – ресурсно забезпечимо процеси повоєнної відбудови.

Своєю чергою, повоєнний час для України буде часом масштабних викликів і можливостей, і без розробки сучасних, адаптованих до умов сьогодення Стратегії кібербезпеки України, наповнення її духом цілепокладань Цифрової стратегії ЄС, їх збалансування з Бюджетною декларацією на 2025–2027 роки, буде вкрай складно забезпечити повоєнну реконструкцію України. Цьому мають сприяти додавання (як під час перегляду, тобто актуалізації, так і форматування нових на наступний програмний період, наприклад 2026–2029 роки) до Стратегії реформування системи управління державними фінансами на 2022–2025 роки і Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації Системи управління державними фінансами до 2025 року сучасних технологій, якими є штучний інтелект, машинне навчання та блокчейн. Тим самим забезпечуючи новий, раніше не досяжний рівень кібербезпеки системи управління державними фінансами та національної економіки.

Перспективи подальших розвідок знаходяться в площині емпірики досягнутого рівня прогресу в забезпеченні кібербезпеки державних фінансів та національної економіки в період дії Стратегії здій-

снення цифрового розвитку, цифрових трансформацій і цифровізації Системи управління державними фінансами до 2025 року, а також відстеження результативності протистояння України в кібервійні з рф завдяки виконанню заходів, які передбачені Планом для Ukraine Facility. ■

БІБЛІОГРАФІЯ

1. Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки : схвалена розпорядженням Кабінету Міністрів України від 17.01.2018 р. № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-p#Text
2. Про Стратегію кібербезпеки України : рішення Ради національної безпеки і оборони України від 14.05.2021 р. URL: https://zakon.rada.gov.ua/laws/show/n0055525-21#n2
3. Стратегія здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року : схвалено розпорядженням Кабінету Міністрів України від 17.11.2021 р. № 1467-р. URL: https://zakon.rada.gov.ua/laws/show/1467-2021-p#Text
4. Концепція створення інтегрованої інформаційно-аналітичної системи «Прозорий бюджет» : схвалено розпорядженням Кабінету Міністрів України від 11.02.2016 р. № 92-р (у ред. від 24.12.2019 р. № 1418-р). URL: https://zakon.rada.gov.ua/laws/show/92-2016-p#Text
5. Stigliz J., Sen A., Fitoussi J.-P. Mis-measuring Our Lives: Why GDP Doesn't Add Up. *Sustainable*. URL: https://elearning.unimib.it/pluginfile.php/566943/mod_resource/content/3/StiglitzSustainabilityE.pdf
6. The Institutional Foundations of the Digital Economy in the 21st Century / ed. by E. G. Popkova, A. Krivtsov, A. V. Bogoviz. Berlin : Walter de Gruyter GmbH & Co KG, 2021. 269 p.
7. Overby H., Audestad J. A. Introduction to Digital Economics. Foundations, Business Models and Case Studies. Cham : Springer Nature, 2021. 353 p.
8. Sustainable Development of Modern Digital Economy / ed. by J. V. Ragulina, A. A. Khachaturyan, A. S. Abdulkadyrov, Z. Sh. Babaeva. Cham : Springer Nature, 2021. 368 p.
9. The Big Data Driven Digital Economy: Artificial and Computational Intelligence / ed. by M. A. Abdalmuttaleb, M. Al-Sartawi. Cham : Springer Nature, 2021. 472 p.
10. Long C., Cangiano M., Middleton E., Stewart J. Digital Public Financial Management. An Emerging Paradigm. London : ODI Working Paper Series, 2023. 63 p.
11. Digital Finance and the Future of the Global Financial System: Disruption and Innovation in Financial Services / ed. by L. Gasiorkiewicz, J. Monkiewicz. New York, NY : Routledge, 2023. 232 p.
12. Benni N. Digital Finance and Inclusion in the Time of COVID-19 : Lessons, Experiences and Proposals. Rome : FAO, 2021. 94 p.
13. Hrubiian O., Jeremic D. Public Finance Management Reform: Digitalization as a Tool to Lift Processes to a New Level of Governance and Eradicate Systemic Issues. *EU4PFM*. URL: https://eu4pfm.com.ua/news/public-finance-management-reform-digitalization-as-a-tool-to-lift-processes-to-a-new-level-of-governance-and-eradicate-systemic-issues
14. Kau G., Lashkari Z. H., Lashkari A. H. Understanding Cybersecurity Management in FinTech: Challenges, Strategies and Trends. Cham : Springer Nature, 2021. 182 p.
15. Kopp E., Kaffenberger L., Wilson C. Cyber Risk, Market Failures, and Financial Stability. *IMF Working Papers*. 2017. Vol. 185. 36 p. URL: https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104
16. Cyber Risks and Financial Stability : It's a Small World After All / F. Adelmann et al. *IMF Working Papers*. 2020. Vol. 7. 32 p. URL: https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2020/12/04/Cyber-Risk-and-Financial-Stability-Its-a-Small-World-After-All-48622
17. Стратегія розвитку фінтеху в Україні до 2025 року. Сталий розвиток інновацій, кешлес та фінграмотність. *Національний банк України*. 2020. 49 с. URL: https://bank.gov.ua/ua/files/DDWIAwXTdqjdClp
18. Стратегія розвитку фінансового сектору України. *Національний банк України*. URL: https://bank.gov.ua/admin_uploads/article/Strategy_finsector_NBU.pdf?v=7
19. Цифровізація економіки України: трансформаційний потенціал : монографія / В. П. Вишневський, О. М. Гаркушенко, С. І. Князєв та ін. Київ : ВД «Академперіодика», 2020. 188 с. DOI: https://doi.org/10.15407/akademperiodyka.398.188
20. Когут Ю. Цифрова трансформація економіки та проблеми кібербезпеки. Київ : Сідкон, 2021. 368 с.
21. Міщенко В. І. Механізми регулювання процесів цифровізації для забезпечення національно укоріненої стійкості економічного розвитку. *Економічний простір*. 2024. № 189. С. 283–290. DOI: https://doi.org/10.32782/2224-6282/189-50
22. Мельник Л. Г., Карінцева О. І., Кубатко О. В. та ін. Цифровізація економічних систем та людський капітал: підприємство, регіон, народне господарство. *Механізм регулювання економіки*. 2020. № 2. С. 9–28. DOI: https://doi.org/10.21272/mer.2020.88.01
23. Криниця С. О. Поняття та сутність цифрової трансформації у публічних фінансах. *Науковий вісник Одеського національного економічного університету*. 2024. № 3–4. С. 63–70. DOI: https://doi.org/10.32680/2409-9260-2024-3-4-316-317-63-70
24. Парубець О. Цифрові інструменти управління місцевими фінансовими ресурсами. *Проблеми і перспективи економіки та управління*. 2023. № 4. С. 225–237. DOI: https://doi.org/10.25140/2411-5215-2023-4(36)-225-237

25. Петруха С. В., Палійчук Т. М., Петруха Н. М. Місцеві фінанси в умовах коронакризи: нова бюджетна архітектоніка та фінансова спроможність регуляції секторальних і соціально-економічних процесів. *Фінанси України*. 2020. № 12. С. 83–105. DOI: https://doi.org/10.33763/finukr2020.12.083
26. Петруха Н., Клименко К., Петруха С. Економіка та державні фінанси – феномен української незламності. *Вчені записки Університету «КРОК»*. 2024. № 2. С. 42–55. DOI: https://doi.org/10.31732/2663-2209-2024-74-42-55
27. Клименко К. В., Петруха Н. М., Петруха С. В. «Зелений» план Маршалла для України: фінансово-економічний та регуляторний контекст. *Наукові праці НДФІ*. 2024. № 1. С. 20–49. DOI: https://doi.org/10.33763/npndfi2024.01.020
28. Шубалий О. М., Петруха С. В., Косінський П. М., Петруха Н. М. Формування системи інформаційно-аналітичного забезпечення розвитку біопаливних виробництв на базі підприємств агросектору. *Наукові праці НДФІ*. 2023. № 3. С. 133–147. DOI: https://doi.org/10.33763/npndfi2023.03.133
29. Петруха Н. М., Петруха С. В. Державне регулювання інтегрованих корпоративних об'єднань в умовах структурно-інституціональної та функціональної трансформації сільської економіки: проблеми методології, теорії, соціально-економічної та секторальної політики : монографія. Київ : Видавничий дім «Професіонал», 2020. 496 с.
30. Digital Tiger: the Power of Ukrainian IT. Research for 2023. 2023. URL: https://itukraine.org.ua/files/ITU_GT.pdf
31. Зовнішня торгівля товарами (відповідно до КПБ6). Зовнішня торгівля послугами (відповідно до КПБ6). URL: https://bank.gov.ua/files/ES/Trade_m.pdf
32. Порядок використання коштів, передбачених у державному бюджеті за програмою «Електронне урядування» : затв. постановою Кабінету Міністрів України від 14.03.2012 р. № 236. URL: https://zakon.rada.gov.ua/laws/show/236-2012-п#n9
33. Державний веб-портал бюджету для громадян. URL: https://openbudget.gov.ua
34. Петруха С., Петруха Н., Куницький К. Інформаційно-консультаційне забезпечення розвитку аграрного сектору: зарубіжний досвід, рекомендації для України. *Економіст*. 2015. № 2. С. 36–41.
35. Порядок обміну електронними документами між Міністерством фінансів України та учасниками бюджетного процесу на рівні державного бюджету із застосуванням автоматизованої інформаційної системи онлайн-взаємодії з розпорядниками коштів державного бюджету : затверджено наказом Міністерства фінансів України від 27.03.2024 р. № 150. URL: https://zakon.rada.gov.ua/laws/show/z0465-24#Text
36. Триває реєстрація розпорядників бюджетних коштів та процес середньострокового планування в ІТ-системі бюджетного планування та моніторингу. URL: https://www.publicfinance.gov.ua/news/4
37. Вебдоступність сайтів державних органів влади : віт за результатами моніторингу. Київ, 2023. 24 с. URL: https://www.undp.org/uk/ukraine/publications/accessibility-state-authorities-websites-report-study-results
38. Cyber Conflict Briefing / data support by J. Bund, K. Zettl-Schabath, M. Müller, C. Borrett. *EuRepoC*. November 2023. URL: https://eurepoc.eu/wp-content/uploads/2023/12/EuRepoC-Cyber-Conflict-Briefing-November-2023-Final.pdf
39. Петруха С. В. Державне антикризове регулювання аграрного сектору економіки України : монографія. Київ : ЦУЛ, 2018. 521 с.
40. Петруха С., Петруха Н. До питання природи та ідентифікації структурних зрушень в економіці: методологічний аспект. *Економіст*. 2013. № 8. С. 23–26.

REFERENCES

Adelmann, F. et al. "Cyber Risks and Financial Stability : It's a Small World After All". *IMF Working Papers*. 2020. https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2020/12/04/Cyber-Risk-and-Financial-Stability-Its-a-Small-World-After-All-48622

Benni, N. *Digital Finance and Inclusion in the Time of COVID-19 : Lessons, Experiences and Proposals*. Rome: FAO, 2021.

"Cyber Conflict Briefing". *EuRepoC*. November 2023. https://eurepoc.eu/wp-content/uploads/2023/12/EuRepoC-Cyber-Conflict-Briefing-November-2023-Final.pdf

"Digital Tiger: the Power of Ukrainian IT. Research for 2023". 2023. https://itukraine.org.ua/files/ITU_GT.pdf

Derzhavnyi veb-portal biudzhetu dlia hromadian. https://openbudget.gov.ua

Digital Finance and the Future of the Global Financial System: Disruption and Innovation in Financial Services. New York, NY: Routledge, 2023.

Hrubiian, O., and Jeremic, D. "Public Finance Management Reform: Digitalization as a Tool to Lift Processes to a New Level of Governance and Eradicate Systemic Issues". *EU4PFM*. https://eu4pfm.com.ua/news/public-finance-management-reform-digitalization-as-a-tool-to-lift-processes-to-a-new-level-of-governance-and-eradicate-systemic-issues

Kau, G., Lashkari, Z. H., and Lashkari, A. H. *Understanding Cybersecurity Management in FinTech: Challenges, Strategies and Trends.* Cham: Springer Nature, 2021.

Klymenko, K. V., Petrukha, N. M., and Petrukha, S. V. "«Zelenyi» plan Marshalla dlia Ukrainy: finansovo-ekonomichnyi ta rehuliatornyi kontekst" [The Marshall's "Green" Plan for Ukraine: The Financial, Economic and Regulatory Context]. *Naukovi pratsi NDFI,* no. 1 (2024): 20-49. DOI: https://doi.org/10.33763/npndfi2024.01.020

Kohut, Yu. *Tsyfrova transformatsiia ekonomiky ta problemy kiberbezpeky* [Digital Transformation of the Economy and the Problems of Cyber Security]. Kyiv: Sidkon, 2021.

Kopp, E., Kaffenberger, L., and Wilson, C. "Cyber Risk, Market Failures, and Financial Stability". *IMF Working Papers*. 2017. https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104

Krynytsia, S. O. "Poniattia ta sutnist tsyfrovoi transformatsii u publichnykh finansakh" [Concept and Essence of Digital Transformation in Public Finance]. *Naukovyi visnyk Odeskoho natsionalnoho ekonomichnoho universytetu*, no. 3-4 (2024): 63-70. DOI: https://doi.org/10.32680/2409-9260-2024-3-4-316-317-63-70

[Legal Act of Ukraine] (2012). https://zakon.rada.gov.ua/laws/show/236-2012-п#n9

[Legal Act of Ukraine] (2016). https://zakon.rada.gov.ua/laws/show/92-2016-p#Text

[Legal Act of Ukraine] (2018). https://zakon.rada.gov.ua/laws/show/67-2018-p#Text

[Legal Act of Ukraine] (2021). https://zakon.rada.gov.ua/laws/show/n0055525-21#n2

[Legal Act of Ukraine] (2021). https://zakon.rada.gov.ua/laws/show/1467-2021-p#Text

[Legal Act of Ukraine] (2024). https://zakon.rada.gov.ua/laws/show/z0465-24#Text

Long, C. *Digital Public Financial Management. An Emerging Paradigm*. London: ODI Working Paper Series, 2023.

Melnyk, L. H. et al. "Tsyfrovizatsiia ekonomichnykh system ta liudskyi kapital: pidpryiemstvo, rehion, narodne hospodarstvo" [Digitization of Economic Systems and Human Capital: Enterprise, Region, National Economy]. *Mekhanizm rehuliuvannia ekonomiky*, no. 2 (2020): 9-28. DOI: https://doi.org/10.21272/mer.2020.88.01

Mishchenko, V. I. "Mekhanizmy rehuliuvannia protsesiv tsyfrovizatsii dlia zabezpechennia natsionalno ukorinenoi stiikosti ekonomichnoho rozvytku" [Mechanisms of Regulation of Digitization Processes to Ensure Nationally Rooted Resilience of Economic Development]. *Ekonomichnyi prostir*, no. 189 (2024): 283-290. DOI: https://doi.org/10.32782/2224-6282/189-50

Overby, H., and Audestad, J. A. *Introduction to Digital Economics. Foundations, Business Models and Case Studies*. Cham: Springer Nature, 2021.

Parubets, O. "Tsyfrovi instrumenty upravlinnia mistsevymy finansovymy resursamy" [Digital Tools to Manage Local Financial Resources of Territorial Communities]. *Problemy i perspektyvy ekonomiky ta upravlinnia*, no. 4 (2023): 225-237. DOI: https://doi.org/10.25140/2411-5215-2023-4(36)-225-237

Petrukha, N. M., and Petrukha, S. V. *Derzhavne rehuliuvannia intehrovanykh korporatyvnykh obiednan v umovakh strukturno-instytutsionalnoi ta funktsionalnoi transformatsii silskoi ekonomiky: problemy metodolohii, teorii, sotsialno-ekonomichnoi ta sektoralnoi polityky* [State Regulation of Integrated Corporate Associations in Conditions of Structural-institutional and Functional Transformation of the Rural Economy: Problems of Methodology, Theory, Socio-economic and Sectoral Policy]. Kyiv: Vydavnychyi dim «Profesional», 2020.

Petrukha, N., Klymenko, K., and Petrukha, S. "Ekonomika ta derzhavni finansy – fenomen ukrainskoi nezlamnosti" [Economy and Public Finances – The Phenomenon of Ukrainian Indomitability]. *Vcheni zapysky Universytetu «KROK»*, no. 2 (2024): 42-55. DOI: https://doi.org/10.31732/2663-2209-2024-74-42-55

Petrukha, S. V. *Derzhavne antykryzove rehuliuvannia ahrarnoho sektoru ekonomiky Ukrainy* [State Anti-crisis Regulation of the Agrarian Sector of the Economy of Ukraine]. Kyiv: TsUL, 2018.

Petrukha, S. V., Paliichuk, T. M., and Petrukha, N. M. "Mistsevi finansy v umovakh koronakryzy: nova biudzhetna arkhitektonika ta finansova spromozhnist rehuliatsii sektoralnykh i sotsialno-ekonomichnykh protsesiv" [Local Finances in the Context of the Coronacrisis: New Budget Architecture and Financial Capacity to Regulate Sectoral and Socio-Economic Processes]. *Finansy Ukrainy*, no. 12 (2020): 83-105. DOI: https://doi.org/10.33763/finukr2020.12.083

Petrukha, S., and Petrukha, N. "Do pytannia pryrody ta identyfikatsii strukturnykh zrushen v ekonomitsi: metodolohichnyi aspekt" [To the Question of the Nature and Identification of Structural Shifts in the Economy: Methodological Aspect]. *Ekonomist*, no. 8 (2013): 23-26.

Petrukha, S., Petrukha, N., and Kunytskyi, K. "Informatsiino-konsultatsiine zabezpechennia rozvytku ahrarnoho sektoru: zarubizhnyi dosvid, rekomendatsii dlia Ukrainy" [Information and Consulting Support for the Development of the Agrarian Sector: Foreign Experience, Recommendations for Ukraine]. *Ekonomist*, no. 2 (2015): 36-41.

"Stratehiia rozvytku finansovoho sektoru Ukrainy" [Strategy for the Development of the Financial Sector of Ukraine]. *Natsionalnyi bank Ukrainy*. https://bank.gov.ua/admin_uploads/article/Strategy_finsector_NBU.pdf?v=7

"Stratehiia rozvytku fintekhu v Ukraini do 2025 roku. Stalyi rozvytok innovatsii, keshles ta finhramotnist" [Fintech Development Strategy in Ukraine until 2025. Sustainable Development of Innovations, Cashless and Financial Literacy]. *Natsionalnyi bank Ukrainy*. 2020. https://bank.gov.ua/ua/files/DDWIAwXTdqjdClp

Shubalyi, O. M. et al. "Formuvannia systemy informatsiino-analitychnoho zabezpechennia rozvytku biopalyvnykh vyrobnytstv na bazi pidpryiemstv ahrosektoru" [Formation of the Information and Analytical Support System for the Development of Bio-

fuel Industries on the Base of Agricultural Sector Enterprises]. *Naukovi pratsi NDFI*, no. 3 (2023): 133-147. DOI: https://doi.org/10.33763/npndfi2023.03.133

Stigliz, J., Sen, A., and Fitoussi, J.-P. "Mis-measuring Our Lives: Why GDP Doesn't Add Up". *Sustainable*. https://elearning.unimib.it/pluginfile.php/566943/mod_resource/content/3/StiglitzSustainabilityE.pdf

Sustainable Development of Modern Digital Economy / ed. by J. V. Ragulina, A. A. Khachaturyan, A. S. Abdulkadyrov, Z. Sh. Babaeva. Cham: Springer Nature, 2021.

"Tryvaie reiestratsiia rozporiadnykiv biudzhetnykh koshtiv ta protses serednyostrokovoho planuvannia v IT-systemi biudzhetnoho planuvannia ta monitorynhu" [The Registration of Managers of Budget Funds and the Process of Medium-term Planning in the IT System of Budget Planning and Monitoring is Ongoing]. https://www.publicfinance.gov.ua/news/4

The Big Data Driven Digital Economy: Artificial and Computational Intelligence / ed. by M. A. Abdalmuttaleb, M. Al-Sartawi. Cham: Springer Nature, 2021.

The Institutional Foundations of the Digital Economy in the 21st Century / ed. by E. G. Popkova, A. Krivtsov, A. V. Bogoviz. Berlin: Walter de Gruyter GmbH & Co KG, 2021.

"Vebdostupnist saitiv derzhavnykh orhaniv vlady : zvit za rezultatamy monitorynhu" [Web Accessibility of Websites of State Authorities : Report on Monitoring Results]. Kyiv, 2023. https://www.undp.org/uk/ukraine/publications/accessibility-state-authorities-websites-report-study-results

Vyshnevskyi, V. P. et al. *Tsyfrovizatsiia ekonomiky Ukrainy: transformatsiinyi potentsial* [Digitization of the Economy of Ukraine: Transformational Potential]. Kyiv: VD «Akademperiodyka», 2020. DOI: https://doi.org/10.15407/akademperiodyka.398.188

"Zovnishnia torhivlia tovaramy (vidpovidno do KPB6). Zovnishnia torhivlia posluhamy (vidpovidno do KPB6)" [Foreign Trade in Goods (According to KPB6). Foreign Trade in Services (According to KPB6)]. https://bank.gov.ua/files/ES/Trade_m.pdf

УДК 338.49:334.012.64
JEL: L26; L53; L86
DOI: https://doi.org/10.32983/2222-4459-2024-6-79-93

ОСОБЛИВОСТІ ПРОЦЕСІВ ЦИФРОВІЗАЦІЇ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ В УКРАЇНІ

©2024 **РЕШЕТНЯК О. І., БЄЛІКОВА Н. В., ЮРЧЕНКО О. К., КАЛАШНІКОВА К. Ю.**

УДК 338.49:334.012.64
JEL: L26; L53; L86

Решетняк О. І., Бєлікова Н. В., Юрченко О. К., Калашнікова К. Ю. Особливості процесів цифровізації малого та середнього бізнесу в Україні

Метою статті є визначення ключових особливостей процесів цифровізації малого та середнього бізнесу в Україні. Аналізуючи й узагальнюючи наукові праці вчених, які були розміщені в базі даних Scopus, за допомогою програми VOSviewer за тематичним напрямом «цифровізація / digitalization» та «МСП / SMEs», було систематизовано погляди на цю проблематику дослідження. Також проведено аналіз сучасного рівня цифровізації малих і середніх підприємств (МСП) України, який продемонстрував, що впровадження та використання цифрових технологій є нижчим порівняно з рівнем цифровізації МСП країн ЄС, що обумовлює необхідність інтенсифікації впровадження цифрових технологій та інструментів для забезпечення їх конкурентоспроможності. Визначено ключові переваги та бар'єри щодо впровадження цифрових технологій у діяльність МСП України, охарактеризовано основні інструменти реалізації цифрової стратегії МСП і сфери їх застосування, зокрема для будівельної галузі. Серед основних перешкод щодо впровадження цифровізації МСП визначено: неможливість інвестування у цифрові інструменти, що мають високу вартість, і відносно високі операційні витрати на обслуговування; недостатність цифрових компетентностей у керівників і співпрацівників; протидія змінам з боку робітників і неготовність до змін з боку керівників. Надано рекомендації щодо цифровізації МСП України в умовах обмежених ресурсів: запровадження «культури навчання» в МСП, що має важливе значення для використання цифрових технологій; створення дорожньої карти досягнення бізнес-цілей цифровізації МСП, визначення чітких пріоритетів щодо цифрових перетворень залежно від критичності бізнес-проблем, які вони вирішують; налагоджування співпраці з компаніями, які можуть бути корисним для забезпечення ефективних процесів цифровізації, дослідження досвіду інших компаній; пошук можливостей отримання грантів та фінансової підтримки від державних програм і міжнародних організацій, спрямованих на підтримку цифровізації МСП; використання agile-підходів у впровадженні цифрових рішень задля забезпечення постійної готовності до швидких змін та адаптації до нових умов ринку.

Ключові слова: *цифровізація, цифрові технології, малі та середні підприємства, конкурентоспроможність, цифрова стратегія, будівельна галузь.*
Рис.: *2.* ***Табл.:*** *3.* ***Бібл.:*** *35.*

Решетняк Олена Іванівна *– доктор економічних наук, доцент, завідувачка сектора промислової політики та інноваційного розвитку відділу промислової політики та енергетичної безпеки, Науково-дослідний центр індустріальних проблем розвитку НАН України (пров. Інженерний, 1а, 2 пов., Харків, 61166, Україна)*
E-mail: *reshetele@ukr.net*
ORCID: *https://orcid.org/0000-0002-1183-302X*
Researcher ID: *https://www.webofscience.com/wos/author/record/520008*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57221964559*