УДК 338:351.865(477)
DOI: 10.18524/2413-9998.2022.3(52).275802

О. А. Маслій,
кандидат економічних наук,
доцент кафедри фінансів, банківського бізнесу та оподаткування,
Національний університет «Полтавська політехніка
імені Юрія Кондратюка»
Першотравневий проспект, 24, м. Полтава, 36011, Україна
e-mail: pugachaleksa@gmail.com

А. П. Максименко,
аспірант кафедри фінансів, банківського бізнесу та оподаткування,
Національний університет «Полтавська політехніка
імені Юрія Кондратюка»
Першотравневий проспект, 24, м. Полтава, 36011, Україна
e-mail: andrmaksymenko@gmail.com

РИЗИКИ ТА ЗАГРОЗИ ЕКОНОМІЧНІЙ БЕЗПЕЦІ УКРАЇНИ У ЦИФРОВІЙ СФЕРІ В УМОВАХ ВІЙНИ

У статті розкрито дуальний вплив цифровізації економіки на економічну безпеку держави. Узагальнено переваги та недоліки цифрової інфраструктури в умовах війни. Визначено ризики і загрози економічній безпеці держави у цифровій сфері в умовах війни. Проаналізовано особливості застосування ударів по цифровій інфраструктурі та використання цифрових технологій у ході сучасних конвенційних воєн. Доведено, що цифрова трансформація, з одного боку, сприяє підвищенню рівня економічної безпеки держави та стійкості національної економіки до впливу зовнішніх і внутрішніх викликів та загроз, а з іншого – є джерелом додаткових ризиків і небезпек у цифровій сфері. Проаналізовано динаміку кібератак РФ проти України як ключових загроз економічній безпеці держави у цифровій сфері. Доведено ефективність протидії ризикам і загрозам економічній безпеці України у цифровій сфері в умовах війни. Обґрунтовано пріоритетність проактивного забезпечення економічної безпеки України з перевагою якісного підходу над кількісним у розвитку як цифрових систем ураження, так і захисту, що потребує збільшення фінансового забезпечення економічної безпеки держави.

Ключові слова: економічна безпека держави, ризики, загрози, цифровізація, діджиталізація, кіберзагрози, війна.

Постановка проблеми у загальному вигляді. Цифровізація стала об'єктивною реальністю в усіх сферах діяльності людства. В сучасному діджиталізованому світі атаки на цифрову інфраструктуру є невід'ємною частиною війни, оскільки вони мають деструктивний соціально-економічний вплив, унеможлив-люють ведення ефективного протистояння та сприяють вичерпанню ресурсів. При цьому генерування загроз у цифровій сфері, як правило, потребує порівняно незначних витрат, супроводжується мінімальними ризиками для атакуючого при потенційно значному розмірі завданої шкоди. Тому передбачення ризиків та реальних загроз економічній безпеці у цифровій сфері, підготовка до них та вчасна реакція актуалізуються із зростанням рівня світового напруження, ескалації наявних конфліктів та у межах існуючих, зокрема і російського вторгнення в Україну.

Аналіз останніх досліджень і публікацій. Вагомий внесок у дослідження загроз економічній безпеці держави, механізмів протидії негативним чинникам безпеки, теоретико-методоло-гічних аспектів моніторингу макроекономічної стабільності зробили такі вчені, як: Барановський О. І., Власюк О. С., Варналій З. С., Жаліло Я. О., Онищенко С. В., Юрків Н. Я., Карпінський Б. А., Бондар Г. Л, а також Алвін Тофлер, Девід Хіршлейфер, Хенк Ян Райндерс, Джонатан Гордон, Олівія Вайт, Дуглас Брук та інші.

Однак, не дивлячись на актуалізацію цієї проблематики в умовах війни РФ проти України, яка є найбільшою конвенційною війною з 1953 року, аспект цифровізації економіки та поява новітніх засобів ураження через застосування у цій війні значної кількості хакерських атак проти інфраструктури, дронів, OSINT-методів розвідки, криптовалют утворюють якісно нові ризики й загрози економічній безпеці держави, які потребують ґрунтовних досліджень.

Постановка завдання. Метою дослідження є вивчення ризиків і загроз економічній безпеці України у цифровій сфері, оцінка

вразливості та резервів цифровізації в умовах війни для забезпечення економічної безпеки держави.

Виклад основного матеріалу дослідження. Війна, розв'язана Російською Федерацією проти України, є глобальним викликом системі міжнародної безпеки. За результатами дослідження Economist Intelligence Unit (EIU) ризики, які виникають внаслідок війни РФ проти України, можуть спричинити дестабілізацію економічної та суспільно-політичної ситуації у світі [1]. Тому в умовах сьогодення проактивне забезпечення економічної безпеки України задля підвищення стійкості національної економіки до впливу зовнішніх і внутрішніх викликів і загроз з урахуванням особливостей цифрової трансформації національної економіки та пов'язаних з цим ризиків набуває пріоритетного значення.

Невпинний соціотехнічний розвиток світової економіки, пов'язаний з новим технологічним переходом до інформаційної ери та домінуванням ринку послуг у розвинених країнах, зробив процес цифровізації невід'ємною складовою глобалізації. Цифрова інфраструктура ще сильніше поєднала світ, дала мережевий доступ одним країнам до інших, зробила мережу Інтернет глобальною. Разом із перевагами розвивалася кіберзлочинність і кібертероризм. Всі ці злочини відбуваються через анонімність агентів мережі Інтернет, у тому числі для посилення негативного впливу транснаціональних компаній, деструктивних спільнот та для реалізації ворожих дій на геополітичному рівні, що постійно генерує нові ризики та загрози для цифрової економіки.

Цифровізація – це впровадження цифрових технологій в усі сфери життя: від взаємодії між людьми до промислових виробництв, від предметів побуту до дитячих іграшок, одягу тощо. Це перехід біологічних та фізичних систем у кібербіологічні та кіберфізичні, тобто об'єднання фізичних та обчислювальних

компонентів. Перехід діяльності з реального матеріально-виробничого світу у світ віртуальних сервісів та онлайн-технологій [2].

Одночасний вплив цих двох факторів, створює феномен цифрової глобалізації. Але, окрім економічного і наукового розвитку, прискорення фінансових операцій і стимулювання розвитку людського потенціалу, він сприяє створенню нових методів і технологій для знищення реальної та цифрової інфраструктури, технологічного шпигунства, втручанню у вибори, розповсюдженню деструктивних ідей і «Fake news», що є реальними загрозами економічній безпеці держави у цифровій сфері.

Таким чином цифрова глобалізація перевела війни й конфлікти у нову площину, стала джерелом нових інструментів впливу на економіку та політичне середовище в умовах війни, а ризики й загрози в інформаційному просторі суттєво підривають обороноздатність країн. Кібертероризм, у тому числі і міждержавний, є одним із найбільш небезпечних ризиків економічній безпеці держави, оскільки це ефективний сучасний інструмент ведення війн та відстоювання геополітичних інтересів.

Прикладом військового застосування ударів по цифровій інфраструктурі є російсько-грузинська війна 2008 року, що супроводжувалася кібератаками на медіа-ресурси, сайти державних органів влади, в тому числі на сайт національного банку Грузії, з метою підриву керованості державою, створення Росією власної повістки цієї війни і обмеження витоку інформації з Грузії. Це можна вважати першим випадком військового вторгнення, що супроводжувалося скоординованою атакою у кіберсфері, яка мала спричинити паніку, виграти час для маневрування та агресивних дій, паралізувати економіку, адміністративні й фінансові інститути, позбавивши їх надійних джерел інформації, представити події у бажаному для себе світлі задля запобігання зовнішньополітичній реакції та санкціям тощо [3-4]. Окрім соціально-політичного впливу

кібератаки мали також і економічний: фінансові установи та малий бізнес сповільнили свою діяльність, електронні ЗМІ, провайдери та власники сайтів втратили доходи від трафіку тощо. Тому повне блокування цифрової інфраструктури під час війни є загрозою економічній безпеці держави з максимальним рівнем впливу, оскільки виступає тригером турбулентності економіки і макроекономічної дестабілізації.

Відносно невелика складова цифрових галузей у національній економіці Грузії у 2008 році та відсутність достатнього досвіду із забезпечення кібербезпеки – основні причини програшу Грузії у інформаційній війні, розв'язаній Росією одночасно з військовим вторгненням. Ця війна продемонструвала високу ефективність кібератак по цифровій інфраструктурі та безкарність атакуючого, а також відносну дешевизну таких атак, адже незначна кількість висококласних спеціалістів-хакерів може зруйнувати усю систему безпеки держави [5].

Застосування цифрових технологій у протистоянні країн може мати катастрофічний вплив на ключові параметри економічної безпеки на макрорівні. У цьому контексті найбільш вразливими в умовах цифрової трансформації є об'єкти критичної інфраструктури. Постійне зростання будівництва критичної інфраструктури (електростанцій, аеропортів, дамб, гребель, аерокосмічної галузі) вирішує поточні потреби, сприяє економічному зростанню, підвищує рівень ефективного використання технологій, проте створює мережу вразливих ланок, доступ до яких, при певному рівні проникнення, можуть мати як терористичні хакерські групи, так і розвідувальні агентства чи інші спецслужби різних держав.

Прикладом застосування цифрових технологій для враження критичної інфраструктури є інцидент «Stuxnet» у 2011 році, коли група хакерів проникла у систему керування іранською атомною електростанцією в місті Бушер на березі Персидської затоки.

Цілеспрямоване хакерське втручання чи помилка при проникненні, могла спричинити значну техногенну катастрофу для країн Перської затоки, загрозу світовому забезпеченню нафтою, а також викликати гуманітарну, інфраструктурну, цифрову, електричну, виробничу, екологічну та політичну кризу для Ірану. Групу, що стояла за атакою не було знайдено, як і не відомий рівень проникнення конфліктуючих держав у інфраструктуру один одного.

Варто відзначити, що конфліктуючі в умовах сьогодення країни, як то Південна Корея, Іран, Пакистан, Тайвань, Росія, Україна та інші, мають значну кількість об'єктів критичної інфраструктури, а їх критичне враження за впливом на економічну безпеку держави рівноцінне масовим ракетним атакам чи застосуванню ядерної зброї.

Іншими вразливими ланками є банківська та адміністративна система держави. Потужна DDoS-атака, може призвести до того, що банки втратять змогу виконувати свої функції, що надалі сповільніть або повністю зупинить оборот ресурсів, товарів і послуг у країні. Внаслідок цього може виникнути ризик невиконання деякими інституціями своїх функції, що в свою чергу несе в собі загрозу дестабілізації фінансової системи або ж, загалом, втрати державної керованості національною економікою.

З іншого боку цифрова економіка та інноваційні технології можуть виступати джерелами резервів для національної економіки під час війни та сприяти підвищенню стійкості національної економіки до зовнішніх і внутрішніх загроз за допомогою ринкових механізмів. Ця теза підтверджена в ході російсько-української війни, яка є найбільшою конвенційною війною з 1953 року, проте не виграна Росією у тому числі завдяки ефективній протидії загрозам у цифровій сфері та високому рівню діджиталізації економіки України.

Для РФ, з принципами петрократичної моделі поведінки, цифрова інфраструктура радше є допоміжною, тому коливання у цій галузі не мають впливу на її зовнішню політику. Проте у 2008 році, не дивлячись на світову кризу, частка інформаційних технологій у структурі ВВП РФ продовжила зростати і склала 3,7 %, а об'єм її цифрового ринку складав 31 млрд. дол. США [6]. Такі цифрові гіганти як «Яндекс» та «ВК» створювали якісні кадри та цифрову мережу для активних агресивних інформаційних дій та кадрового поповнення як хактивістів, так і професійних хакерів.

Росія, починаючи з 2007 року, активно вкладалася в цифрові засоби враження, починаючи із кібератаки на Естонію. У 2008 році подібні атаки передували масштабному вторгненню в Грузію і мали періодичний характер з 2014 року проти України. Особливу активність хакерські атаки мали напередодні повномасштабного вторгнення в Україну у 2022 році, спрямовані проти банківської системи, урядових сайтів, системи зв'язку [7-8]. Так, у лютому 2022 року за даними Державної служби спеціального зв'язку та захисту інформації України на державний сектор було здійснено близько 143 тис. кібератак, а з початком повномасштабного вторгнення РФ їх кількість кратно зросла до 42,7 млн атак у травні 2022 року (рис. 1).

Російсько-українська кібервійна 2014-2022 рр. є частиною гібридної війни та невід'ємною складовою широкомасштабної війни, котра була розпочата у 2022 році за грузинським сценарієм. Російська агресія проти України у цифровій сфері має три цілі: вразити енергетичну безпеку, створюючи перешкоди для ведення бойових дій на сході України; викрасти цінну фінансову, політичну й військову інформацію, завдавши фінансових втрат та знизивши інвестиційну привабливість України; підбурювати напруженість у суспільстві, провокуючи соціально-політичну кризу.

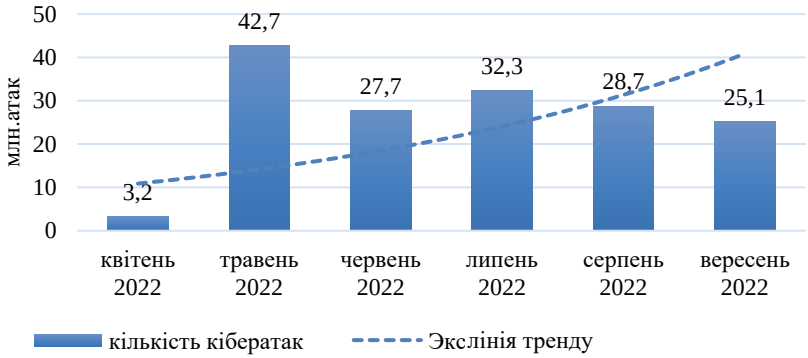

Рис. 1. Динаміка кількості кібератак на державний сектор України протягом квітня – вересня 2022 року

Джерело: побудовано за даними Держспецзв'язку України [9].

Загрозу становило використання російського або вразливого програмного забезпечення, що було скомпрометоване, створено з великою кількістю передбачених дефектів або передчасно заражене вірусними програмами. Такі програми довгий час знаходилися у роботі багатьох підприємств і через це хакери мали широкий доступ до баз даних різних установ. Також було скомпрометовано і вітчизняне, зокрема військове, програмне забезпечення, що могло видавати позиції українських військових [10-11].

Використання неякісного, дешевого, піратського або ненадійного програмного забезпечення створило безліч ризиків економічній безпеці України у цифровій сфері. Це було зумовлено мовними та фінансовими аспектами, так як аналогічне програмне забезпечення західних країн було на англійській мові та/або дорогими. Окрім того, поширенню загроз сприяло масове використання російських соцмереж «Вконтакте», «Одноклас-ники» та антивірусів «Лабаратория Касперского», «DoctorWeb». З рештою всі ці джерела небезпек були нейтралізовані на законодавчому рівні

шляхом прямої заборони їх використання в України, як один із контрзаходів цієї кібервійни.

Найбільшу небезпеку становив доступ хактивістів, хакерів та ворожих спецслужб до електромережі України. У 2015 році були атаковані «Прикарпаттяобленерго», «Чернівціобленерго» та «Київобленерго» з дистанційним відключенням підсистем, викраденням та видаленням даних, блокуванням дистанційного доступу. Не врятувало системи контролю навіть відсутність прямого підключення до інтернету, хактивісти та хакери змогли проникнути до них через систему внутрішньої мережі і довгий час розробляли її, створюючи все нові і нові загрози, маючи повний безперебійний доступ то пультів керування. На заваді повному знищенню підстанцій, що призвело би до значних фінансових та політичних втрат, стала поспішність атаки та зв'язок електростанцій з проросійськими олігархами, а також можливість ручного режиму керування підстанціями [12].

Таким чином, при певному рівні проникнення у цифрову сферу національної економіки, ворог може влаштувати «блекаут» для держави, вимкнувши її електромережу, і тим самим повністю зупинивши фінансову, адміністративну та інформаційну керованість. Проте, поки що такі операції надскладні, потребують багато часу і можуть бути нівельовані системою ручного керування. Тому у другій половині 2022 року РФ вдалася до ракетних і дронових ударів по енергоінфраструктурі, оскільки не змогла вразити її дистанційно.

Іншими цілями цифрових атак РФ в Україні були й потенційно можуть бути сервери Міністерства фінансів Україні, Державної казначейської служби Україні та Пенсійного фонду Україні. Такі атаки генерують загрози фінансовій, зокрема бюджетній, складовій економічної безпеки держави, проте навряд чи мають

стратегічний воєнний сенс, окрім як підірвати довіру до можливості державою виконувати свої функції.

Значну небезпеку становила атака на програму M.E.Doc у 2017 році, більш відома як атака «Petya». Ціллю цієї атаки були саме фінансового-економічні наслідки, зокрема параліч підприємств, розрахунків, створення недовіри до українського програмного забезпечення, шантаж підприємств і вимога викупу, шифрування та видалення даних. Через доступ лише до розробника утиліти була скомпрометована популярна програма, створений бекдор, а потім відбулося масове ураження усіх користувачів. З метою мінімізації зазначених загроз систематично виділяються додаткові кошти для оновлення систем захисту в держустановах.

Кібервійна РФ проти України у 2014-2022 рр. продемонструвала значну вразливість енергетичної, бюджетної, виробничої складової економічної безпеки держави при значному рівні цифровізації економіки у разі спланованих атак. Для запобігання загрозам економічній безпеці України у цифровій сфері за проактивним підходом до її забезпечення були заблоковані російські ресурси, через які проводилися атаки, виділене додаткове фінансування відділів цифрової безпеки у силових структурах, було профінансовано CERT-UA для активної протидії, з'явилися волонтерські рухи із протидії інформаційно-цифровим атакам (Inform Napalm, Миротворець, Український Кіберальянс), залучено трастовий фонд НАТО для оновлення програмного і технічного забезпечення, залучено іншу партнерську допомогу. Це призвело до кількісного та технічно-програмного покращення кіберзахисту України в умовах війни.

Вжиті превентивні заходи довели свою ефективність та своєчасність, адже напередодні повномасштабного вторгнення 14 січня 2022 року були атаковані держсайти Міноборони України, МЗС, ДСНС, «Дії» та інші. Ціль цієї атаки була репутаційною,

інформаційною проти дружніх відносин України та Польщі і, можливо, мала на меті оцінити реакцію з кіберзахисту української сторони [13]. 15-16 лютого 2022 року почалася DDoS-атака проти найбільших українських банків з метою дестабілізації суспільства, нанесення поточних збитків зменшуючи мобільність фінансової інфраструктури напередодні вторгнення, але атака була відбита силами безпеки українських банків, силових структур та за партнерської підтримки США [7]. 23-24 лютого 2022 року, під час вторгнення, відбулися масштабні атаки проти держсайтів, банків та логістичних доменів для дестабілізації суспільства, зупинки української економіки, подавлення витоку інформації, просування своєї парадигми, оскільки паралельно із самою атакою була розгорнута діяльність пропагандистів, проте атака своїх цілей не досягла.

Після цього атаки продовжувалися у значно слабшому вимірі, проте мали на меті інформаційно-політичні, а не безпосередньо економічні цілі, майже не застосовувалися по об'єктах цифрової та фінансової інфраструктури, оскільки банківські сервери були перенесені за межі території України, вийшовши із зони ураження російськими інформаційно-цифровими атаками. Згодом українські інформаційні сили здійснили успішну контратаку на російську цифрову інфраструктуру, в результаті чого була нанесена шкода секретній інформації, інфраструктурі, базам даних [7; 8; 14].

Отже, в цілому ефективність протидії ризикам і загрозам економічній безпеці України у цифровій сфері в умовах війни є високою. Цьому сприяла швидка цифрова трансформація національної економіки та реалізація резервів цифровізації. Частка інформаційних технологій у 2014 році складала 3,5 % у структурі ВВП України, а у період коронокризи вона зросла до 4,9 % у 2020 році. При цьому офіційний показник є заниженим, адже у сегменті інформаційних технологій висока частка тіньової економіки. У російському секторі IT ситуація дещо гірша внаслідок санкцій, зокрема

технологічних, та активній імміграції спеціалістів. Так, починаючи з 2014 року російський ринок IT-послуг значно скоротився й частка інформаційних технологій у ВВП РФ у 2022 році становила 2,7 % проти 4 % в Україні (рис. 2).

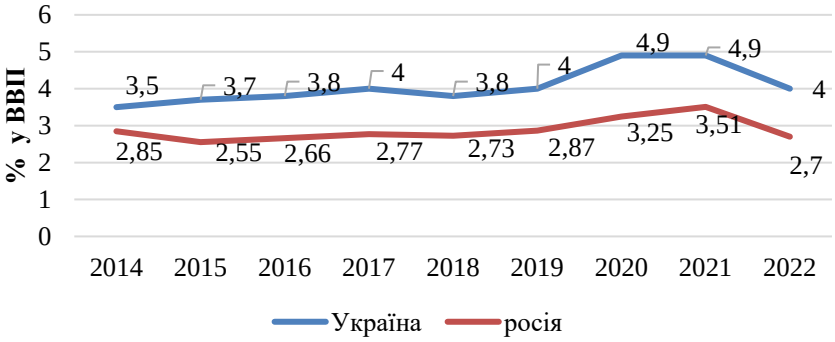

Рис. 2. Частка інформаційних технологій у структурі ВВП України та РФ протягом 2014-2022 рр.

За часткою інформаційних технологій у структурі ВВП Україна розвиває технологічну перевагу над РФ. Проте за обсягом ВВП РФ майже в 10 разів перевищує обсяг ВВП України, тому для забезпечення української кібербезпеки має реалізовуватися потенціал якості шляхом подальшого підвищення кваліфікації українських IT-спеціалістів, додаткової фінансової підтримки розвитку цифрового сектору національної економіки від міжнародних партнерів та залучення до кібервійни союзників, без загрози для них самих.

При цьому цифровізація в Україні створює додаткові резерви фінансової стійкості національної економіки в умовах війни. Варто відмітити, що й до війни фінансова безпека України знаходилася у обмежено негативному стані зі значним рівнем ризиків та загроз, а також деякими позитивними тенденціями загалом [15],

тому криза викликана COVID-19 та війною вдарили по слабкій економіці. Так, у загальній структурі експорту України третину займає експорт ІТ-послуг, який у 2021 році складав близько 36 % поряд із агропромисловим комплексом та сировинною промисловістю. У той же час передбачається подальший розвиток цифрового сектору національної економіки України під час війни, адже він сприяє надходженню валюти у країну та підвищенню економічної активності у турбулентний період. Крім цього розвиток цифрової сфери також сприяв формуванню вагомого джерела фінансового забезпечення економічної безпеки України в умовах війни шляхом акумуляції крипторесурсів, допомоги криптоінвесторів і криптобірж.

В цілому, галузь інформаційних технологій є найбільш стійкою, перспективною та виступає драйвером забезпечення економічної безпеки України в умовах війни та повоєнного відновлення. За попередніми результатами та тенденціями у 2022 році можна передбачити потенційні ризики та виклики економічній безпеці України у цифровій сфері.

Першим, найбільшим очевидним, є перенасичення ІТ-індустрії за таких умов спеціалістами-початківцями. Згідно з аналітикою Djinni, зарплатні очікування фахівців зменшилися, а на одну позицію в середньому претендує 12 спеціалістів, що в 5 разів більше, ніж в липні 2021 року. Ситуація ще гостріша для «джунів» – в цій ніші на одну вакансію припадає понад 30 спеціалістів [16]. Як наслідок це сприяє зменшенню плинності кадрів у компаніях і скороченню витрат для бізнесу, але дискримінує робітників і пришвидшує перегрівання галузі.

Працевлаштуванню українців у іноземних ІТ-компаніях, основних споживачах такого типу робочої сили, також не сприяють два фактори: віялові відключення електроенергії, які виключають можливість цілодобової присутності фахівця у проєкті, та ризик

втрати замовником фахівця, оскільки мобілізувати можуть навіть ключового спеціаліста у проекті. Перший виклик вирішується фірмами завдяки генераторам та системам «Starlink», а окремі спеціалісти можуть користуватися воркспейсом. А щодо другого виклику потрібне складне і пропрацьовано рішення держави, яке дозволить бізнесу, у тому числі закордонному, бронювати важливих спеціалістів. Проте із цим існують значні юридичні перешкоди, загальна складність соціальної складової та першочергові потреби національної безпеки.

Крім цього глобальні несприятливі тенденції, пов'язані із «перегріванням» ІТ-сектору світової економіки, виступають каталізаторами ризиків економічній безпеці України. Світовий ІТ-ринок потребує перезавантаження на тлі потенційно можливої рецесії після різкого сплеску потреб на цифровізацію під час карантинних обмежень. Тому світові компанії суттєво зменшують витрат, в тому числі шляхом звільнення понад 152 000 ІТ-фахівців у 2022 році [17]. В Україні також відбулося падіння на 3 % кількості працівників серед топ-50 ІТ-підприємств [18]. Такі тенденції можуть суттєво перешкоджати використання резервів цифровізації економіки України під час війни в контексті забезпечення економічної безпеки держави.

Висновки і пропозиції. Таким чином, цифровізація економіки створює чимало переваг: пришвидшує оборотність фінансових активів, знижує пороги та перешкоди до входження в бізнес, зменшує рівень всіх видів витрат шляхом автоматизації та доступу до глобального ринку праці, утворює нові робочі місця тощо. Передумовами виникнення цих переваг цифровізації можна визначити високу рентабельність ІТ, при низькій собівартості і невеликих інвестиціях у матеріальні активи, з якими, у випадку зовнішніх шоків, можуть бути перебої. Важливою є гнучкість та можливість працювати на внутрішній ринок, покриваючи попит національної

економіки на програмне забезпечення, інфраструктуру, а надлишки – реалізовувати назовні, без значних витрат на доставку послуг чи товарів, що є джерелом валютної виручки і має позитивний вплив на купівельну маржу. В цілому цифровізація економіки пришвидшує фінансові операції, оборотність активів, вивільняє кошти і ресурси, сприяє спрямуванню інвестицій у високоризикові та високоприбуткові старт-ап проєкти, що дозволяють стримувати спад національної економіки та підтримувати достатній рівень економічної безпеки держави в умовах війни.

Проте з іншого боку діджиталізація економіки робить її вразливою до хакерських атак, а знищення цифрової інфраструктури чи її аналогових складових може завдати значної шкоди обороноздатності країни та її економічній безпеці в умовах війни.

Так, основними ризиками і загрозами економічній безпеці України у цифровій сфері в умовах війни є: використання ворогом кібератак для економічної, політичної та військової розвідки; ураження об'єктів критичної інфраструктури з використанням цифрових технологій; перешкоджання діяльності державних і комерційних підприємств, установ, організацій; поширення фейк-ньюс для дестабілізації суспільства.

Зі зростанням рівня цифровізації економіки пріоритетність протидії кіберзагрозам є беззаперечною. Тому діджиталізація економіки має супроводжуватися пропорційним зростанням безпекових заходів: захистом даних, диверсифікацією ризиків, навчанням спеціалістів та поширенням медіаграмотності. При цьому зростаючі бюджетні витрати на безпекові заходи, що мають ключове значення в умовах війни, створюють нові ризики та виклики економічній безпеці держави у фінансовій сфері. Саме тому існує потреба в подальшому дослідженні і прогнозуванні впливу реальних загроз у цифровій сфері на всі складові соціально-економічної безпеки держави.

Використання цифрового простору у збройних конфліктах сьогодення потребує формування методики ідентифікації та оцінки нового типу цифрових загроз, що є фундаментальною основою державної кібербезпеки.

Список використаної літератури

1. Global operational risk review. How war is fuelling geopolitical uncertainty. Economist Intelligence Unit (EIU), 2022. URL:https://www.eiu.com/n/campaigns/operational-risk-review-2022.
2. Економічна стратегія України 2030. *Український інститут майбутнього*. URL: https://strategy.uifuture.org/index.html.
3. Keizer G. Cyberattacks knock out Georgia's Internet presence. Computerworld. URL: https://www.computerworld.com/article/2532289/cyberattacks-knock-out-georgia-s-internet-presence.html.
4. Swaine J. Georgia: Russia «conducting cyber war». The Telegraph. URL: https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html.
5. Hollis D. Cyberwar Case Study: Georgia 2008. *Small Wars Journal*. 2011. № 1. P. 1-9. URL: https://web.archive.org/web/20220304223742/https:/small-wars-journal.com/blog/journal/docs-temp/639-hollis.pdf.
6. Onyshchenko V., Yehorycheva S., Maslii O., Yurkiv N. Impact of Innovation and Digital Technologies on the Financial Security of the State. *Lecture Notes in Civil Engineering*. 2020. Vol. 181. P. 749–759. DOI: https://doi.org/10.1007/978%2D3%2D030%2D85043%2D2_69.
7. Нова кібератака на банки була «найбільшою в історії України» й досі триває. *BBC News Україна*. URL: https://www.bbc.com/ukrainian/news-60401775.
8. Dyer E. Russia's dreaded cyberwarriors seem to be struggling in Ukraine. *CBC News*. URL: https://www.cbc.ca/news/politics/russia-ukraine-cyber-cyberwar-1.6455055.
9. Кількість кібератак на Україну продовжує зростати. *Державна служба спеціального зв'язку та захисту інформації України*. URL: https://cip.gov.ua/ua/news/kilkist-kiberatak-na-ukrayinu-prodovzhuye-zrostati.
10. Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units. *Crowdstrike Global Intelligence Team*, 2016. 11 p. URL: https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf.

11. Geers K. Cyber War in Perspective: Russian Aggression against Ukraine. NATO CCD COE Publications, Tallinn, 2015, 175 p. URL: https://web.archive.org/web/20160816132103/https:/ccdcoe.org/multi-media/cyber-war-perspective-russian-aggression-against-ukraine.html.
12. Zetter K. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *WIRED*. URL:https://www.wired.com/2016/03/inside-cunning-unpreceden-ted-hack-ukraines-power-grid.
13. Тарасовський Ю., Антонюк Д., Сапітон М. Хакери атакували українські урядові сайти. Можлива причина – вразливість у системі управління контентом. Що треба знати. *Forbes*. URL: https://forbes.ua/news/khakeri-v-ataku-vali-ukrainski-uryadovi-sayti-ne-pratsyuyut-sayti-minoboroni-mzs-dsns-dii-140-12022-3212.
14. Як борються українські кібервійська. *Українська правда*. URL: https://www.pravda.com.ua/columns/2022/03/1/7327173.
15. Maslii O., Maksymenko A., Onyshchenko S. The Threats of Ukraine Financial Security: Identification and Systemization. *Економіка і регіон*. 2019. № 2 (73). С. 73–80. DOI: https://doi.org/10.26906/eir.2019.2(73).1629.
16. Григораш М. Як змінився український ринок IT за останні півроку. *SPEKA.media*. URL: https://speka.media/dereva-ne-rostut-do-nebes-abo-yak-zminivsya-ukrayinskii-rinok-it-za-ostanni-pivroku-v47edv.
17. Tech Layoff Tracker and Startup Layoff Lists. *Layoffs.fyi*. URL: https://layoffs.fyi.
18. Топ-50 IT-компаній України, літо 2022: кількість спеціалістів зменшилася на 3%, а у «великої п'ятірки» оновився склад. *DOU*. URL: https://dou.ua/lenta/articles/top-50-summer-2022.
19. Вишковська С. Як IT-індустрія розвиває інші галузі економіки у 2022 році. *Finance.ua*. URL: https://finance.ua/ua/goodtoknow/jak-it-industrija-rozvyvae-inshi-galuzi-ekonomiky.
20. Pugach A. A., Matkovskiy A. V. Analysis the Threats to Economic Security of Ukraine in Modern Conditions of Functioning the National Economy. *European Applied Sciences*. 2014. № 2. P. 196.
21. Маслій О. А., Глушко А. Д. Державне фінансове регулювання як інструмент мінімізації загроз економічній безпеці України в умовах воєнного стану. *Цифрова економіка та економічна безпека*. 2022. Вип. 2 (02). С. 125–130. URL: http://dees.iei.od.ua/index.php/journal/article/view/78/75.

Стаття надійшла 05.12.2022 р.

Oleksandra Maslii,
PhD in Economics,
Associate Professor of the Department of Finance, Banking and Taxation,
National University «Yuri Kondratyuk Poltava Polytechnic»
24, Pershotravnevy Avenue, Poltava, 36011, Ukraine
e-mail: pugachaleksa@gmail.com

Andrii Maksymenko,
Postgraduate student of Finance, Banking and Taxation Department,
National University «Yuri Kondratyuk Poltava Polytechnic»
24, Pershotravnevy Avenue, Poltava, 36011, Ukraine
e-mail: andrmaksymenko@gmail.com

RISKS AND THREATS TO UKRAINE'S ECONOMIC SECURITY IN THE DIGITAL SPHERE IN TIMES OF WAR

The article reveals modern trends and dual impact of economic digitalization on the economic security of the state. It was established that, in addition to economic and scientific development, financial operations acceleration and stimulation of human potential development, digitalization is a catalyst for real threats to the state economic security in the digital sphere. The advantages and disadvantages of the development, exploitation and existence of digital infrastructure in wartime are summarized. The peculiarities of the use of strikes on digital infrastructure and the use of digital technologies in the course of modern conventional wars were analyzed. It was determined that risks and threats to the state economic security in the digital sphere are an effective modern tool for waging wars and defending geopolitical interests. It was assessed the preconditions and historical course of the main digital threats to the Ukrainian economy caused by the aggressor state actions. It was proved that digital transformation, firstly, contributes to increasing the state economic security level and the resilience of the national economy to external and internal challenges and threats, and secondly, acts as a source of additional risks and dangers in the digital sphere. The dynamics of Russian cyberattacks against Ukraine as key threats to the state economic security in the digital sphere was analyzed. It was proved the effectiveness of counteracting risks and threats to Ukraine's economic security in the digital sphere in times of war due to the rapid digital transformation of the national economy and the digitalization reserves implementation. The main directions of minimizing risks and threats to the economic security of Ukraine in the digital sphere in the war conditions are determined. The priority of proactive ensuring of Ukraine's economic security with the advantage of a qualitative approach over a quantitative one in the development of both digital damage and protection systems was substantiated. The need to

increase the financial support of the state economic security in order to improve the systems and mechanisms of digital confrontation in the conditions of a conventional war was proven.

Keywords: state economic security, risks, threats, digitalization, cyber threats, war.

References

1. Economist Intelligence Unit (2022). Global operational risk review. How war is fuelling geopolitical uncertainty. Available at: https://www.eiu.com/n/campaigns/operational-risk-review-2022.
2. Ukrainian Institute of the Future (2022). *Ekonomichna stratehiia Ukrainy 2030* [Economic Strategy of Ukraine 2030]. Available at: https://strategy.uifuture.org/index.html.
3. Keizer, G. (2008). Cyberattacks knock out Georgia's Internet presence. Computerworld. Available at: https://www.computerworld.com/article/2532289/-cyber-attacks-knock-out-georgia-s-internet-presence.html.
4. Swaine, J. (2008). Georgia: Russia 'conducting cyber war'. The Telegraph. Available at: https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html.
5. Hollis, D. (2011). Cyberwar Case Study: Georgia 2008. *Small Wars Journal*, 1, pp. 1-9. Available at: https://web.archive.org/web/20220304223742/https:/smallwarsjournal.com/ blog/journal/docs-temp/639-hollis.pdf.
6. Onyshchenko, V., Yehorycheva, S., Maslii, O. & Yurkiv, N. (2020). Impact of Innovation and Digital Technologies on the Financial Security of the State. *Lecture Notes in Civil Engineering*. Volume 181. pp. 749–759. DOI: https://doi.org/10.1007/978%2D3%2D030%2D85043%2D2_69.
7. BBC News Ukraine (2022). *Nova kiberataka na banky bula «naibilshoiu v istorii Ukrainy» y dosi tryvaie* [New cyberattack on banks was «the largest in the history of Ukraine» and is still ongoing]. Available at: https://www.bbc.com/ukrainian/news-60401775 [in Ukrainian].
8. Dyer, E. (2022). Russia's dreaded cyberwarriors seem to be struggling in Ukraine. *CBC News*. Available at: https://www.cbc.ca/news/politics/russia-ukraine-cyber-cyberwar-1.6455055
9. State Service for Special Communications and Information Protection of Ukraine (2022) *Kilkist kiberatak na Ukrainu prodovzhuie zrostaty* [The number of cyberattacks on Ukraine continues to grow]. Available at: https://cip.gov.ua/ua/news/kilkist-kiberatak-na-ukrayinu-prodovzhuye-zrostati.
10. Global Intelligence Team (2016). Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units. Crowdstrike. Available at: https://www.crowdstrike.com/wp-content/brochures/FancyBearTracks UkrainianArtillery.pdf.

11. Geers, K. (ed.) (2015). Cyber War in Perspective: Russian Aggression against Ukraine. NATO CCD COE Publications, Tallinn, 175 p. Available at: https://web.archive.org/web/20160816132103/https:/ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine.html.
12. Zetter, K. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Available at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid.
13. Tarasovskyi, Yu., Antoniuk, D. & Sapiton, M. (2022). *Khakery atakuvaly ukrainski uriadovi saity. Mozhlyva prychyna – vrazlyvist u systemi upravlinnia kontentom. Shcho treba znaty* [Hackers attacked Ukrainian government websites. A possible reason is a vulnerability in the content management system. What you need to know – Forbes.ua]. Available at: https://forbes.ua/news/khakeri-v-atakuvali-ukrainski-uryadovi-sayti-ne-pratsyuyut-sayti-minoboroni-mzs-dsns-dii-140-12022-3212 [in Ukrainian].
14. Ukrainska Pravda (2022). *Yak boriutsia ukrainski kiberviiska* [How Ukrainian cyber troops are fighting]. Available at: https://www.pravda.com.ua/columns/2022/03/ 1/7327173/ [in Ukrainian].
15. Maslii, O., Maksymenko, A. & Onyshchenko, S. (2019). The Threats of Ukraine Financial Security: Identification and Systemization. *Economy and Region*, no. 2(73), pp. 73–80. DOI: https://doi.org/10.26906/eir.2019.2(73).1629.
16. Hryhorash, M. (2022). *Yak zminyvsia ukrainskyi rynok IT za ostanni pivroku* [Trees don't grow to the sky or how the Ukrainian IT market has changed over the past 6 months]. Available at: https://speka.media/dereva-ne-rostut-do-nebes-abo-yak-zminivsya-ukrayinskii-rinok-it-za-ostanni-pivroku-v47edv [in Ukrainian].
17. Layoffs.fyi (2022). Tech Layoff Tracker and Startup Layoff Lists. Available at: https://layoffs.fyi.
18. DOU (2022). *Top-50 IT-kompanii Ukrainy, lito 2022: kilkist spetsialistiv zmenshylasia na 3%, a u «velykoi piatirky» onovyvsia sklad* [Top 50 IT companies in Ukraine, summer 2022: the number of specialists decreased by 3%, and the «Big Five» has a new team] *DOU*. Available at: https://dou.ua/lenta/articles/top-50-summer-2022/ [in Ukrainian].
19. Vyshkovska, S. (2022). *Yak IT-industriia rozvyvaie inshi haluzi ekonomiky u 2022 rotsi* [How the IT industry will develop other sectors of the economy in 2022]. Available at: https://finance.ua/ua/goodtoknow/jak-it-industrija-rozvyvae-inshi-galuzi-ekonomiky [in Ukrainian].
20. Pugach, A. A. & Matkovskiy, A. V. (2014). Analysis the Threats to Economic Security of Ukraine in Modern Conditions of Functioning the National Economy. *European Applied Sciences*, vol. 2, p. 196.
21. Maslii, O. A. & Hlushko, A. D. (2022). Derzhavne finansove rehuliuvannia yak instrument minimizatsii zahroz ekonomichnii bezpetsi Ukrainy v umovakh

voiennoho stanu [State financial regulation as a tool to minimize threats to Ukraine's economic security under martial law]. *Tsyfrova ekonomika ta ekonomichna bezpeka*, vol. 2 (02), pp. 125–130. Available at: http://dees.iei.od.ua/index.php/journal/article/view/78/75 [in Ukrainian].