УДК 338.245:351.863
DOI: https://doi.org/10.32782/2224-6282/188-7

Максименко А.П.
аспірант кафедри фінансів, банківського бізнесу та оподаткування,
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
ORCID: https://orcid.org/0009-0006-6606-5132

Maksymenko Andrii
National University "Yuri Kondratyuk Poltava Polytechnic"

РЕАЛЬНІ ТА ПОТЕНЦІЙНІ ЗАГРОЗИ ЦИФРОВОЇ ЕКОНОМІКИ В УМОВАХ ВІЙНИ

У статті в хронологічний послідовності розкрито послідовну суперечливу роль цифровізації економіки та її вплив на економічну безпеку держави в умовах війни. На досвіді цифрового сектору та економіки шести держав у чотирьох кіберконфліктах узагальнено переваги та недоліки цифрової інфраструктури в умовах війни. Оцінено резервний потенціал, створений цифровізацією економіки, для забезпечення економічної безпеки держави в умовах військових дій та повоєнного відновлення. Проаналізовано специфіку та можливості завдання ударів по цифровій інфраструктурі, використання цифрових технологій у ході сучасних конвенційних воєн. Доведено дуальний вплив на забезпечення безпеки держави та стійкості національної. Проаналізовано динаміку та ефект від кібератак РФ проти Естонії, Грузії та України в короткостроковій та довгостроковій перспективах. Доведено ефективність протидії загрозам економічній безпеці України у цифровій сфері в умовах війни. Обґрунтовано подальші кроки розвитку проактивного забезпечення безпеки цифрової економіки України.

Ключові слова: *економічна безпека, загрози, інфраструктура, війна, цифровізація, глобалізація.*

REAL AND POTENTIAL THREATS TO THE DIGITAL ECONOMY IN WAR

The constant progress of science and technology, as well as the means of processing and transmitting information and the Internet in particular, has led to the massive spread of digital tools in all aspects of social activity. This leads to a major transformation of the economic and industrial infrastructure, has a significant positive effect on business development, but also has a corresponding effect on the development of crime. Thus, real and potential threats require special attention, particularly in the context of the global security crisis, the spread of wars and armed hybrid conflicts, and the increasing use of digital infrastructure for military purposes. The methods used in the paper include statistical, general mathematical, comparative, dialectical, systematic approach, and system analysis. The graphical method was used to build graphs, and presentation of the study uses the historical method. This article chronologically reveals the consistently contradictory role of economic digitalization in the state's economic security in times of war. Based on the experience of the digital sector of six countries in four cyber conflicts, the advantages and disadvantages of digital infrastructure in wartime are summarized. The reserve capacity created by the digitalization of the economy to ensure the economic security of the state in the context of hostilities and post-war recovery was assessed. The specificity and possibilities of striking digital infrastructure together with the use of digital technologies in modern conventional wars are analyzed. The dual impact of digital technologies on the security of the state and the sustainability of the national economy is highlighted. The dynamics and effects of Russian cyberattacks against Estonia, Georgia, and Ukraine in the short and long term are analyzed. The effectiveness of counteracting threats to Ukrainian economic security in the digital sphere during the war is proven. The article substantiates further steps to ensure the security of Ukraine's digital economy proactively. The article has practical implications for the development of state policy on measures to ensure economic security in the digital aspect. It can also be used for further systematic study of cyber warfare and threats to the digitalization of the national economy.

Keywords: *economic security, threats, infrastructure, war, digitalisation, globalisation.*

JEL Classification: *H56, O33*

Постановка проблеми. Досвід війн в епоху поширення мережевих технологій, широкого застосування програмного забезпечення та комп'ютерної обробки інформації, накопичений з початку XXI століття, демонструє суперечливі тенденції створювати як інфраструктурні вразливості, так і фінансові та кадрові резерви. Активне застосування хакерських атак, безпілотних апаратів, BIG DATA та OSINT методів розвідки, криптовалют тощо утворюють якісно нові загрози, що потребують актуалізації знань.

Аналіз останніх джерел досліджень і публікацій. Вагомий внесок у дослідження загроз економічній безпеці держави, механізмів протидії, теоретико-методологічних аспектів моніторингу, оцінці впливу цифровізації на військовій дії зробили такі вчені, як: Барановський О.І., Варналій З.С., Жаліло Я.О., Онищенко С.В., Юрків Н.Я., Карпінський Б.А., Маслій О.А. а також Алвін Тофлер, Девід Хіршлейфер, Дейл В.Джорсон, Пауль Ізбел та інші. Однак, не дивлячись на актуалізацію даної проблематики внаслідок цифрової глобалізації світової економіки, комплексні дослідження загроз цифровій інфраструктурі та економіці у контексті сучасної війни та новітніх засобів ураження потребують подальших досліджень з урахуванням досвіду повномасштабного російського вторгнення в Україну.

Мета статті. У рамках забезпечення економічної безпеки України метою дослідження є удосконалення методичного інструментарію вивчення та передбачення військово-економічних стратегічних загроз цифрової економіці, оцінка вразливості та резервного потенціалу цифрової економіки на основі систематиза-

ції та адаптації накопиченого світового та національного досвіду.

Виклад основних результатів дослідження. 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.

Синергія цифровізації, що стала доступною завдяки поширенню технологій, та глобалізації, яка прискорювалась із розквітом мережі Інтернет утворює новий економічно-суспільний контекст (рис. 1).

Важливим питанням протидії загрозам є здатність економіки цифрових послуг виступати резервною для воюючої держави. Визначаючи, резерв – це запас чого-небудь, який спеціально зберігається для використання в разі потреби. Резерв також трактують як невикористані можливості, засоби для здійснення чого-небудь [3].

Важливими аспектами резервів економіки є: висока ринкова ціна і ліквідність, легкість відтворення, стійкість до несприятливих умов, достатньо велика кількість. Для держави такими резервами можуть виступати: енергоресурси, рідкоземельні метали, внутрішні та зовнішні запозичення, мікрочіпи та системи їх виготовлення, агропродукція, добрива та інші продукти хімічної промисловості, технологічні інновації. Використати резерви можна також з різною метою.

Відомо, що петрократії – олігархічно-авторитарні режими засновані на володінні над запасами нафти чи газу, проводять більш агресивну зовнішню політику, чим вища ціна за барель нафти [14]. Таким чином енергоресурси в даному випадку виступають страхуванням, від можливих економічних втрат.

Цифрова продукція і ринок цифрових послуг є відносно новими та припали на відносно мирний період розвитку економіки, проте мають характеристики резервного потенціалу. Передумовами цього потенціалу можна визначити високу рентабельність IT, при низькій собівартості і невеликих інвестиціях у матеріальні активи, у поєднанні із високими прибутками галузі. 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. Останнім позитивним впливом є сумарний ефект від цифровізації і цифрової економіки, що пришвидшує фінансові операції, оборотність активів, вивільняє кошти і ресурси від автоматизації процесів, спрямовує інвестиції у високоризикові та високоприбуткові «стартап» проєкти, що дозволяють швидко рости і розвиватися національній економіці загалом.

Першою війною з активним застосуванням цифрових технологій та нової інфраструктури зв'язку – загальновизнано є війна у Перській затоці 1990–1991 років [7]. Проте економіка Іраку не була цифровізованою в 1990 р., так і у 2003 р., і не являється у 2022 р. Сам конфлікт спричинила суперечка довкола ціни на нафту – іракський лідер Саддам Хусейн звинуватив Кувейт та ОАЕ в надмірному видобутку, внаслідок якого ціна нафти впала до 7 доларів замість 18 [4], що підкреслює вплив нафти на воєнні дії. Попри те, що з 2003 року значно розвинувся мобільний зв'язок та інтернет, доступ до нього мали лише 5% населення Іраку через 4 роки після окупації силами коаліції та 10 років, після початку вторгнення та повалення режиму Каддафі [9].

Таким чином, не дивлячись на якісно новий тип застосування технологій, використання цифрової інфраструктури, – резервний потенціал цифрової економіки у контексті цієї війни розглянути неможливо. Доля сектору IT в економіці Іраку була і залишається низькою.

Так само і для США прогнозували класичні монетарні загрози економіки: прискорення та наближення рецесії, послаблення впливу долара. Окрім того перед-

Рис. 1. Визначення глобалізації і цифровізації та їх трансформація в цифрову глобалізацію

Джерело: складено авторами на матеріалах [1; 2]

бачалося завершення економічного циклу, що і так спричиняло негативні та деструктивні тенденції в економіці. Цифровий вплив Іраку проти США також був малоймовірним. Проте, попри стримані песимістичні прогнози, економіка США мала зростання, пов'язана як із швидкими успіхом на війні, так і з швидким відскоком циклу [8].

Хоча існує певна кореляція, між зростанням ВВП, різкому збільшенню частки інформаційних технологій у структурі економіки та цими війнами. Так у 1991 році ціни на комплектуючі до персонального комп'ютера стали значно знижатися. Звільнені таким чином кошти були направлені на розробку програмного забезпечення для цієї техніки, що ще сильніше прискорило розвиток використання ПК. У цей же час відбулося остаточне становлення мережі Інтернет у Сполучених штатах і за всі 90-ті роки складова інформаційних технологій у ВВП пришвидшила зростання з 4% до 17%, доки «криза доткомів» не зупинила роздутий оптимізм; значним чином приріст цієї індустрії почався саме у 1991–1992 рр. Потім відновлення галузі відбулося у 2003 році, коли приріст знову зріс з 4% до 11%, таким чином станом на 2020 рік складає 5,5% у загальній структурі ВВП, випереджаючи видобуткові, інфраструктурні, будівничі, агрокультурні та культурно-туристичні галузі і досягаючи показників сектору реальної торгівлі [10–13].

Проте США – демократична країною і частка інформаційних технологій у їх сукупному ВВП є значною, але відносно невеликою, щоб спровокувати чи спонсорувати розв'язання нових конфліктів, захищати від зовнішніх шоків у наслідок агресивних дій. Обидві війни з Іраком мали іноземних спонсорів, тому ІТ, як провокативний чинник, впливу не мав.

З іншого боку інформаційна економіка та інноваційні технології можуть виступати певними джерелами резервів, гасити негативні наслідки від зовнішньої політки. Якщо ворог не може повноцінно атакувати цифрову інфраструктуру, то сама система здатна, ринковими механізмами, справлятися із загрозами і мати загальний позитивний вплив на економіку.

Росія, починаючи з 2007 року, активно вкладалася в цифрові засоби ураження, починаючи із кібератаки на Естонію. У 2008 році подібні атаки передували масштабному вторгненню в Грузію і мали періодичний характер з 2014 року проти України.

Кібератаки проти Естонії показали загрози цифровізації економіки та приклад кібервійни з усіма її особливостями: безкарності, транскордонності, а також ефективності. Агенти ворожої держави, працюючи спільно з організованою злочинністю, можуть спричинити величезні затори на дорогах у найбільших містах країни – достатньо великі, щоб паралізувати бізнес, ЗМІ, уряд і державні служби, а також відрізати від світу. Це, безумовно, буде мало би розглядатися, як серйозний ризик для національної безпеки, якщо тільки атаки не відбуваються через Інтернет. На момент цих атак для більшості урядів захист національної безпеки від кібервійни – означав не допустити хакерів до важливих урядових комп'ютерних систем. І набагато менше уваги приділялося ризикам, пов'язаним з широкомасштабним порушенням роботи публічного інтернету [5].

Ці події змусили низку військових організацій по всьому світу переглянути важливість мережевої безпеки для сучасної військової доктрини та створено Центр передового досвіду НАТО з питань кооперативного кіберзахисту (CCDCOE).

Рядом академічних вчених був затверджений «Талліннський посібник», покликаний забезпечити глобальну норму в кіберпросторі, застосовуючи існуюче міжнародне право до кібервійни: держави не мають суверенітету над Інтернетом, але вони мають суверенітет над компонентами Інтернету на своїй території. Головною думкою другої редакції виступає твердження, що найбільш руйнівні дії слід розглядати як «збройні атаки» і держави мають право на самозахист від них. Проте, виступаючи думкою професійної спільноти експертів, він не мав подальшого значного впливу на воєнні доктрини чи конвенції, тому не утворив порядку ведення кібервійни.

Кібератаки у війні Росії проти Грузії у 2008 році були зосереджені на медіа-ресурсах, комунікаціях та мали на меті підірвати керованість державою, створити власну повістку цієї війни і обмежити витік інформації в довколишній медіа-простір. Все це мало спричинити паніку, виграти час для маневрування та агресивних дій, паралізувати економіку, адміністративні та фінансові інститути, позбавивши їх надійних джерел інформації, погасити зовнішньополітичну реакцію та санкції, виставити події у бажаному для себе світлі тощо [17–18]. Ці атаки мали на меті нанести соціально-політичну та економічну шкоду, завдати Грузії збитків та додатково послабити грузинську економіку, виходячи з думки, що основну атаку взяли на себе «хактивісти» [19], то шкода була нанесена значно більша за витрати. При тому, незначна кількість висококласних спеціалістів-хакерів може переважати над усією системою безпеки держави, особливо якщо вони можуть підготуватися до атаки, вторгнувшись у систему зарання [15].

Постає питання джерела переваги в спеціалістах, потужності та можливостях Росії проти Естонії та Грузії: чи було це викликано лише економічно-військовою перевагою, чи й технологічною також.

Частка цифрових технологій у ВВП Грузії була об'єднана у групу «Комунікації» і мала відносно незначний вклад, так у 2007 доля становила 3,13%, а за підсумками першого півріччя, до початку бойових дій, вже 3,3% і складала близько 18% приросту ВВП, та за підсумками року вона склала 14,5% приросту у частці ВВП і була другою за величиною приросту, коли всі інші галузі, окрім видобування руди, торгівлі та державного соціального сектору, зазнали значного спаду внаслідок війни.

Сектор інформаційних технологій Естонії у відповідні роки складав 4,64% та 4,57% і зазнав незначного спаду, відповідно до зміни у структурі експорту та початку світової рецесії 2008 року. Проте це призвело до скорочення зовнішнього рахунку поточних операцій та продовження зростання експорту, зокрема і завдяки транзиту російської нафти [26].

Можна зазначити, що через відносно невелику складову цифрових галузей у національній економіці Естонія у 2007 році та Грузія у 2008 році не мали достатнього досвіду і цивільно-комерційного захисту у цій інфраструктурі, а тому зазнали значного тиску під час війни. Та, порівняно із відповідною часткою у Росії (рис. 2), Грузія мала аналогічні показники, а Естонія навіть більше, проте їх ВВП у ці роки було в

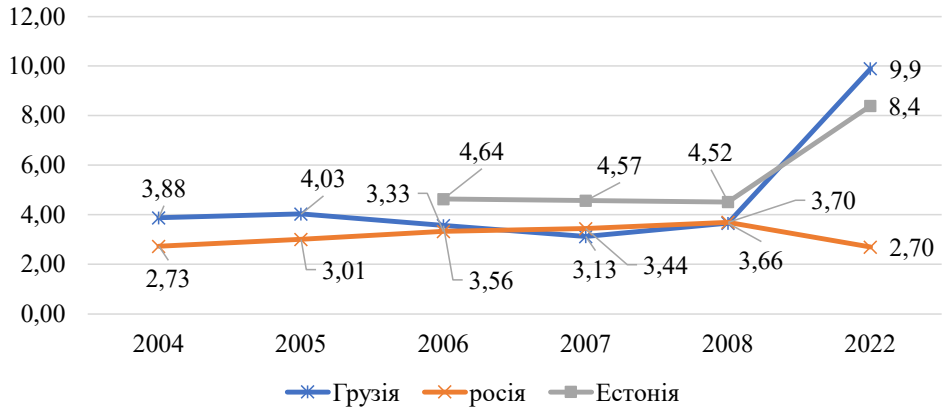

Рис. 2. Частка інформаційних технологій у складі ВВП Грузії, Естонії та росії, 2004–2022 рр.

Джерело: складено авторами на матеріалах [16; 20–24]

три-чотири менше від розміру цифрового ринку Росії, тому вони самостійно не могли протистояти підготовленим цифровим нападам, до яких залучали багато «хактивістів».

З іншого боку, галузь цифрових технологій змогла швидко відновитися і хоча дещо втратила потенціал – все одна була складовою відновлення Грузії. Зараз частка ІТ складає близько 10% ВВП і є важливою галуззю в економіці. Грузія стала популярної країною для релокейту спеціалістів з ІТ для усієї Східної Європи та Центральної Азії.

Естонія, у свою чергу, демонструє протилежні показники, де після кібератаки у 2007 році в наступному – скоротилася частка ІТ у ВВП, попри зростання користувачів мережі Інтернет та кратному збільшенню електронних сервісів за цей період.

Для Росії, з принципами енергоресурсної моделі економіки, цифрова інфраструктура виступає допоміжним джерелом доходів та середовищем для вербування спеціалістів. У 2008 році, не дивлячись на світову кризу, частка інформаційних технологій продовжила зростати і склала 3,7%. Попри те об'єм ринку складав 31 млрд дол. США і подібні цифри були потім лише у 2011–2013 роках, і станом на 2023 рік такі значення не було відновлені.

Можна зробити припущення, що внаслідок агресивних дій цей ринок скорочувався і не міг бути повноцінним резервом для економіки, попри те що сам мав приріст. Такі цифрові гіганти як «Яндекс» та «ВК» здебільшого приносили додатковий дохід в економіку, створювали та переманювали якісні кадри, сприяли розвитку цифрової мережі для інформаційних операцій та сфери застосування «м'якої сили».

Об'єктивною реальністю, на той період, була відсутність достатнього рівня протоколів захисту інтернет-мереж, недостатній розвиток цивільних та військових систем протидії DDoS-атакам тощо. Тож, Росія мала змогу задіяти і високоякісні кадри і «хактивістів», через розвинену мережу форумів, та таким чином агресор використав значну перевагу не лише на землі, воді і в повітрі, а й у цифровому просторі де завдав значної шкоди незахищеній від цифрового впливу економіці Грузії, спершу провівши тести без очікувань проти Естонії, завдавши їй економічних збитків.

Головним протистоянням у сучасній історії кіберсфери є російсько-українська кібервійна 2014–2023 рр. Напередодні повномасштабного вторгнення Росія сподівалася повторити успіх грузинської кампанії, оскільки проросійські пропагандисти і «хактивісти» ставили на три цілі: створити перешкоди для протидії вторгненню, встановити контроль над інформацією та спровокувати соціально-політичну кризу.

Ще одним місцем протистояння у кібервійні – став ринок криптовалют, де Україна та Росія є лідерами з володінням криптовалют у населення.

Для України акумуляція крипторесурсів стала джерелом надходжень та можливістю швидко використати стабільні цифрові валюти, а влада швидко організувала відповідну інфраструктуру, 16 березня 2022 року були остаточно підписані закони, що легалізували криптовалюту. Також вплив мала новітня технологія NFT, коли прибуток від продажу цифрових токенів спрямовувався на гуманітарні чи військові потреби.

Для Росії вони стали засобом обходу санкцій, оскільки ззовні відслідкувати чи контролювати переміщення такого роду активів майже неможливо. Також ними була розбудована тіньова цифрова інфраструктура, а тому криптовалюти допомагають знижувати економічний тиск, проводити тіньові схеми і отримувати підсанкційні ресурси. Замість легалізації наявної некримінальної мережі, яка також була розглянута на початку 2023 року, Росія заявила про наміри створити цифровий рубль, рівноцінний готівковому та безготівковому. Маючи на меті монополізацію, посилення регулювання монетарно-фінансової безпеки та обхід санкцій.

У структурі ВВП України частка сектору інформаційних технологій у 2014 році складала 3,5% (тут і далі без урахування тимчасово окупованих територій), відносно невелике значення, порівняно з 10% у переробної галузі та сільським господарством. Усупереч тезі про резервність цієї галузі у 2015–2016 роках зростання складало 0,3–0,1%.

Варто відзначити, що частка ІТ значно зросла у період коронокризи, коли цифрова інфраструктура стала набагато більш потрібною, до 4,9% у 2020 році. Експорт ІТ-послуг у 2021 р. складав 36% та 43% на І квартал 2023, конкуруючи із агропромисловим комплексом та сировиною. У кінці 2022 року вона стала єдиною галуззю, якій вдалося наростити експорт на 5,8% під час повномасштабного вторгнення, попри очікування у 40–45% [32], а станом І півріччя 2023 року

експорт зменшився на 9,3% у порівнянні з таким же періодом минулого року.

Станом на 2022 рік частка ІТ у ВВП склала 4,6% у 2–3 рази поступаючись АПК та переробній промисловості, проте значно збільшивши частку у 3 і 4 кварталі. Також значна кількість вчених та підприємців передбачають подальший розвиток цифрового сектору під час війни і, попри загальноекономічний спад, можливість до подальшого розвитку і перебудови ринку. Тим самим ІТ може забезпечувати економіку валютою та оборотністю у турбулентний період, важливий вплив має і потенціал для військового програмного забезпечення.

В Україні також відбулося падіння кількості працівників на 6,6% за пів року серед найбільших 50 підприємств, скоріше за все звільнення працівників у менших проєктах склали більші цифри, впритул до закриття і ліквідації. Показники бронювання працівників ІТ склали усього 1,4%, попри незначне зростання кількості таких працівників, що перебувають на службі в ЗСУ [33]. Це може становити загрозу виходу компаній з ринку та за закриттям поточних контрактів, можуть бути призупинені подальші відносини, з безпекових аспектів, через можливість «зриву» проєктів.

Що стосується російського сектору ІТ, то у 2014 році ринок та експорт ІТ-послуг значно скоротилися на 38% та 12% відповідно [29], що стало наслідком введених санкцій, загостренню соціально-політичного режиму всередині країни і початку відтоку спеціалістів та бізнесу. Сам сектор відновився після падіння і стагнації лише у 2021 році, причиною чому стала коронокриза та послідуюча потреба у цифровізації що спричинила зростання на 8%, станом на 2022 рік ІТ складає 2,71%. Проте залишилася однією з небагатьох, що не зазнала значного спаду і після шокового періоду має приріст близько 6–8% на квартал до попереднього [29], а активні дії держпосадовців із лобіювання цієї галузі, зокрема надання відстрочок від призову, має на меті стимулювання. Основний попит припав на державні воєнні замовлення або на імпортозаміщення для російського бізнесу. Попри те дослідники відмічають значний ріст зарплат, що може свідчити про кадровий голод.

Таким чином, ринковий вакуум, що виник після введення санкцій внаслідок вторгнення Росії в Україну у 2022 році, призвів до наростання попиту на заміщення послуг. Подальші технічні санкції, виведення цифрових фінансових інструментів (SWIFT, MasterCard, Visa), а також активні бойові дії з використанням значної кількості програмного забезпечення та складної програмної інженерії лише збільшували запити, чим частково перекрили збитки від втрати експорту.

Порівнюючи частку інформаційних технологій в економіці України та Росії (рис. 3) видно, що Україна мала та розвивала технологічну перевагу, проте усе одно стикалася з постійними атаками і мала недостатньо розвинену систему кібербезпеки. Економіки двох держав – неспівставні, майже десятикратна різниця і тому для української кібербезпеки потрібні додаткові економічні вливання та додаткова кваліфікація, що забезпечувалася партнерами, таким чином реалізуючи потенціал якості.

Тому слабкість галузі – означає низьку якість кадрів, у тому числі кримінальних та військових. Атака на цифрову інфраструктуру України 14 січня мала деструктивний вплив, проте вже 23–24 лютого була менш сильною, аніж передбачалося, і не завдала значних руйнацій. Україна зберігала керованість і фінансово-цифрову інфраструктуру, зокрема мобільний банкінг та можливість розраховуватися картками. Також це дало змогу українській стороні нанести аналогічні атаки, за підтримки світових «хактивстів» і міжнародної партнерської допомоги, пошкодивши цифрову інфраструктуру Росії, після чого активних дій у кіберпросторі довго не спостерігалося до атаки на мережу «Київстар» та атаки ГУР на податкову службу РФ у грудні 2023.

Таким чином сектор цифрової економіки під час війни має резервні характеристики, зокрема він в обох країнах не зазнав значного спаду. Значно більший потенціал він має усередині країни, за рахунок імпортозаміщення та потреб воєнного чи карантинного часу, аніж назовні країни. Безпекові аспекти та високі ризики інвестицій та співпраці з агентами у зоні воєнних дій не дозволяє ІТ бути рівноцінною заміною енергоресурсів чи продукції аграрного сектору, оскільки попит на них лише зростає внаслідок катастрофи чи кризи.

Саме тому резервний потенціал цифрової економіки в першу чергу варто розглядати, через призму внутрішнього попиту і лише потім, як потенційний ринок збільшення доходів від експорту.

Цифрова економіка України двічі, за останній час, потребувала швидкої трансформації на засадах

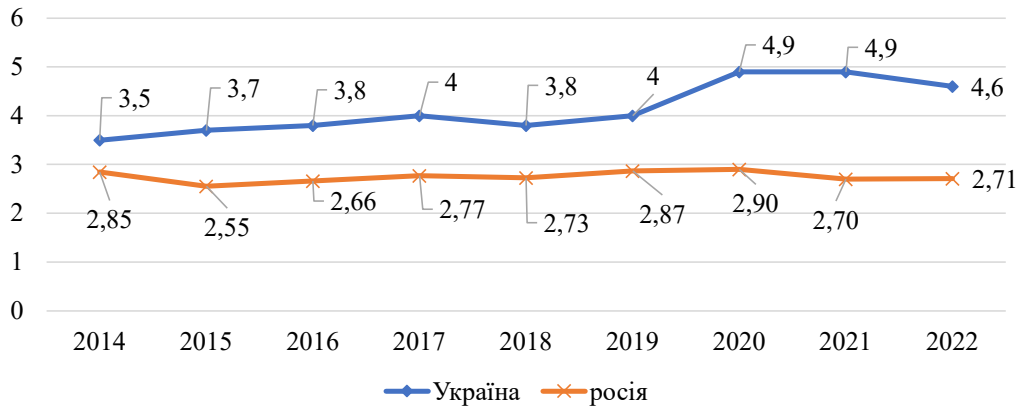

Рис. 3. Частка інформаційних технологій у складі ВВП України та росії, 2014–2022 рр.

Джерело: складено авторами на матеріалах [27–30]

дистанціювання, цифровізації, аутсорсу та сервитизації, цьому сприяла розвинута інфраструктура, зокрема пошти, швидкісного мобільного Інтернету, онлайн-банкінгу і відносна дешевизна праці ІТ-спеціалістів на внутрішньому ринку. Так, вперше, в умовах карантинних обмежень ключову роль у збереженні економічної активності відіграли резерви цифровізації економіки.

Приріст електронної комерції через пандемію за 2020 рік склав 33% при прогнозних 15%, а за 2022 рік – він становив 27%. Стосовно показника сервитизації, то порівнюючи з 2019 роком роздрібний продаж у квітні 2020 року зменшився на 15%, у травні 2020 року – ще на 3,1%, а приріст показників на 15,7% відбувся лише у жовтні. У 2022 році у 2022 році показник роздрібної торгівлі впав на 21,4% і ще на 9,1% у І кварталі 2023 р. Це означає, що вперше українській економіці знадобилося 7 місяців для сервитизації послуг. Вдруге спад продовжується і через 12 місяців, проте має тенденцію до сповільнення.

Що стосується загальноекономічних показників, то обсяг ВВП України у 2020 році через жорсткі карантинні обмеження скоротився на 3,8%, а вже протягом 2021 року відбулося його зростання на 3,4%. На відміну від пандемії економічні наслідки воєнного стану значно масштабніші. Спад ВВП у 2022 становив 29,1% що приблизно на 10% менше від очікуваного. Це вказує на необхідність залучення значно більших резервів ніж ті, що бути використані протягом 2020–2021 років. Тому, на відновлення втраченої економіки, інфраструктури, повернення інвестиційної привабливості можуть знадобитися десятиліття або значні фондові програми. Якщо розраховувати час на сервитизацію пропорційно до витрат ВВП, то на це має піти 54 місяці, проте передбачений на 2023 рік ріст ВВП сктановить 2,9%.

Таким чином галузь інформаційних технологій та цифрової економіки не створила достатньо ресурсів, щоб перекрити економічні втрати, але попри те і втратила власних показників в умовах постійних пошкоджень, відтоку кваліфікованих кадрів та високих ризиків. За таких умов галузь є перспективною з точки зору забезпечення економічної безпеки держави, проте не створює значного резерву для України.

Зростання експорту цієї галузі здебільшого пов'язано із тимчасовою окупацією частин українських областей, блокуванням портів, руйнацією підприємств та значними мінуваннями територій, відсутністю достатньої логістики та інфраструктури для наземного вивезення продукції.

З іншого боку, приклад Росії показує можливості переорієнтації цифрового сектору на задоволення власних потреб, неможливий для більшості інших секторів економіки. Цифрова глобалізація створила значний внутрішній та зовнішній постійний попит на послуги.

Але галузь інформаційних технологій та цифрової економіки важлива не лише економічних впливом, а й кваліфікаційним. Враховуючи велике залучення до війни комп'ютерів, складної програмованої техніки, інструментів мережі Інтернет – військо потребує відповідних кадрів.

Іншим ефектом і ціллю залучення цифрової економіки до війни є виникнення, поширення та розвиток галузі «Military-Tech». Починаючи з 2014 року і таких проєктів, як програми «Кропива» й «Дельта», безпілотників «Валькірія» і «Лелека-100» і продовжуючи сучасними рішеннями, створеними після початку повномасштабного вторгнення. Яким, разом із військом, потрібна велика кількість відповідних висококваліфікованих кадрів.

Серед об'єктів розробки: військове програмне забезпечення, повітряні, морські та наземні безпілотні апарати, навчальні симулятори, радіостанції, кібербезпека та моніторингові програми, баражуючи боєприпаси, антидронові системи, твердопаливні двигуни тощо. Ці сфери і є внутрішнім резервом для України, який можливо не покриває економічного занепаду, проте конвертуючи у безпековий аспект, покриває запити і потреби війська.

Таким чином, звертаючи увагу на повоєнне відновлення і резервність цифрової економіки у цьому напрямі, можна зазначити, що Україна матиме значний досвід і напрацювання, перевірені бойовими діями. Варто також очікувати на спад попиту після завершення активних бойових дій.

Разом із тим безпекові рішення можуть бути потрібні не лише у військовому аспекті. Враховуючи регіоналізацію, характерну для цифрової глобалізації, утримання провідних позицій на цьому ринку можуть якісно змінити економіку і вивести державу з аграрно-ресурсного на товаро-технологічний рівень розвитку. Але на заваді знову можуть стати класичні загрози: нестача інвестицій, непрозоре фінансування та рейдерські захвати, бюрократія і недостатній або надмірний нормативний супровід тощо.

Окремо варто відміти залучення до кібервійни союзників, без загрози для них самих. Росії у атаці допомагали, за деякими журналістськими даними, сили КНР [26], Грузії у 2008 році – Німеччина та Естонія [17], а під удар тоді попала і нейтральна Туреччина [16], Україні допомагають країни НАТО [6; 26]. Таким чином, розвиненого сектору цифрової економіки дозволяє брати участь у кіберконфліктах, без прямого залучення, виключено за рахунок професійних кадрів та протоколів захисту.

Передача технологій та комплексних рішень, особливо у сфері кібербезпеки, може становити ключову роль розвитку несилової допомоги, а питання контролю над суверенними частинами інтернету поставатимуть все гостріше із подальшою цифровою глобалізацією.

Висновки. Цифрова економіка одночасно поєднує критичні та резервні аспекти. Вона є важливою інфраструктурою сучасних бізнес-процесів і її враження хакреськими атаками чи фізичними ударами по енергетичній інфраструктурі здатні призвести до непропорційно великих збитків. З іншого боку вона може покривати внутрішній попит для імпортозаміщення та локалізації, слугує джерелом кадрів для війська, «Military-Tech» та кібербезпеки, має гарні показники експорту, приносить великі валютні надходження, потенційно може бути драйвером повоєнного відновлення.

У той самий час чим більший рівень цифрової глобалізації країни – тим більші загрози і пропорційно ним – більші витрати на забезпечення безпеки: захист персональних даних, диверсифікацією ризиків, навчання спеціалістів та поширення медіаграмотності.

Також від розвитку галузі залежить кількість цивільних та військових спеціалістів, ціна розробки та якість програмного забезпечення, а також можливості залучати «хактивістів» до інфовійни та цифрового протистояння, можливість забезпечувати безпеку власної цифрової інфраструктури та наносити удари по ворожій. Додаткову роль грає можливість проведення безкарної допомоги в кіберсегменті; OSINT-розслідувань, які грають на інформаційне забезпечення мирного населення, та пошук військових цілей.

Тому покладання великих надій виключно на галузі цифрової економіки – є проявом надмірної віри в ефект технологій, проте воєнне значення у період активних бойових дій із залученням все нових засобів та інструментів – переоцінити складно. Цифрова індустрія не є золотою жилою, оскільки окрім великої кількості потенційних переваг, вона створює і значні вразливості та інструменти для злочинних дій, а це в свою чергу потребує безпекових заходів та своєчасних нормативно-регуляторних дій.

Список використаних джерел:

1. Глобалізація. Посібник з освіти в області прав людини за участі молоді. URL: https://www.coe.int/uk/web/compass/globalisation (дата звернення: 11.10.2023).
2. Економічна стратегія України 2030. *Український інститут майбутнього*. URL: https://strategy.uifuture.org/index.html (дата звернення: 11.10.2023).
3. Бусел В.Т. Великий тлумачний словник сучасної української мови. Ірпінь: ВТФ "Перун", 2003. 1087 с.
4. Plans for New Nuclear Reactors Worldwide. URL: https://world-nuclear.org/information-library/current-and-future-generation/plans-for-new-reactors-worldwide.aspx#:~:text=Today%20there%20are%20about%20440,10%%20of%20the%20world's%20electricity (дата звернення: 15.10.2023).
5. Cyberwarfare. Wayback Machine. URL: https://web.archive.org/web/20081209081836/http://www.economist.com/world/international/displaystory.cfm?story_id=E1_JNNRSVS (дата звернення: 20.10.2023).
6. Нова кібератака на банки була "найбільшою в історії України" й досі триває. URL: https://www.bbc.com/ukrainian/news-60401775 (дата звернення: 21.10.2023).
7. Toffler A. War and anti-war. New York, NY : Warner Books, 1995. 370 p. URL: https://archive.org/details/WarAndAntiWar-Toffler (дата звернення: 25.10.2023).
8. Isbell P. Economic Aspects of the War in Iraq. URL: https://www.realinstitutoelcano.org/en/analyses/economic-aspects-of-the-war-in-iraq/ (дата звернення: 26.10.2023).
9. Ірак через 10 років після війни: цифри і факти. URL: https://www.bbc.com/ukrainian/news/2013/03/130321_iraq_war_numbers_10years (дата звернення: 14.11.2023).
10. Jorgenson D.W. U.S. Economic Growth in the Information Age. *Issues in Science and Technology*. 2001. Vol. 18. No. 1. URL: https://issues.org/jorgenson/ (дата звернення: 01.11.2023).
11. Gross Domestic Product by Industry for 2003. U.S. URL: https://www.bea.gov/news/2004/gross-domestic-product-industry-2003 (дата звернення: 01.11.2023).
12. Yuskavage R.E., Pho Y.H. Gross Domestic Product by Industry for 1987–2000 New Estimates on the North American Industry Classification System. URL: https://apps.bea.gov/scb/pdf/2004/11November/1104GDP_by_Indy.pdf (дата звернення: 01.11.2023).
13. GDP share by industry U.S. 2022. URL: https://www.statista.com/statistics/248004/percentage-added-to-the-us-gdp-by-industry/ (дата звернення: 03.11.2023).
14. The ebb and flow of Federal fortune. URL: https://www.economist.com/free-exchange/2015/01/16/the-ebb-and-flow-of-federal-fortune (дата звернення: 03.11.2023).
15. Hollis D. Cyberwar Case Study: Georgia 2008. URL: https://web.archive.org/web/20220304223742/https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf (дата звернення: 04.11.2023).
16. Matei A.I., Savulescu C. Empirical Analysis of ICT, Economic Growth and Competitiveness in the EU. Proceedings of the International Conference on ICT Management, Wroclaw, September 15, 2012. URL: https://ssrn.com/abstract=2173340 (дата звернення: 04.11.2023).
17. Keizer G. Cyberattacks knock out Georgia's Internet presence. URL: http://www.computerworld.com/s/article/9112201/Cyberattacks_knock_out_Georgia_s_Internet_presence (дата звернення: 05.11.2023).
18. Swaine J. Georgia: Russia 'conducting cyber war'. URL: https://web.archive.org/web/20220304223741/https:/www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html (дата звернення: 05.11.2023).
19. Marching off to cyberwar. URL: http://www.economist.com/science/tq/displaystory.cfm?story_id=12673385&CFID=34793589&CFTOKEN=83946352 (date of access: 05.11.2023).
20. Melikidze G., Amaglobeli D., Baindurashvili K. Georgian economy continues rapid growth in Q2 2008. *Government of Georgia*. URL: https://www.gov.ge/files/34_272_580195_q2_08_real_gdp_growth_7.9_080924.pdf (дата звернення: 06.11.2023).
21. Enpi 08-14. European Training Foundation. 2010. 126 p. URL: https://www.etf.europa.eu/sites/default/files/m/C12578310056925BC12576EF002E304F_NOTE868FGP.pdf (дата звернення: 07.11.2023).
22. GDP by industry Georgia U.S. 2022. URL: https://www.statista.com/statistics/304946/georgia-real-gdp-by-industry/ (дата звернення: 07.11.2023).
23. Sharing insights elevates their impact. URL: https://www.spglobal.com/marketintelligence/en/mi/industry/economics-country-risk.html (дата звернення: 07.11.2023).
24. Commission staff working document 2023 country report – Estonia. Brussels: European Commission, 2023. 73 p. URL: https://economy-finance.ec.europa.eu/system/files/2023-05/ET_SWD_2023_606_en.pdf (дата звернення: 08.11.2023).
25. Republic of Estonia: 2008 Article IV Consultation–Staff Report. International Monetary Fund, 2009. 43 p. URL: https://www.imf.org/external/pubs/ft/scr/2009/cr0986.pdf (дата звернення: 09.11.2023).
26. Tucker M. China accused of hacking Ukraine days before Russian invasion. URL: https://www.thetimes.co.uk/article/china-cyberattack-ukraine-z9gfkbmgf (дата звернення: 09.11.2023).
27. Офіційний сайт Державної служби статистики України. URL: http://www.ukrstat.gov.ua (дата звернення: 10.11.2023).
28. Експорт IT-послуг зріс у 2021 році на 36% – до $6,8 млрд. URL: https://finbalance.com.ua/news/eksport-it-posluh-zris-u-2021-rotsi-na-36---do-68-mlrd (дата звернення: 11.11.2023).

29. Russia: ICT services export value by type 2022. URL: https://www.statista.com/statistics/1024850/russia-information-services-exports-value-by-type/ (дата звернення: 14.11.2023).
30. CEE: e-commerce growth by country 2022. URL: https://www.statista.com/statistics/1167234/e-commerce-growth-in-cee-region/ (дата звернення: 13.11.2023).
31. Europe and Central Asia Economic Update:War In The Region. URL: https://www.worldbank.org/en/region/eca/publication/europe-and-central-asia-economicupdate. (дата звернення: 01.09.2023).
32. IT 2023: що насправді відбувається з вітчизняним ринком. URL: https://www.ukrinform.ua/rubric-technology/3692904-it-2023-so-naspravdi-vidbuvaetsa-z-vitciznanim-rinkom.html (дата звернення: 14.11.2023).
33. Топ-50 IT-компаній України, літо 2023: мінус 6 тисяч фахівців за пів року, сервісні компанії мають менше клієнтів, продуктові наймають активніше. URL: https://dou.ua/lenta/articles/top-50-summer-2023/ (дата звернення: 14.11.2023).

References:

1. *Hlobalizatsiia*. Posibnyk z osvity v oblasti prav liudyny za uchasti molodi. Available at: https://www.coe.int/uk/web/compass/globalisation (accessed October 11, 2023).
2. Ekonomichna stratehiia Ukrainy 2030. Ukrainskyi instytut maibutnoho. URL: https://strategy.uifuture.org/index.html (accessed October 11, 2023).
3. Busel V. T. (2003) *Velykyi tlumachnyi slovnyk suchasnoi Ukrainskoi movy*. Irpin: VTF "Perun", 1087 p.
4. Plans for New Nuclear Reactors Worldwide. Available at: https://world-nuclear.org/information-library/current-and-future-generation/plans-for-new-reactors-worldwide.aspx#:~:text=Today%20there%20are%20about%20440,10%%20of%20the%20worlds%20electricity (accessed October 15, 2023).
5. Cyberwarfare. Wayback Machine. Available at: https://web.archive.org/web/20081209081836/http://www.economist.com/world/international/displaystory.cfm?story_id=E1_JNNRSVS (accessed October 20, 2023).
6. Nova kiberataka na banky bula "naibilshoiu v istorii Ukrainy" y dosi tryvaie. Available at: https://www.bbc.com/ukrainian/news-60401775 (accessed October 21, 2023).
7. Toffler A. (1995) *War and anti-war*. New York, NY : Warner Books, 370 p. Available at: https://archive.org/details/WarAndAntiWar-Toffler (accessed October 25, 2023).
8. Isbell P. Economic Aspects of the War in Iraq. Available at: https://www.realinstitutoelcano.org/en/analyses/economic-aspects-of-the-war-in-iraq/ (accessed October 26, 2023).
9. Irak cherez 10 rokiv pislia viiny: tsyfry i fakty. Available at: https://www.bbc.com/ukrainian/news/2013/03/130321_iraq_war_numbers_10years (accessed November 14, 2023).
10. Jorgenson D. W. (2001) U.S. Economic Growth in the Information Age. *Issues in Science and Technology*, vol. 18, no. 1. Available at: https://issues.org/jorgenson/ (accessed November 1, 2023).
11. Gross Domestic Product by Industry for 2003. U.S. Available at: https://www.bea.gov/news/2004/gross-domestic-product-industry-2003 (accessed November 1, 2023).
12. Yuskavage R.E., Pho Y.H. Gross Domestic Product by Industry for 1987–2000 New Estimates on the North American Industry Classification System. Available at: https://apps.bea.gov/scb/pdf/2004/11November/1104GDP_by_Indy.pdf (accessed November 1, 2023).
13. GDP share by industry U.S. 2022. Available at: https://www.statista.com/statistics/248004/percentage-added-to-the-us-gdp-by-industry/ (accessed November 3, 2023).
14. The ebb and flow of Federal fortune. Available at: https://www.economist.com/free-exchange/2015/01/16/the-ebb-and-flow-of-federal-fortune (accessed November 3, 2023).
15. Hollis D. Cyberwar Case Study: Georgia 2008. Available at: https://web.archive.org/web/20220304223742/https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf (accessed November 4, 2023).
16. Matei A. I., Savulescu C. Empirical Analysis of ICT, Economic Growth and Competitiveness in the EU. Pro(September 15, 2012) ceedings of the International Conference on ICT Management, Wroclaw. Available at: https://ssrn.com/abstract=2173340 (accessed November 4, 2023).
17. Keizer G. Cyberattacks knock out Georgias Internet presence. Available at: http://www.computerworld.com/s/article/9112201/Cyberattacks_knock_out_Georgia_s_Internet_presence (accessed November 5, 2023).
18. Swaine J. Georgia: Russia conducting cyber war. Available at: https://web.archive.org/web/20220304223741/https:/www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html (accessed November 5, 2023).
19. Marching off to cyberwar. Available at: http://www.economist.com/science/tq/displaystory.cfm?story_id=12673385&CFID=34793589&CFTOKEN=83946352 (accessed November 5, 2023).
20. Melikidze G., Amaglobeli D., Baindurashvili K. Georgian economy continues rapid growth in Q2 2008. Government of Georgia. Available at: https://www.gov.ge/files/34_272_580195_q2_08_real_gdp_growth_7.9_080924.pdf (accessed November 6, 2023).
21. Enpi 08-14. European Training Foundation. (2010) 126 p. Available at: https://www.etf.europa.eu/sites/default/files/m/C12578310056925BC12576EF002E304F_NOTE868FGP.pdf (accessed November 7, 2023).
22. GDP by industry Georgia U.S. (2022). Available at: https://www.statista.com/statistics/304946/georgia-real-gdp-by-industry/ (accessed November 7, 2023).
23. Sharing insights elevates their impact. Available at: https://www.spglobal.com/marketintelligence/en/mi/industry/economics-country-risk.html (accessed November 7, 2023).
24. Commission staff working document 2023 country report - Estonia. Brussels: European Commission. (2023) 73 p. Available at: https://economy-finance.ec.europa.eu/system/files/2023-05/ET_SWD_2023_606_en.pdf (accessed November 8, 2023).
25. Republic of Estonia: 2008 Article IV Consultation–Staff Report. International Monetary Fund. (20090 43 p. Available at: https://www.imf.org/external/pubs/ft/scr/2009/cr0986.pdf (accessed November 9, 2023).
26. Tucker M. China accused of hacking Ukraine days before Russian invasion. Available at: https://www.thetimes.co.uk/article/china-cyberattack-ukraine-z9gfkbmgf (accessed November 9, 2023).
27. Ofitsiinyi sait Derzhavnoi sluzhby statystyky Ukrainy. Available at: http://www.ukrstat.gov.ua (accessed November 10, 2023).
28. Eksport IT-posluh zris u 2021 rotsi na 36% - do $6,8 mlrd. Available at: https://finbalance.com.ua/news/eksport-it-posluh-zris-u-2021-rotsi-na-36---do-68-mlrd (accessed November 11, 2023).

29. Russia: ICT services export value by type 2022. Available at: https://www.statista.com/statistics/1024850/russia-information-services-exports-value-by-type/ (accessed November 14, 2023).

30. CEE: e-commerce growth by country 2022. Available at: https://www.statista.com/statistics/1167234/e-commerce-growth-in-cee-region/ (accessed November 13, 2023).

31. Europe and Central Asia Economic Update:War In The Region. Available at: https://www.worldbank.org/en/region/eca/publication/europe-and-central-asia-economicupdate. (accessed September 1, 2023).

32. IT 2023: shcho naspravdi vidbuvaietsia z vitchyznianym rynkom. Available at: https://www.ukrinform.ua/rubric-technology/3692904-it-2023-so-naspravdi-vidbuvaetsa-z-vitciznanim-rinkom.html (accessed November 14, 2023).

33. Top-50 IT-kompanii Ukrainy, lito 2023: minus 6 tysiach fakhivtsiv za piv roku, servisni kompanii maiut menshe kliientiv, produktovi naimaiut aktyvnishe. Available at: https://dou.ua/lenta/articles/top-50-summer-2023/ (accessed November 14, 2023).