НОВІ ТЕХНОЛОГІЇ

https://doi.org/10.15407/economyukr.2021.05.040
УДК 339.54+339.9+304+004
JEL: O33, D91, E71, F52

В.Р. СІДЕНКО, д-р екон. наук, чл.-кор. НАН України,
науковий консультант Українського центру економічних і політичних досліджень
ім. Олександра Разумкова, головний науковий співробітник
ДУ «Інститут економіки та прогнозування НАН України»
вул. П. Мирного, 26, 01011, Київ, Україна
e-mail: v_sidenko@ukr.net
ORCID: https://orcid.org/ 0000-0002-4195-5351

ВИКЛИКИ І РИЗИКИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ: СВІТОВИЙ ТА УКРАЇНСЬКИЙ КОНТЕКСТИ*

Визначено, що ризики впровадження цифрових технологій є зворотним боком процесу створення ними нових комерційних і комунікаційних можливостей. Акцентовано увагу на низці особливо небезпечних ризиків — підвищення інформаційної незахищеності особистості, інтенсифікація інформаційного шуму, що спричиняє непродуктивну втрату часу, значне розширення можливостей маніпулювання свідомістю людини і поведінкою споживачів, спотворення модусів мислення та руйнування національних культур, можливі негативні екологічні наслідки. Зроблено висновок про неприпустимість форсованого і незбалансованого впровадження цифрових технологій в країні з деформованими соціальними інститутами і високим рівнем криміналізації.

Ключові слова: *цифрова (електронна) торгівля; інформаційно-комунікаційні технології; цифрові технології; ендогенні технологічно зумовлені економічні та соціальні ризики; кібербезпека; інформаційна незахищеність.*

Сьогодні вже загальновизнано, що світ вступив в епоху кардинальних соціально-економічних змін, зумовлених новітніми технологіями Четвертої промислової революції, які поширюються на весь комплекс відносин у сферах виробництва, розподілу, обміну та споживання матеріальних і нематеріальних благ. Новітня технологічна революція пов'язана, як відомо, з низкою

* Статтю підготовлено в рамках НДР «Формування інституційної архітектоніки інформаційно-мережевої економіки» ДУ «Інститут економіки та прогнозування НАН України» (2018—2020 рр.) (державний реєстраційний № 0117U001686).

Цитування: Сіденко В.Р. Виклики і ризики цифрової трансформації: світовий та український контексти. *Економіка України*. 2021. № 5. С. 40—58. https://doi.org/10.15407/economyukr.2021.05.040

суттєвих технологічних інновацій, які, серед іншого, включають [1]: наносенсори та Інтернет наноречей (nanosensors and the Internet of nanothings), що забезпечують мініатюризацію під'єднання до мережі; блокчейн-технології як революційні децентралізовані системи, що базуються на довірі (the blockchain) [2]; відкриті екосистеми штучного інтелекту (open AI ecosystem), які дозволять перехід від штучного до «контекстуального» інтелекту, появу досконалих персональних помічників для виконання рутинних справ у рамках систем Інтернету речей. Згідно з OECP, центральну роль у групі цифрових технологій мають відігравати: аналітика, побудована на великих базах даних (Big data analytics); блокчейн-технології (Blockchain); Інтернет речей (Internet of things — IoT); штучний розум (Artificial intelligence) [3].

Усі ці технологічні інновації зумовлюють глибокі й масштабні зміни системного характеру економічних (і не тільки економічних) відносин, переформатування самих їх основ і появу нових соціально-економічних інститутів. Так, основу новітніх відносин становлять уже не тільки і не стільки відносини власності, скільки можливості доступу до тих чи інших благ, ресурсів, інформації. Кардинальні технологічні інновації тією чи іншою мірою впливають і дедалі більше впливатимуть і на технології здійснення комерційних операцій, зумовлюючи величезні зміни в цьому аспекті, зокрема, істотно впливаючи на роль і форми діяльності різного роду комерційних посередників.

Ці зміни значно пришвидшені пандемією COVID-19, яка, завдавши істотного удару по багатьох секторах економіки країн світу, водночас створила безпрецедентні можливості для розвитку бізнесу у віртуальному цифровому середовищі, що істотно прискорило формування нової «малоконтактної економіки» (low touch economy) [4]. Саме вона в умовах пандемії стає, парадоксальним чином, головним стабілізуючим і водночас дестабілізуючим квазісектором [5] економіки, одночасно підминаючи під себе компанії, що виявляють нездатність до перебудови моделей бізнес-діяльності. Ця глобальна тенденція, яка малоймовірно істотно послабшає після завершення нинішньої пандемії, буде визначальним структуроперетворювальним чинником розвитку — чинником, який навряд чи може ігноруватися будь-якою національною економікою і будь-якою державою, яка дбає про своє майбутнє.

Для України, економіка якої тривалий час перебуває в стані структурної деградації та занепаду внаслідок спотвореного процесу ринкового реформу-

---

[1] Top 10 Emerging Technologies of 2016 / World Economic Forum, Meta-Council on Emerging Technologies. — 2016. — June. — 18 p. [Електронний ресурс]. — Режим доступу : http://www3.weforum.org/docs/GAC16_Top10_Emerging_Technologies_2016_report.pdf

[2] Уже понад півсотні найбільших банків світу оголосили ініціативи щодо впровадження цих технологій. Відповідні проєкти здійснюють також Microsoft, IBM та Google.

[3] OECD Science, Technology and Innovation Outlook 2016. — Ch. 2: Future Technology Trends. — Paris : OECD Publishing, 2016. — 192 p. (doi: https://doi.org/10.1787/sti_in_outlook-2016-en).

[4] The New Low Touch Economy. How to navigate the world after COVID-19 : Report / Board of Innovation, 2020 [Електронний ресурс]. — Режим доступу : https://info.boardofinnovation.com/hubfs/Innovate%20low%20touch%20economy.pdf; The Winners of the Low Touch Economy. How companies can recover and grow in the new normal : Strategy Report / Board of Innovation [Електронний ресурс]. — Режим доступу : https://www.boardofinnovation.com/low-touch-economy/ (дата звернення: 28.04.2020).

[5] Саме квазісектором, тому що вона має виразно міжсекторний, багатогалузевий характер, складається з великої кількості сегментів, що діють у найрізноманітніших сферах економічної активності.

вання, цей новітній мегатренд пов'язаний як з певними можливостями виходу із «зачарованого кола» невдалих трансформацій, так і з серйозними ризиками і загрозою самому існуванню — в разі нездатності знайти адекватні відповіді на ці новітні технологічні та соціально-економічні виклики або наявності системних помилок у здійсненні політики цифровізації.

Не можна сказати, що ці проблеми перебувають поза увагою органів державного управління України і українських науковців. Спостерігається підвищена активність з розробки різного роду державних програм і законодавчих актів у цій сфері, що свідчить про перебування вказаного питання у фокусі економічної політики; істотно зросла і кількість наукових публікацій в Україні з цих питань [1—10]. Проте турбує певний подвійний дисбаланс у висвітленні впровадження цифрових технологій в українську економіку. По-перше, має місце явне переважання аналізу їх позитивних аспектів впливу — при очевидно меншій увазі до пов'язаних з ними ризиків і можливих негативних побічних наслідків. Такий дисбаланс в аналізі значною мірою зумовлений тим, що, по-друге, ризики новітніх цифрових технологій сприймаються переважно як екзогенні — пов'язані з дією негативних екстерналій, в якості яких можуть виступати зловмисні втручання в роботу кіберсистем або ж використання їх можливостей зловмисниками чи організованими злочинними угрупованнями, з формуванням відповідних мереж на кшталт Dark Internet або ж із цілеспрямованою політикою окремих держав, які залучають новітні цифрові технології як складову гібридних методів ведення геополітичного протиборства. Я не маю наміру приділяти увагу цим аспектам, вважаючи, що вони вже достатньо акцентовані в наукових дослідженнях і політичних документах останнього періоду[6].

Отже, **мета статті** — дослідити ендогенні ризики, пов'язані з цифровими технологіями, тобто тими, що породжуються самими цифровими технологіями і комплексно впливають на всю систему соціально-економічних відносин та її гуманітарну складову, показати, що такі ризики часто (якщо не здебільшого) є продовженням переваг цифровізації, своєрідним ефектом «перетворення на протилежність» — у разі гіпертрофії та/або незбалансованого розвитку цифрових технологій.

Такий акцент цього дослідження жодним чином не заперечує величезного позитивного потенціалу впливу новітніх цифрових технологій на економіку та суспільство: він, однак, підкреслює відносний характер таких переваг і те, що вони можуть бути нейтралізовані негативними процесами, спричиненими цими самими цифровими інноваціями.

Слід звернути увагу і на ще одну характерну особливість методології цього дослідження: воно не є вузькоекономічним, хоча й виконувалося в рамках тематики економічних досліджень. Проте в процесі цього дослідження я переконався в архаїчності традиційних підходів економічного аналізу, відокремленого від питань соціальних, соціально-психологічних та соціально-ціннісних аспектів розвитку, тому намагаюся підходити до цього питання міждисциплінарно і вважаю, що лише такий метаекономічний ана-

[6] У цьому контексті варто відзначити ґрунтовний багатоплановий аналіз групи міжнародних експертів, які асоціюють нинішній стан речей з «епохою кібербезпорядку» [11].

ліз[7] може наблизити нас до розуміння глибинної природи тих викликів, які породжуються поширенням цифрових технологій.

СОЦІАЛЬНО-ЕКОНОМІЧНІ РИЗИКИ ЦИФРОВИХ ТЕХНОЛОГІЙ — ЗВОРОТНИЙ БІК НОВИХ КОМЕРЦІЙНИХ МОЖЛИВОСТЕЙ

Процес кардинальної перебудови глобальної системи економічних відносин перебуває під впливом складного і суперечливого комплексу чинників, у якому різні фактори діють різноспрямовано, не лише стимулюючи, але подекуди і дестимулюючи перетворення. Тому загальний вектор руху формується як агрегуюча функція такої взаємодії суперечливих чинників і відображає певний баланс «плюсів» та «мінусів».

В економічному плані цифровізація, безперечно, створює цілу низку важливих комерційних переваг, які включають істотне розширення спектра пропозиції для споживачів, зниження витрат товарообігу і цін на товари та послуги, кардинальне прискорення темпу проведення комерційних операцій, створення можливостей для продуктивної комунікації між продавцями і покупцями, величезний потенціал для вивчення преференцій покупців та моделювання їх поведінки, розширення можливостей виходу на нові ринки для нових компаній (у тому числі малого та мікробізнесу), впровадження сучасних ефективних логістичних систем і нових варіантів для формування виробничих ланцюгів, що максимально наближаються до споживача, тощо (детальніше у [10, с. 91—92]). Проте майже всі ці комерційні переваги мають свої вразливості, які можуть бути актуалізовані внаслідок або спонтанних збоїв у функціонуванні дуже складних і дедалі ускладнюваних систем управління віртуальним комерційним середовищем, або, тим більше, цілеспрямованих дій певних злочинних угруповань чи недружніх держав, які в нинішній час гострого геополітичного протистояння все частіше використовують кіберзброю в комплексному арсеналі «гібридних» заходів протиборства.

Сьогодні кібербезпека перетворилася на ключову проблему розвитку світової економіки і торгівлі, а електронна (цифрова) злочинність стала дійсно глобальною загрозою. Не випадково Всесвітній економічний форум у Давосі, який щороку (протягом уже 15 років) випускає доповідь з питань глобальних ризиків (The Global Risks Report), останнім часом оцінює ймовірність негативних наслідків, що випливають з дії ризиків цифрового середовища, як найвищу після групи екологічних ризиків, хоча до 2012 р. перші взагалі не фігурували в провідній п'ятірці глобальних ризиків (табл. 1). І хоча в рейтингу ризиків 2020 р. кібератаки і шахрайство або викрадення даних посіли лише шосте й сьоме місця, оцінка рівня їх імовірності залишається дуже високою (3,7 за п'ятибальною шкалою при середньому рівні за всіма ідентифікованими експертами ВЕФ ризиками в 3,31).

[7] На жаль, «мейнстримні» економісти надто захопились абстрактним концептом Homo Oeconomicus, який насправді часто не дає можливості правильно оцінювати поведінку людини як суб'єкта суспільно-економічної діяльності, в якій економічні та неекономічні міркування, ринкові та неринкові механізми нерозривно сплетені.

Таблиця 1. **П'ять головних глобальних ризиків за рівнем імовірності їх реалізації у**

№	Роки							
	2007	2008	2009	2010	2011	2012	2013	
1	Інфраструктурний колапс	Вибухове зростання цін активів	Колапс цін активів	Колапс цін активів	Буревії та циклони	Диспаритет у рівнях доходів	Диспаритет у рівнях доходів	
2	Хронічні захворювання	Нестабільність на Близькому Сході	Уповільнення зростання економіки Китаю	Уповільнення зростання економіки Китаю	Паводки	Фіскальні дисбаланси	Фіскальні дисбаланси	
3	Нафтовий ціновий шок	Проблеми неспроможних держав (Failed and failing states)	Хронічні захворювання	Хронічні захворювання	Корупція	Викиди парникових газів	Викиди парникових газів	
4	Жорстке падіння економіки Китаю	Нафтовий ціновий шок	Розриви в глобальному управлінні	Фіскальні кризи	Втрата біорозмаїття	Кібератаки	Кризи водопостачання	
5	Вибухове зростання цін активів	Хронічні захворювання	Виникнення процесу деглобалізації	Розриви в глобальному управлінні	Зміна клімату	Кризи водопостачання	Старіння населення	

Джерело: The Global Risks Report 2020. — 15th Ed. / World Economic Forum in partnership Landscape, 2007—2020 [Електронний ресурс]. — Режим доступу: http://www3.weforum.

За рівнем потенційного руйнівного впливу [8] ризики у цифровому середовищі ще жодного разу не входили до першої п'ятірки глобальних ризиків, проте і цей індикатор також має тенденцію до зростання. Як наслідок, у оцінках 2020 р. ризик колапсу інформаційної інфраструктури вже посів шосте місце, а ризик кібератак — восьме, причому оцінка обох ризиків помітно перевищує середній рівень за всіма ризиками (3,5) [9]. Як зазначають автори цієї доповіді ВЕФ, п'яте покоління (5G) мереж, квантові обчислення та штучний інтелект створюють не тільки можливості, а й нові власні загрози.

«Відсутність глобальної системи управління технологічними ризиками, що фрагментують кіберпростір, може стримувати економічне зростання, загострювати геополітичне суперництво і розширювати поділи всередині товариств» [10]. Експерти ВЕФ запропонували ідентифікацію основних ризиків цифрових інновацій (табл. 2).

Слід окремо зазначити, що поширення коронавірусної пандемії витіснило станом на початок 2021 р. «цифрові ризики» за межі першої п'ятірки

[8] За методологією ВЕФ, застосовуються два виміри дії глобальних ризиків — імовірність їх реалізації (likelihood) та потенційна сила руйнівного впливу (impact).

[9] The Global Risks Report 2020. — 15th Ed. / World Economic Forum in partnership with Marsh & MacLennan and Zurich Insurance Group. — Fig. II: The Global Risks Landscape 2020 [Електронний ресурс]. — Режим доступу: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

[10] Там само. — P. 62.

2007—2020 рр.

2014	2015	2016	2017	2018	2019	2020
Диспаритет у рівнях доходів	Міждержавні конфлікти	Вимушена міграція	Екстремальні погодні явища	Екстремальні погодні явища	Екстремальні погодні явища	Екстремальні погодні явища
Екстремальні погодні явища	Екстремальні погодні явища	Екстремальні погодні явища	Вимушена міграція	Стихійні лиха	Провал у здійсненні кліматичної політики	Провал у здійсненні кліматичної політики
Безробіття	Провали в національному державному управлінні	Провал у здійсненні кліматичної політики	Стихійні лиха	Кібератаки	Стихійні лиха	Стихійні лиха
Провал у здійсненні кліматичної політики	Розвал або криза окремих держав	Міждержавні конфлікти	Терористичні атаки	Шахрайство з даними або їх викрадення	Шахрайство з даними або їх викрадення	Втрата біорозмаїття
Кібератаки	Безробіття	Природні катастрофи	Шахрайство з даними або їх викрадення	Провал у здійсненні кліматичної політики	Кібератаки	Спричинені людиною природні катастрофи

with Marsh & MacLennan and Zurich Insurance Group. — Fig. I : The Evolving Risks org/docs/WEF_Global_Risk_Report_2020.pdf

глобальних ризиків [11]. Проте в якості пріоритетних (шосте і сьоме місця у рейтингу ризиків) визнано їх нові види — «концентрація цифрової влади» (digital power concentration) та «цифрова нерівність» (digital inequality). Внесені зміни в методологію оцінки ризиків включають виокремлення довгострокових «екзистенційних» ризиків з часовим горизонтом дії 5—10 років, серед яких четверту позицію посідає ризик «несприятливих результатів технологічного прогресу» (adverse tech advances), на який вказує практично кожний другий експерт (50,2%).

Останнім часом низкою організацій на національному і міжнародному рівнях проводиться діяльність з кількісної оцінки різного роду ризиків, пов'язаних з кібербезпекою та впливом новітніх ІКТ на довкілля та соціальні процеси. Найбільш відомий приклад такого вимірювання подає Міжнародний союз електрозв'язку (International Telecommunication Union — ITU), який запровадив Індекс глобальної кібербезпеки (Global Cybersecurity Index — GCI). Він вимірює прихильність країн до кібербезпеки на глобальному рівні на основі аналізу п'яти «стовпів» (pillars) — 1) правових заходів, 2) технічних заходів, 3) організаційних заходів, 4) нарощування потенціалу та 5) рівня

[11] The Global Risks Report 2021. — 16th Ed. / World Economic Forum in partnership with Marsh & MacLennan, SK Group and Zurich Insurance Group. — P. 11, 14 [Електронний ресурс]. — Режим доступу : http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (дата звернення: 12.05.2021).

Таблиця 2. **Основні ризики у цифровому середовищі за ідентифікацією експертів ВЕФ**

	Ризики, пов'язані з цифровими інноваціями
Кібератаки	Цифрові технології Четвертої промислової революції за своєю природою є вразливими до різних форм кібератак — від простої крадіжки даних та вимог викупу і до втручання в роботу систем з потенційно широкомасштабними наслідками. Зростає організована кіберзлочинність, з якою дедалі важче боротися. Формується самостійна бізнес-модель «кіберзлочин як послуга» (cybercrime-as-a-service) в міру того, як ускладнюється інструментарій так званого даркнету (Darknet) — особливого сектору глобальної мережі, де здійснюються операції поза законом. Особливо широкі можливості для кіберзлочинності створюють механізми Інтернету речей. За оцінкою, у 2021 р. втрати від кіберзлочинності можуть сягнути 6 трлн дол.
Вразливість баз даних	Поширення нових інформаційних технологій та IoT підвищує загрози захищеності так званих чутливих даних — від ідентифікаційних даних особи, про стан здоров'я та фінанси і до конфіденційної інформації, яка належить приватним компаніям і державним органам. Зростання витоку даних стимулюється тим, що вони перетворюються на об'єкт ринкової торгівлі даними, обсяг якої нині оцінюється в близько 200 млрд дол.
Штучний інтелект	Створює потенційно найбільш істотні екзистенційні ризики, що включають не бачені раніше можливості маніпулювання свідомістю через поширення неправдивої інформації та можливе створення в перспективі нових інтерфейсів «мозок — комп'ютер» і гіперавтоматизованих комплексів (робототехніка + штучний інтелект), функціонування яких може опинитися поза межами людського контролю
Технології 5G (у перспективі 6G)	Створення нової високошвидкісної інфраструктури потребує величезних інвестицій на нові об'єкти і демонтажу застарілих. Такі витрати можуть становити значну фінансову проблему, не підйомну для багатьох
Квантові обчислення	Унаслідок кардинального (на декілька порядків) прискорення обчислень уразливими стають сучасні технології шифрування, що ставить під загрозу системи захисту даних і режими регулювання доступу до мереж, які обслуговують критичну інфраструктуру, пов'язану з національною безпекою
Хмарні сервіси	Спричиняють небувалу концентрацію у віртуальному просторі великих масивів потенційно чутливої інформації, яка може містити персональні дані та національні й комерційні секрети, що можуть стати об'єктом несанкціонованого доступу
	Геополітичні ризики
Утворення паралельних кіберпросторів	Зростаюча тенденція до посилення розбіжностей між країнами в їх протоколах здійснення операцій у кіберпросторі створює загрозу технологічної фрагментації цього простору, особливо в рамках політики окремих країн щодо встановлення «кіберсуверенітету»: це може призвести до порушення зв'язків між окремими секторами глобального кіберпростору
Формування переваг «першопроходців»	Країни, які йдуть попереду в запровадженні новітніх технологій функціонування кіберпростору, дістають істотні переваги, впливаючи вирішальним чином на формування нових стандартів і виробничих мереж. Це може зумовлювати зміни в глобальному балансі сил, спричиняючи загострення суперництва і протиріч
Нова «цифрова» гонка озброєнь	Відбувається зміна в природі національної та міжнародної безпеки, де ключовими стають питання гарантування захисту критичної інфраструктури, підтримки суспільних цінностей та запобігання виникненню міждержавних конфліктів. Цифрові технології спричиняють асиметричні зрушення у сфері військової справи, дозволяючи здійснення атак на великі країни з боку малих, а також недержавних структур. Виникає нова технологічна гонка озброєнь у кіберпросторі

Закінчення таблиці 2

Розрив з'єднаності міжнародних систем обміну даними	Посилюється значення фактора надійності учасників критичної інформаційної інфраструктури. Зростає ймовірність припинення обміну даними, що може призвести до порушення взаємодії між різними системами
	Економічні ризики
Ризик втрати контролю над ключовими технологіями	Ті, хто контролює інформаційні системи, дістають переваги в проведенні досліджень та економічному розвитку, формуючи й регулюючи основні тренди. Інші країни потрапляють у залежність від цих тенденцій, які вони фактично не мають змоги регулювати
Нові витрати, пов'язані з фрагментацією кіберпростору	Зумовлює підвищення трансакційних витрат бізнесу і зниження продуктивності через необхідність створення різних виробничих ліній для окремих ринків з різними стандартами і протоколами обміну даними
Втрата сталості розвитку	Наростаюча фрагментація зумовлюватиме збільшення негативного екологічного впливу. Сучасні системи забезпечення функціонування штучного інтелекту потребують дуже великих витрат енергії
Монетарні та фіскальні ризики	Формуються передумови для зростання нерівності можливостей між окремими компаніями і країнами. Нові цифрові валюти, які функціонують поза чітко визнаними регулятивними рамками, можуть підривати стабільність національних валют і міжнародні зусилля проти відмивання брудних грошей, а втрата довіри до цифрових грошей здатна порушити загальну фінансову стабільність
	Соціальні ризики
Утворення цифрових розривів і поглиблення розривів у добробуті	Різні швидкості запровадження новітніх цифрових технологій можуть поглиблювати соціальну нерівність і нерівність між окремими країнами, а також між працівниками різної кваліфікації (особливо сильно вражаючи працівників з найнижчою кваліфікацією), між різними регіонами (зокрема, високорозвинутими міськими районами і технологічно відсталими сільськими регіонами). При цьому може утворитися «зачароване коло»: збільшення розривів у доходах і «втеча мозків» ускладнюють для тих, хто відстає, скорочення відставання та унеможливлює необхідні інвестиції, які б дозволяли доступ на створювані Четвертою промисловою революцією новітні ринки; це дестимулює дослідження в новітніх сферах, ще більше посилюючи «втечу мозків»
Формування людської дистопії	Відсутність глобальних технологічних рамок призводить до феномену дистопії, наприклад, унаслідок кібербулінгу, встановлення постійного режиму нагляду і порушення конфіденційності, поширення неправдивої інформації та монетизації інформаційних даних про окремих осіб. Усі ці фактори можуть спричиняти руйнування довіри в суспільстві

Джерело: The Global Risks Report 2020. — 15th Ed. / World Economic Forum in partnership with Marsh & MacLennan and Zurich Insurance Group. — P. 62—67 [Електронний ресурс]. — Режим доступу : http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (дата звернення: 12.05.2021).

співпраці — з формуванням на їх основі інтегрального показника [12]. Значення цього індексу за 2018 р. свідчать, що найбільш надійна система кібербезпеки існує у Великій Британії (GCI дорівнює 0,931 за шкалою від 0 до 1),

[12] Global Cybersecurity Index — 2018 / International Telecommunication Union (ITU) [Електронний ресурс]. — Режим доступу : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (дата звернення: 12.05.2021).

США (0,926), Франції (0,918), Литві (0,908) та Естонії (0,905), Сінгапурі (0,898), Іспанії (0,896), Малайзії (0,893), Норвегії (0,892), Канаді (0,892), Австралії (0,890). Окремі ключові «гравці» на полі цифрових технологій посідають у цьому рейтингу далеко не провідні місця: Росія — лише 26-те (0,836), Китай — 27-ме (0,828), Індія — 47-ме (0,719). Але показово, що і технологічно просунута й законослухняна Швейцарія посідає лише 37-ме місце (0,788), а Ірландія, один з лідерів у галузі розробки програмного забезпечення, — 38-ме (0,784). Україна ж узагалі на цьому фоні виглядає відверто слабкою — з 0,661 посідає 54-те місце у світі серед 175 країн і 32-ге в Європі. Це, безумовно, свідчить про високу актуальність для України вирішення завдань зміцнення кібербезпеки.

ПАНОРАМА РИЗИКІВ ЦИФРОВОЇ ЕКОНОМІКИ І СУСПІЛЬСТВА: ЧИ БАЧИМО МИ ВСІ ФРАГМЕНТИ КАРТИНИ?

Слід зазначити, що за всієї великої кількості й розмаїття наведених ризиків і загроз, ідентифікованих ВЕФ, їх перелік, на мій погляд, є неповним і «різнокаліберним». Різні види ризиків мають дуже неоднаковий рівень методологічного опрацювання, а окремі з них ідентифіковано переважно на рівні лише загальної якісної оцінки, яка не дає можливості встановити їх розмірність і механізми впливу. Але головне полягає в тому, що наведені ризики не впорядковано за їх системною значущістю, і при цьому деякі вкрай важливі негативні наслідки поширення сучасних інформаційних технологій, які потребують ретельного вивчення й реагування, фактично залишаються в тіні. Ці ризики необхідно вивести на авансцену наукового аналізу та політичного порядку денного, для чого їх слід належним чином акцентувати.

По-перше, це створення і швидко прогресуюче посилення — завдяки інформатизації та накопичення великих баз даних — режиму ***інформаційної незахищеності особистості*** як особливого прояву процесу зниження рівня особистої безпеки в сучасному світі. Йдеться не просто про якісь випадкові, спорадично виниклі порушення та збої у функціонуванні мереж, що базуються на цифрових технологіях, а про ендогенні вразливості, іманентно властиві операціям у цифровому форматі. Адже, набуваючи безсумнівних додаткових переваг в аспекті ринкового вибору (режиму доступу до товарів та послуг), отримання нової інформації та знань і швидкості здійснення різного роду операцій, особа стає дедалі вразливішою внаслідок неконтрольованого поширення у віртуальному просторі важливої особистої інформації, до якої безперешкодний доступ дістають і ті, хто має або може мати відносно цієї особи злочинні чи просто недобросовісні наміри. У цьому контексті слід зазначити, що глобальна тенденція до зростання електронної злочинності за нинішнього стану культури людського суспільства стає фактично ***невідворотним побічним наслідком прогресу новітніх інформаційних технологій, зворотним боком медалі, своєрідною платою за отримання нових комунікаційних опцій.*** Чи завжди ці ризики виправдовуються додатковими можливостями у сфері споживання? Вочевидь, відповідь на це запитання не може бути однозначно позитивною чи однозначно негатив-

ною, вона залежить від конкретного контексту операцій та ціннісних преференцій суб'єктів цих операцій.

Окреслена проблема є дуже складною, і її навряд чи можна вирішити суто технологічними або юридичними інструментами (національними або міжнародними), адже неможливо передбачити всі ймовірні варіанти злочинних дій або приставити до кожного контролера, який стежитиме за тим, як ця особа використовує цифрове середовище. Існують серйозні сумніви в тому, що дана проблема може мати реальні перспективи ефективного розв'язання у світі, якому бракує справжніх, а не декларованих людських цінностей і в якому бал правлять гроші. Загалом прогрес новітніх ІКТ має базуватися на високому рівні взаємної довіри в суспільстві, але він зустрічає фундаментальні обмеження у формі успадкованих від минулого дуже інерційних суспільних цінностей і модусів суспільної поведінки, які часто ставлять нездоланні бар'єри на шляху підвищення рівня довіри.

Як наслідок, ми повинні уникати однобічного акценту на максимізацію функцій споживача, а досягати компромісу між ними та міркуваннями безпеки особистості. При цьому важливий не стільки темп поширення новітніх цифрових інновацій, скільки їх якість у самому широкому розумінні цього терміна. Створення ж цієї якості означає насамперед закладання відповідного культурного фундаменту для поширення новітніх цифрових технологій.

Цей аспект проблеми стає особливо значущим для тих країн, які мають недостатньо розвинуті соціальні інститути, адже для них намагання вирішити всі проблеми суто технологічним засобом — впровадження новітніх інформаційно-комунікаційних технологій — може стати своєрідним «троянським конем», який здатен зруйнувати традиційні соціальні інститути і ввести всередину системи традиційних культурних цінностей нові інституційні коди, побудовані здебільшого на примітивному прагматизмі та пріоритеті матеріальних цінностей і комфорту. А вирвана з усталеного суспільно-економічного контексту людина стає не тільки інформаційно, але й соціально та психологічно не захищеною — схильною до різного роду неврозів і психічних розладів, суїцидів та різних асоціальних дій.

По-друге, є підстави вважати, що екологічні ризики, пов'язані з новими цифровими технологіями, сьогодні навряд чи можуть бути адекватно оцінені в повному обсязі — через значний рівень невизначеності та малу вивченість багатьох новітніх технологій саме в контексті взаємодії людської діяльності та природних процесів. Зокрема, нині у нас не може бути впевненості в абсолютній безпечності значного підвищення щільності електронних комунікацій, яке буде неодмінно спричинене впровадженням форматів зв'язку 5G і в подальшому 6G (дослідження щодо якого вже розпочались) [13]. Адже якими безпечними, з точки зору інтенсивності електромагнітного забруднення довкілля, не виглядали б ці нові технологічні формати телекомунікацій, ідеться про можливість кардинального зростання інтенсивності самих комунікацій, до яких підключаться десятки, а згодом навіть сотні мільярдів різних приладів,

[13] Ідеться не стільки про рівень безпеки самого випромінювання, що відбувається в цьому форматі, скільки про те, що буде кардинально розширене поле застосування цифрових контактів завдяки IoT: це може створити якісно нову ситуацію порівняно з нинішнім станом сукупного електромагнітного навантаження на довкілля та людину.

що функціонуватимуть у режимі IoT [14]. Тому не випадково останнім часом у різних частинах світу створюються суспільні рухи та спостерігаються демонстрації [15], які виступають проти впровадження цих недостатньо вивчених технологічних форматів зв'язку, і навіть мали місце акції знищення інфраструктурного обладнання мобільного зв'язку. І хоча такі екстремістські заходи навряд чи можуть бути виправданими з правової та моральної точок зору, втім вони акцентують наявність проблеми, на яку повинні шукати відповідь вчені, інженери та винахідники, політики та урядовці. У протилежному випадку зручності й нові можливості нових технологій стануть нічим, якщо їх упровадження вестиме до зниження рівня безпеки життя людини, створюватиме нові джерела для нових захворювань і ризиків втрати здоров'я [16].

Привертаючи увагу до потенційно небезпечних екологічних впливів, слід мати на увазі, що навіть уже добре акцентована проблема значної енергомісткості новітніх інформаційних технологій (зокрема, у зв'язку з функціонуванням нових цифрових валют, а також так званих Великих даних — Big Data) може бути лише фрагментом значно більшого за масштабом енергетичного виклику людству. Про це, зокрема, свідчать деякі нещодавні дослідження, проведені британським фізиком Мелвіном Вопсоном (Melvin Vopson) [12], який передрікає настання «інформаційної катастрофи». Його теоретична модель передбачає, що за збереження нинішніх тенденцій через кілька сотень років на Землі не вистачить енергії для зберігання всієї цифрової інформації [17]. Навіть зважаючи на поки що суто теоретичну аргументацію цього передбачення, від неї навряд чи можна просто так відмахнутися. Це особливо актуально в тому контексті, що поставлені людством завдання протидії руйнівній зміні клімату та обмеження зростання середньосвітової температури атмосфери потребують кардинального скорочення енергогенерації та енергоспоживання у світі. І навіть якщо впровадження новітніх цифрових технологій сприятиме помітному скороченню енергомісткості різних економічних та соціальних процесів, чи можемо ми бути впевнені, що ***витрати на розгортання та утримання цифрової інфраструктури не зведуть нанівець або, принаймні, не поглинуть значну частину цієї потенційно можливої економії енергії?***

Таким чином, будь-які інновації у сфері цифрових технологій повинні проходити дуже ретельну і незалежну екологічну експертизу: знову слід констатувати, що жодне підвищення матеріального добробуту та міркуван-

---

[14] Це додаткове електромагнітне навантаження дуже ***нерівномірно*** розподілятиметься в територіально-географічному аспекті, надмірно концентруючись у глобальних містах та інших осередках техногенної цивілізації, що, не виключено, стане додатковим фактором розбалансування природних процесів на додаток до вже існуючих кліматичних змін.

[15] Швейцарцы протестуют против 5G / DW. — 2019. — 22 сент. [Електронний ресурс]. — Режим доступу : https://p.dw.com/p/3Q1rN (дата звернення: 29.09.2019).

[16] У цьому зв'язку варто звернути увагу на те, що саме в період розквіту системи електронних комунікацій та мобільного зв'язку, надзвичайно високих інших антропогенних впливів на природу з 1990-х років людство зіткнулось із значним пришвидшенням поширення новітніх вірусів — спочатку імунодефіциту HIV (AIDS), згодом коронавірусної хвороби в різних варіантах – SARS, MERS, SARS-Cov2, останній з яких породив глобальну пандемію з соціально-економічними наслідками, які поки що важко оцінити повною мірою. Чи є це випадковим збігом у часі? Можливо.

[17] За оцінками, у 2000 р. загальний глобальний обсяг сфери цифрових даних досяг 59 зеттабайт (10^{21} байт) [11, p. 8].

ня зручності й комфорту не можуть бути виправданням для політики, яка здатна містити в собі реальні загрози довкіллю та здоров'ю людини.

По-третє, хвилеподібне поширення інформації, зумовлене впровадженням нових цифрових технологій обміну даними, далеко не завжди має корисний для людини та суспільства характер, оскільки водночас створює величезний вал інформаційного шуму, який, у свою чергу, спричиняє значні втрати часу на пошук корисної інформації, «розчиненої» в інформаційному океані. При цьому потенційні виграші від скорочення часу здійснення комерційних та інших трансакцій можуть бути нейтралізовані втратами часу на обробку зайвих масивів інформації (по суті, спаму), що може зумовити ***втрату найбільш цінного для людини активу — часу, відпущеного для нашого життя***. Феномен інформатизації взагалі дуже суперечливий: з одного боку, він є абсолютно необхідним компонентом процесу здобуття знань, а з іншого — може легко заміняти знання хаотично зібраною, безсистемною та не зрозуміло на що придатною інформацією. А отже, «інформаційна епоха» М. Кастельса [18], на мій погляд, зовсім не є тотожною суспільству, що базується на знаннях. Нерідко людина може просто втрачати орієнтацію в потоках суперечливої (і, можливо, не завжди достовірної) інформації, формувати під її впливом ***викривлене уявлення про реальність або взагалі потрапляти в пастку віртуальної реальності*** — з її штучно створеними орієнтаціями та критеріями оцінок, несправжніми переживаннями і радощами, по суті штучним, дегуманізованим життям.

Звідси виникає істотна і водночас дуже складна та суперечлива (з позиції прав і свобод людини) проблема фільтрації даних, мета якої — пропускати до аналізу лише ті обсяги потенційно корисної інформації, що є абсолютно необхідними для правильного прийняття життєво важливих рішень. А це означає актуальність формування і поширення відповідних і технічних, і аналітичних експертних систем — не виключено, за допомогою відповідних систем штучного інтелекту, пристосованих для первинної обробки даних. У цьому питанні дуже важливо знаходити правильний баланс індивідуальних прав і свобод та суспільних інтересів (у яких втілюються спільні інтереси виживання та розвитку соціуму) [19]. Є підстави вважати, що знаходження суспільного компромісу в цьому питанні неможливе без широких за складом і перманентних за характером взаємодій держави, бізнесу та суспільства.

У цьому контексті слід звернути увагу на ще один аспект проблеми, що розглядається. Отже, по-четверте, вже сьогодні ми маємо дедалі більше підтверджень того, що новітні цифрові технології зумовлюють значне розширення можливостей маніпулювання свідомістю та поведінкою споживачів через відповідні інтернет-платформи і соціальні мережі, які дійсно справляють ***амбівалентний вплив на стан людської свободи***. Це лише на перший погляд формальне розширення свободи вибору зумовлює піднесення рівня

[18] Мається на увазі його всесвітньо відома праця «Інформаційна епоха» [13].

[19] Це, як доводить досвід упровадження систем регулювання Інтернету в Китаї та Російській Федерації, є дуже непростим завданням, вирішення якого може супроводжуватися різного роду «переборами». Але при цьому шлях необмеженої свободи потоку інформації в глобальній мережі також не є виходом, оскільки створює потенційно необмежені можливості для соціально деструктивних дій.

свободи людини. Насправді таке розширення свободи може виявитись ілюзорним. При цьому йдеться, насамперед, про безпрецедентні нові можливості для систематичного застосування — завдяки новітнім ІКТ — витончених методів соціально-психологічного впливу, які при форматуванні поведінки потенційного споживача на ринку здатні ефективно стимулювати до придбання навіть непотрібних товарів і послуг, формування манії споживання, які нерідко мають наслідком марнотратне витрачання коштів. Дистанційна купівля товарів може створювати умови для введення в оману споживачів, які часто роблять комерційний вибір не на підставі огляду реального товару, а сприймаючи його картинку в Інтернеті, яка, проте, може неадекватно відображати якості товару. Продавці мають усі можливості створювати спеціалізовані групи коментаторів на своїх веб-сторінках, які цілеспрямовано підтримують окремі бренди та моделі, непрямим методом обмежуючи де-факто вільний вибір споживача за рахунок формування «спільної думки».

Більше того, зазначені впливи в сучасному світі стають дедалі більш комплексними і систематичними, де-факто переформатовуючи всю матрицю життєвих смислів і мотивів поведінки людини, нерідко деформуючи її культурну матрицю. За таких умов вибір людини все частіше зумовлюється штучно нав'язаними через мережі символами і знаками схвалення чи засудження. А передача від покоління до покоління життєвих навичок і смислів, яка віками була головним каналом забезпечення культурної спадкоємності в суспільстві, за таких умов порушується, якщо не руйнується взагалі. Поведінка особистості дедалі сильніше визначається не сімейними цінностями і не оцінками людей, що проживають поруч, а законами інтернет-натовпу і похідних від цього феноменів (зокрема, тих, що називаються новітнім англійським терміном «флешмоб» (flash mob), що вже міцно облаштувався в українській мові та мовах інших народів). Де-факто формується своєрідна «***цифрова культура натовпу***», що керує поведінкою, як економічною, так і неекономічною, великих мас людей.

Це є надзвичайно складною проблемою, яка, радше за все, вимагатиме відповідного коригування та впровадження істотних змін у системах виховання особистості (формування в неї стійкого психологічного імунітету до будь-яких вторгнень у сферу свідомості). До того ж це потребує впровадження якісно вищих стандартів регулювання діяльності електронних ЗМІ та соціальних мереж, які повинні бути саме інформаційними посередниками, а не четвертою чи п'ятою владою [20]. У даному випадку проблема виходить далеко за межі суто економічних міркувань, стає виразно гуманітарною.

По-п'яте, в умовах швидкого поширення цифрової комерції мислення людини може також дедалі більше комерціалізуватись, і комерційні начала в людській свідомості почнуть домінувати над культурними засадами мислення. Сьогодні вже з'являються публікації, в яких автори стурбовані руйнуванням національних культур та їх заміщенням уніфікованими цифровими алгоритмами спілкування і віртуалізацією реальності.

[20] Самі по собі претензії сучасної медіаеліти та медіамагнатів, які стоять за ними, на роль суспільно найвпливовішої гілки влади є потенційно небезпечними для суспільства, якщо в ньому не існує чітко визначених меж інформаційного впливу на людей. Адже такий вплив здатен дуже легко перетворювати ЗМІ та електронні мережі, склад і керівництво яких суспільством не обирається, на засіб ерозії демократичного устрою.

Так, американець британського походження Ендрю Кін (Andrew Keen) [14] стверджує, що Інтернет вбиває культуру людської цивілізації, замінюючи її інформаційним ерзацом, зменшуючи роль професіоналів та підносячи малограмотних дилетантів, знецінюючи традиційні суспільні інститути. На його думку, успіх дедалі менше залежить від таланту і дедалі більше — від уміння працювати в Інтернеті. Особливою мірою це зачіпає такі сектори «виробництва культурного продукту», як книговидання, кіновиробництво, звукозапис, журналістика, де якісний продукт витісняється спрощеними дешевими замінниками, що циркулюють у мережі.

Ще далі йде у цьому відношенні Ніколас Карр (Nicholas Carr) — автор бестселера «Пустушка. Що Інтернет робить з нашим мозоком» [15; 16]. Він стверджує, що Інтернет містить у собі кардинальну загрозу — ***послаблення людського інтелекту*** через формування звички до поверхового сприйняття інформації, неглибокого мислення та ненадійного засвоєння знань. На його думку, Інтернет стимулює до швидкого засвоєння мало пов'язаних між собою частин інформації, які походять з великої кількості джерел: швидке і неглибоке сканування інформації витісняє роздуми та рефлексію, ментальне конструювання смислів та логічних схем; відбувається атрофія пам'яті та деформація самого процесу мислення, яке стає фрагментарним, кліповим і примітивним.

Навіть якщо автори цих тверджень дещо перебільшують, їх не можна просто так проігнорувати, вони потребують проведення відповідних досліджень у сферах медицини, психології та соціології. Адже в цій площині постають дійсно екзистенційні загрози людству, пов'язані з можливою ***дегуманізацією***. Перекладаючи все більшу частину робіт на роботів і машинні системи, людина сама може дедалі значнішою мірою ставати додатком до роботів і машин, що здатне вести до втрати самого сенсу людського життя й самого сенсу соціально-економічного прогресу. І, можливо, це стає найбільш ***масштабним в історії викликом для суспільства і людини***. Не випадково фахівці схиляються до думки, що вирішення ключових проблем, пов'язаних із цифровою трансформацією та впровадженням штучного інтелекту, лежить не стільки в площині технологічних рішень, скільки у сфері соціально-етичних засад [21].

УКРАЇНСЬКА «ДЕРЖАВА У СМАРТФОНІ»: ЧИ ВРАХОВАНО ВСІ РИЗИКИ?

У всьому комплексі політичних зрушень, які здійснені українською владою з середини 2019 р., питання цифрової трансформації посідають, напевно, найбільш помітне місце в аспекті позитивних досягнень. Проте прогрес у цій сфері настільки випереджає просування по інших напрямах проголошених реформ, особливо щодо забезпечення реального верховенства права і торжества закону, що на фоні загальної недовіри населення до більшості

[21] Ключовий висновок, який зробив авторитетний міжнародний колектив дослідників цієї проблеми, полягає в тому, що зазначені інноваційні процеси мають набути форми «справжнього і щирого морального зобов'язання окремих людей та закладів у пошуках загального блага» [11, p. 152—153]. При цьому антропологічні та етичні міркування (етичний імператив) повинні стати дієвими силами, що розвиватимуть відповідну організаційну культуру, спрямовану на формування та управління технологічними інноваціями у людський розвиток.

суспільних інститутів виникає запитання: «Наскільки він є прийнятним — щодо безпеки соціально-економічних трансформацій?»

Україна останнім часом звертається до успішного досвіду цифровізації низки країн, зокрема Естонії. При цьому її керманичі безпідставно вважають, що процес цифровізації є суто технологічним питанням, прагматичне вирішення якого автоматично розв'яже всі болючі соціально-економічні проблеми — корупції, бюрократизації, нерівних ринкових можливостей, ухиляння від податків та ін. При цьому ігнорується та обставина, що політика цифровізації мала успіх саме в тих країнах, де ще до її початку вже були створені й функціонували досить ефективні суспільні інститути. Не цифрові технології позбавили від корупції та високого рівня злочинності Естонію, скандинавські країни та низку країн Східної Азії: навпаки, саме останні уможливили відносно безболісне впровадження новітніх цифрових технологій функціонування економіки та суспільства, які в подальшому дійсно посилили якість чинних суспільних інститутів.

Однак новітніми цифровими технологіями можуть ефективно користуватися не тільки добропорядні громадяни, але й особи та організації із злочинними намірами. Більше того, оскільки вони можуть володіти «на старті» значно більшими фінансовими ресурсами, ніж середній громадянин, існує висока ймовірність, що ***темп асиміляції новітніх цифрових технологій у тіньовому та кримінальному секторах економіки і суспільства буде вищий за середній***. Так, останнім часом чимало написано про нові комерційні можливості, які створюють новітні технології «блокчейн» та емісія нових цифрових валют, проте не менше написано і про можливості їх використання злочинним світом. Технологічні інновації не є носіями моралі та совісті: останні існують виключно в людській свідомості та колективних психологічних архетипах, які формуються суспільством і передаються від покоління до покоління. Тому вони є амбівалентними з точки зору можливих суспільних ефектів застосування. І результат їх використання вирішальною мірою залежить від того, на який інституційний ґрунт вони лягають, і насамперед від того, якою є система неформальних інститутів суспільства, що реально скеровує поведінку в умовах, де формальні інститути (закон і створені формальні регулятивні інституції) пробуксовують — як це має місце, на жаль, в Україні.

«Держава у смартфоні» може дуже легко стати «скринькою Пандори» в країні, де немає відповідальності чиновників за зловживання своїми повноваженнями і нецільове використання інформації, до якої вони отримують доступ згідно із своїми службовими повноваженнями; де службова і взагалі будь-яка конфіденційна інформація легко перетворюється на предмет ринкової купівлі-продажу; де правоохоронні органи не виконують належним чином своїх функцій щодо захисту інтересів громадян, а суди вирішують справи, керуючись більше меркантильними критеріями, ніж законом [22]. Для країн

[22] Наприклад, хто в сучасній Україні може гарантувати, що, купуючи онлайн, покупець не наражатиметься на небезпеку несанкціонованої передачі чутливої фінансової інформації про себе, а користуючись медичними послугами онлайн — не поставатиме під загрозою поширення серед сторонніх осіб даних про стан свого здоров'я, або ж, здійснюючи операції з нерухомим майном (житлом, будинками, земельними ділянками), не зазнаватиме ризику втручання сторонніх осіб (злочинців) в існуючі записи в державних реєстрах? Відповіді на ці запитання, вочевидь, є зрозумілими.

з такими інституційними характеристиками стрибок у цифрову економіку і цифрове суспільство може реально стати стрибком у безодню без парашута.

На жаль, усі аспекти ризиків перебувають десь у глибокій тіні української політики цифрової трансформації, і лише проблема кібербезпеки більшменш акцентується внаслідок дії зовнішніх обставин (відповідь на політику Росії, зобов'язання перед США і ЄС). Але, як було вже показано, ризики цифровізації далеко не вичерпуються аспектом кібербезпеки, а мають значно ширший соціально-економічний контекст. Більшість же реальних соціально-економічних ризиків навіть не обговорюється в сучасному українському політикумі.

В умовах, коли домінуючий нині в державному апараті формат мислення має дуже невиразну стратегічну орієнтацію і керується майже виключно поточними міркуваннями, а саме формування державного апарату та афілійованих недержавних дорадчих структур уражене хворобою непотизму, втрачається здатність до комплексного, різнобічного аналізу структурно складних процесів, що відбуваються сьогодні у світі та Україні. Будь-які складні постановки проблем з боку незалежної наукової громадськості, які час від часу трапляються, не зустрічають позитивного відгуку в бюрократичному лабіринті, який відверто тяжіє до простих, але психологічно забарвлених і візуально яскравих картинок, а не до поглибленого аналізу складних дилем суспільно-економічного розвитку.

З огляду на сказане, українське суспільство має вимагати від тих, хто формує політику держави, більш соціально відповідального ставлення до складних проблем сучасності, до яких, безперечно, належить і проблема цифровізації наших економіки та суспільства. Це питання не має стати виключною компетенцією однієї особи або уповноваженої ним групи керуючих осіб: воно має бути предметом широких суспільних дискусій за участю всіх зацікавлених осіб, а не лише «своїх».

Отже, доцільно було б зусиллями громадянського суспільства створити ***спеціальну постійно діючу платформу для широких суспільних дискусій з питань цифровізації економіки та суспільства***, ставлячи їй за мету повну ідентифікацію всіх проблем, перешкод та реальних і потенційно можливих ризиків й загроз, які виникають у цьому контексті. Ми повинні чітко розуміти, що будуємо під гаслом цифровізації — чи то підвалини цивілізації вільних людей майбутнього, де технології підпорядковано найвищим людським цінностям, чи то прообраз технологічного концтабору, керованого новою технологічною «елітою», де всі перебувають під контролем і на всіх є управа. Громадяни України повинні самі визначати базові параметри тих механізмів, які істотно впливатимуть на наші права і свободи, не залишаючи виключне право вирішення цих проблем замкненим корпораціям політичних кланів і бюрократів та тісно пов'язаних з ними медіамагнатів, щодо яких українське суспільство має сьогодні мінімальний рівень довіри.

ВИСНОВКИ

Ризики впровадження цифрових технологій є результатом не стільки недосконалої політики чи помилок цифровізації, скільки зворотним боком процесу створення ними нових комерційних і комунікаційних можливостей. Вони створюються амбівалентним характером цифрових технологій, які, будучи нейтральними до суспільної моралі, рівною мірою можуть використовуватись і на благо, і на шкоду.

Серед розмаїття ризиків, які пов'язані з цифровими технологіями та ідентифікуються міжнародними організаціями, що діють у цій сфері, можна виокремити низку особливо небезпечних, яким досі не приділяють достатньо уваги, принаймні, такої, як питанням кібербезпеки. Проведене дослідження дозволило визначити широку групу ендогенних технологічно зумовлених ризиків цифрової трансформації. До них відносяться: підвищення інформаційної незахищеності особистості; інтенсифікація інформаційного шуму та зумовлене цим зростання марних втрат часу; значне розширення можливостей маніпулювання свідомістю людини та поведінкою споживачів; спотворення модусів мислення та руйнування національних культур; можливе посилення негативних екологічних наслідків, зокрема, через енергомісткість новітніх цифрових технологій.

Економічні та соціальні ефекти від упровадження цифрових технологій значною мірою зумовлюються станом інституційного середовища країни, наявністю в ній істотних деформацій формальних і неформальних інститутів, існуючим рівнем криміналізації. За наявності таких деформацій неприпустимою є політика форсованого і незбалансованого впровадження новітніх цифрових технологій, оскільки їх можливостями можуть скористатися, насамперед, особи та соціальні угруповання із злочинними асоціальними намірами. У такому разі впровадження цифрових технологій буде підпорядковане не цілям розширення можливостей і свобод людини, а цілям наживи або посилення контролю над поведінкою людей та громадських об'єднань. Політика поширення новітніх цифрових технологій має бути в таких країнах обережною і виваженою, міцно пов'язаною з паралельними поліпшеннями в структурі та механізмах функціонування суспільних інститутів.

З метою знаходження шляхів адекватного управління процесами цифрової трансформації, своєчасного виявлення зумовлених нею ризиків та загроз бажано, щоб ключові фахівці та професійні організації створили єдину постійно діючу платформу (мережу) для широких суспільних дискусій з питань цифровізації економіки й суспільства та її наслідків для людини і суспільства. У перспективі постійні контакти в цих питаннях держави, суспільства та бізнесу мали б стати обов'язковою нормою, закріпленою законом.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Рибка С.В., Кільчицький Є.В., Післегін О.М.* Кіберпростір, управління інфраструктурою, кібербезпека // Стратегічна панорама. — 2015. — № 1. — С. 126—134.
2. *Савчук М.М.* Захист інформаційних технологій та кібербезпека : стенограма наук. доповіді на засіданні Президії НАН України 25.09.2019 р. // Вісник Національної академії наук України. — 2019. — № 11. — С. 23—28.

3. *Ємельянов В.М., Бондар Г.Л.* Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України // Публічне управління та регіональний розвиток. — 2019. — № 5. — С. 493—523.
4. *Маковець О.П., Дрозд І.К.* Кібербезпека як фактор фінансової безпеки підприємства // Економіка. Фінанси. Право. — 2020. — № 5 (3). — С. 31—35.
5. *Попівняк Ю.М.* Кібербезпека та захист бухгалтерських даних в умовах застосування новітніх інформаційних технологій // Бізнес Інформ. — 2019. — № 8. — С. 150—157.
6. *Гуцалюк М.* Безпека Інтернет-торгівлі // Правова інформатика. — 2007. — № 1. — С. 29—31.
7. *Цимбалюк І.* Безпека електронної торгівлі (організаційно-правовий аспект) // Правова інформатика. — 2012. — № 3. — С. 69—76.
8. *Вишневський В.П., Гаркушенко О.М., Князєв С.І.* та ін. Цифровізація економіки України: трансформаційний потенціал : моногр. ; [за ред. В.П. Вишневського, С.І. Князєва] / НАН України, Інститут економіки промисловості. — К. : Академперіодика, 2020. — 188 с.
9. *Тарасевич В.М., Білоцерківець В.В., Завгородня О.О.* та ін. Цифровий вимір інноваційно-інформаційної економіки : моногр. ; [за ред. В.М. Тарасевича]. — Дніпро : ПМП «Економіка», 2021. — 448 с.
10. *Сіденко В.* Мегатренди розвитку електронної торгівлі у контексті сучасної технологічної революції // Економіка України. — 2018. — № 11—12. — С. 82— 103.
11. AI in the Age of Cyber-Disorder: Actors, Trends, and Prospects / ISPI and Brookings ; [F. Rugge (Ed.)]. — Milan : Ledizioni Ledi Publishing, 2020. — 157 p.
12. *Vopson M.M.* The information catastrophe // AIP Advances. — 2020. — No. 10, 085014 [Електронний ресурс]. — Режим доступу: https://aip.scitation.org/doi/10.1063/5.0019941 (дата звернення: 18.08.2020).
13. *Кастельс М.* Информационная эпоха: экономика, общество и культура ; [пер. с англ. под науч. ред. О.И. Шкаратана]. — М. : ГУВШЭ, 2000. — 608 с.
14. *Keen A.* The Cult of the Amateur: How Today's Internet Is Killing Our Culture. — New York : Doubleday/Currency, 2007. — 228 p.
15. *Карр Н.Дж.* Пустышка. Что интернет делает с нашими мозгами ; [пер. с англ.]. — СПб. : Best Business Books, 2012. — 256 с.
16. *Carr N.* The Shallows: What the Internet Is Doing to Our Brains, Updated Edition. — New York : W.W. Norton & Company, 2020. — 320 p.

Стаття надійшла 26.10.2020 і була оновлена 13.05.2021

REFERENCES

1. Rybka S., Kilchuzkiy E., Pislegin O. Cyberspace, infrastructure management, cyber security. *Strategic Panorama*, 2015, No. 1, pp. 126-134 [in Ukrainian].
2. Savchuk M. Information technology protection and cyber security (Transcript of scientific report at the meeting of the Presidium of NAS of Ukraine, September 25, 2019). *Visnyk of the National Academy of Sciences of Ukraine*, 2019, No. 11, pp. 23-28 [in Ukrainian].
3. Yemelyanov V., Bondar H. Cyber security as a component of national security and cyber protection of critical infrastructure of Ukraine. *Public Administration and Regional Development*, 2019, No. 5, pp. 493-523 [in Ukrainian].
4. Makovets O., Drozd I. Cybersecurity as factor of financial security of the enterprise. *Economics, Finances, Law*, 2020, No. 5 (3), pp. 31-35 [in Ukrainian].
5. Popivniak Yu. Cybersecurity and protection of accounting data under conditions of modern information technology. *Business Inform*, 2019, No. 8, pp. 150-157 [in Ukrainian].
6. Gutsalyuk M. Security of Internet trade. *Legal Informatics*, 2007, No. 1, pp. 29-31 [in Ukrainian].
7. Tsymbaliuk I. E-commerce security (organizational and legal aspect). *Legal Informatics*, 2012, No. 3, pp. 69-76 [in Ukrainian].
8. Vishnevsky V., Garkushenko O., Knyazev S. et al. Digitization of Ukraine's Economy: Transformation Potential. V.P. Vishnevsky, S.I. Knyazev (Eds.). NAS of Ukraine, Institute of Industrial Economics, Kyiv, Akademperiodyka, 2020 [in Ukrainian].

9. Tarasevych V., Bilotserkivets V., Zavgorodnya O. et al. Digital Dimension of Innovation and Information Economy. V.M. Tarasevych (Ed.). Dnipro, PMP «Ekonomika», 2021 [in Ukrainian].
10. Sidenko V. Megatrends of e-commerce development in the context of modern technological revolution. *Economy of Ukraine*, 2018, No. 11-12, pp. 82-103 [in Ukrainian].
11. AI in the Age of Cyber-Disorder: Actors, Trends, and Prospects. F. Rugge (Ed.). ISPI and Brookings, Milan, Ledizioni Ledi Publishing, 2020.
12. Vopson M.M. The information catastrophe. *AIP Advances*, 2020, No. 10, 085014, available at: https://aip.scitation.org/doi/10.1063/5.0019941 (accessed on: 18.08.2020).
13. Castells M. The rise of the network society. Moscow, HSE University, 2000 [in Russian].
14. Keen A. The Cult of the Amateur: How Today's Internet Is Killing Our Culture. New York, Doubleday/Currency, 2007.
15. Carr N. The Shallows: What the Internet Is Doing to Our Brains. Saint Petersburg, Best Business Books, 2012 [in Russian].
16. Carr N. The Shallows: What the Internet Is Doing to Our Brains, Updated Edition. New York, W.W. Norton & Company, 2020

Received on October 26, 2020 and updated on May 13, 2021

Volodymyr Sidenko, Dr. Sci. (Econ.), Corresponding Member of the NAS of Ukraine,
Scientific Consultant of the Razumkov Centre, Principal Researcher
Institute for Economics and Forecasting of the NAS of Ukraine

CHALLENGES AND RISKS OF DIGITAL TRANSFORMATION:
GLOBAL AND UKRAINIAN CONTEXTS

The risks of digitalization of the economy are the reverse side of the process that creates by digital technology new commercial and communication opportunities for individuals and society as a whole. They arise from the ambivalent nature of digital technologies, their generally neutral nature in relation to the norms of public morality.

Among the risks associated with digital technology, cybersecurity issues that focus on exogenous (in relation to digital content) risks are now prioritized. At the same time, much less attention is given to endogenous technologically determined risks of digital transformation: increase of personal information insecurity, intensification of information noise and growth of unproductive loss of time, considerable expansion of opportunities to manipulate human consciousness and behavior, risk of distortion of the modes of thinking and culture, adverse environmental consequences, primarily due to the significant energy intensity of digitalization.

The economic and social effects of digital technologies are largely determined by the state of the formal and informal institutional environment of a country. Given the institutional distortions and high crime rates, the policy of forced and unbalanced introduction of digital technologies can produce negative social effects, including the growth of new forms of criminalization of economic activity, strengthening control over the behavior of people and public associations. The policy of dissemination of the latest digital technologies in institutionally problematic countries should be careful, balanced and strongly connected to the parallel improvement in the structure and functioning mechanisms of public institutions.

It is necessary to create a single permanent platform (network) for broad public discussions on the digitalization of the economy and society and its consequences for man and society.

***Keywords**: digital (electronic) trade; information and communication technologies; digital technologies; endogenous technologically determined economic and social risks; cybersecurity; information insecurity.*