УДК 338:330:37.0

Бондар-Підгурська О. В.
доктор економічних наук, доцент, професор кафедри менеджменту
ВНЗ Укоопспілки «Полтавський університет економіки і торгівлі», Полтава, Україна,
bondarpodgurskaa@gmail.com
ORCID ID: https://orcid.org/0000-0001-7792-4023

Глєбова А. О.
кандидат економічних наук, доцент, доцент кафедри менеджменту і логістики
Національного університету «Полтавська політехніка імені Юрія Кондратюка», Полтава,
Україна, alliaglebova@gmail.com
ORCID ID: https://orcid.org/0000-0002-7030-948X

СТАН, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ЦИФРОВОЇ ОСВІТИ УКРАЇНИ У ВОЄННИЙ І ПІСЛЯВОЄННИЙ ПЕРІОДИ

Анотація. *Метою дослідження є вивчення стану, проблем і перспектив розвитку цифрової освіти України у воєнний та післявоєнний періоди, а також розроблення рекомендацій щодо активізації цього процесу. Застосовано методи аналізу й синтезу, узагальнення, візуалізації та ін. Цифрову освіту України розглянуто як чинник розвитку економіки в окреслені періоди. На основі аналізу наукових праць фахівців із зазначеної проблематики надано авторське тлумачення терміна «цифрова освіта» як надання знань і навичок громадянам щодо вільного та безпечного користування цифровими технологіями. На підставі аналізу цифрових навичок українців у 2019–2021 рр. цифрову освіту позиціоновано як таку, що дає змогу задовольняти життєво важливі потреби суспільства в інформації й забезпечує конкурентоспроможність економічної системи країни. Наголошено на необхідності формування та підвищення рівня цифрових компетентностей у громадян і включення їх в освітньо-професійні програми в закладах освіти. У результаті запропоновано комплексний підхід щодо створення системи цифрової освіти для молоді, дорослих та людей похилого віку на основі формування навичок використання цифрових технологій і сервісів, що сприятиме задоволенню життєво важливих інтересів людини, суспільства, держави в інформації та підвищенню якості й комфортності життя населення загалом.*

Ключові слова: *цифрова освіта, цифрові компетентності, цифрові технології, інформаційно-комунікаційні технології, кіберзагрози, життєво важливі інтереси.*

JEL classification: I25.

DOI: 10.32987/2617-8532-2023-1-22-37.

Розвиток цифрових технологій наприкінці XX – на початку XXI ст. надав суспільству нові можливості щодо задоволення життєво важливих інтересів (ЖВІ) населення та забезпечення високого рівня комфортності його життя. За даними звіту Digital 2021 [1], чисельність користувачів Інтернету й цифрових послуг зростає: у 2021 р. вона становила понад 4 млрд осіб, тобто понад 58 % населення планети. Користувачі витрачають на Інтернет близько 6 годин на день, практично стільки ж, як на сон. Оскільки сучасна людина майже 40 % свого життя проводить онлайн,

актуалізується питання цифрової освіти, котра дає змогу набути навички й знання, необхідні для використання цифрових технологій (ЦТ), та підвищити конкурентоспроможність фахівців на ринку праці.

Водночас організація системи цифрової освіти пов'язана з низкою проблем. По-перше, сама система освіти нині розвивається значно повільнішими темпами порівняно з ЦТ, а впровадження інформаційно-комунікаційних технологій (ІКТ) відбувається фрагментарно, переважно як реакція на виклики зовнішнього середовища. По-друге, якщо протягом останніх 10–15 років студенти ЗВО знайомляться з новітніми ІКТ уже в процесі навчання, то старше покоління, котре здобуло освіту 20–30 років тому, отримує ці знання в міру виникнення потреби в них. При цьому сьогодні підготувати фахівця за раз (за 4–5 років) і на все життя не можливо, адже щорічно оновлюється близько 5 % теоретичних та 20 % професійних знань. Отже, цифрова освіта відіграє стратегічну роль для громадян щодо можливостей задоволення їхніх життєво важливих потреб в інформації й розширення їх доступу до ринку праці.

Аналіз останніх досліджень і публікацій щодо стану й розвитку цифрової освіти та інформаційної безпеки дає підстави констатувати, що ці питання вивчають як науковці, так і практики, зокрема В. Антонюк, В. Ляшенко, О. Новікова [2], О. Бондар-Підгурська, А. Глєбова [3; 4], Н. Краус [5], Л. Ляхоцька, В. Ляхоцький [6], І. Малицька [7] та ін. Однак є потреба в комплексному підході до формування системи цифрової освіти на основі ІКТ і ЦТ для молоді, дорослих та людей похилого віку, що передбачатиме набуття ними цифрових компетентностей і сприятиме створенню цифрового освітнього простору.

Метою статті є дослідження стану, проблем і перспектив розвитку цифрової освіти в Україні в умовах воєнного стану й післявоєнної розбудови економіки, а також надання рекомендацій щодо активізації її розвитку.

XXI ст. – час активного розвитку діджитал-технологій, які надають широкі можливості, забезпечують основні бізнес-процеси та відкривають райдужні перспективи для бізнесу, держави, громадян, що набули цифрові компетентності (ЦК). Нині цифрові технології (блокчейн, хмарні технології, мобільний зв'язок, штучний інтелект, ІКТ, робототехніка, концепція розумного міста тощо) стали невід'ємною частиною нашого життя. Їх активними користувачами є не лише бізнес і громадяни, а й держава, оскільки ЦТ відкривають нові можливості для всіх користувачів – населення, інвесторів, держави, бізнесу та ін. Разом із тим саме знання та навички, що їх покликана формувати цифрова освіта, визначатимуть конкурентоспроможність фахівців, рівень і якість життя населення, а також стійкість розвитку економіки загалом.

Розвиток цифрової освіти пов'язаний із появою нових термінів («цифрові компетенції», «цифрові навички», «цифрові технології») поряд із такими категоріями, як «онлайн-освіта», «дистанційна освіта», «інформаційно-комунікаційні технології», котрі потребують узагальнення й систематизації.

Зокрема, Н. Краус під цифровою освітою розуміє саме «таку освіту, яка, головним чином, функціонує за

рахунок цифрових технологій, тобто електронних транзакцій, які реалізуються шляхом використання Інтернету» [5].

У Європі розроблено одну із семи головних ініціатив стратегії Єврокомісії «Європа 2020» – цифрова програма для Європи (Digital Agenda for Europe, 2014), котра визначила розвиток цифрової освіти. Відповідно, у 2018 р. складено План дій із цифрового навчання (The Action Plan on Digital Learning, 2018). При цьому, як зазначає І. Малицька, у країнах Східної та Південно-Східної Європи цифрову освіту включено в більш широкомасштабні державні стратегії, а 18 систем освіти в Західній, Центральній і Північній Європі (Болгарії, Чехії, Данії, Німеччини, Ірландії, Іспанії, Франції, Італії, Люксембургу, Угорщини, Австрії, Словенії, Словаччини, Швеції, Великої Британії, Швейцарії та Норвегії) мають власну окрему стратегію цифрової освіти [7].

ЄС розроблено «План дій цифрової освіти, 2021–2027» (Digital Education Action Plan, 2021-2027), який є ключовим чинником Європейського освітнього простору до 2025 р. (European Education Area 2025), і «Цифровий компас 2030: європейський шлях» (2030 Digital Compass: the European way for the Digital Decade) [8]. Так, у «Плані дій цифрової освіти, 2021–2027» розвиток цифрової освіти розглядається через ЦК і навички, необхідні кожній людині задля отримання рівного доступу до цифрової інфраструктури, можливостей процвітання в житті, пошуку роботи та висловлення активної позиції громадянина.

На Симпозіумі про досягнення в освітніх технологіях 2021 р. (Symposium on Advances in Educational Technology) цифрова освіта розглядалася з позиції використання штучного інтелекту, доповненої реальності, гейміфікації, хмарних технологій, комп'ютерного моделювання, онлайн-, мобільних технологій, цифрових додатків тощо в освітньому середовищі [9].

На нашу думку, цифрова освіта – це надання знань і навичок громадянам щодо вільного й безпечного користування цифровими технологіями. До таких технологій варто віднести Інтернет, соціальні мережі, YouTube, онлайн-книги, довідники, сервіси онлайн-спілкування (Zoom, Google meet та ін.), онлайн-навчання (Moodle, Prometeus, Дія.Освіта), відеофайли, комп'ютерні ігри й тренажери, а також технології блокчейну, електронного підпису, Big Data, смарт-технології тощо. *Зауважимо, що існує істотна різниця між поняттями «технології цифровізації» та «технології оцифрування окремих складових технологій». Цифровізація передбачає інтеграцію технологій на основі ЦТ, а отже, їх перехід на новий рівень якості й досконалості. При цьому ІКТ є етапом, що передує ЦТ, а останні – синонімом терміна «діджитал-технології» (ДТ).* Так цифрова освіта стає ключовим чинником розвитку національної економіки, що сприятиме підвищенню добробуту населення. Вона дає змогу, застосовуючи здобутки НТП, задовольняти потреби громадян в інформації та робить їх спроможними отримувати, обробляти й використовувати її завдяки набутим знанням і навичкам із користування ІКТ та ЦТ.

Водночас ЦТ створюють нові інформаційні загрози (вішинг, смішинг, фішинг тощо), котрі стають реальною небезпекою для користувачів і впли-

вають на їхній матеріальний та соціально-психологічний стан, а в окремих випадках – і на політичну систему держави. Тому оволодіння громадянами ЦК має розглядатись як інструмент протистояння інформаційним загрозам та мінімізації їх наслідків, що стає важливим не лише для них особисто, а й для держави в цілому. Наочно цей процес можна продемонструвати на прикладі України.

Протягом 2014–2022 рр. стало очевидно, що кібербезпека є важливою частиною національної безпеки України, оскільки чисельність користувачів Інтернету в цей період із кожним роком зростала, а держава проводила активну політику діджиталізації державних послуг. За даними Держспецзв'язку, у І кв. 2022 р. здійснено більш ніж 1 350 атак [10], які супроводжували розгортання повномасштабних військових дій на території України. Під час кібератак зловмисники використовували методи соціальної інженерії та цифрові інструменти (смішинг, вішинг, фішинг тощо) з метою отримання персональних даних і даних державних реєстрів, викрадення коштів фізичних та юридичних осіб, причому це стало не лише українською проблемою, а світовою тенденцією. Так, за даними дослідження Canalys, у 2020 р. спостерігалося рекордне зростання числа кіберзлочинів: зламано понад 12 млн записів, які містили велику кількість персональних даних, а чисельність відомих атак програм-вимагачів збільшилася майже на 60 % [11]. Головними причинами посилення кібератак стали неправильні конфігурації хмарних баз даних і фішингові кампанії, націлені на технічні вразливості й низький рівень цифрової освіти працівників. Отже, цифровій освіті наразі відведено провідну роль у формуванні навичок і вмінь щодо безпечного користування ЦТ.

Аналіз темпів розвитку світового ринку кібербезпеки у 2021 р. за технологіями (оптимістичний та песимістичний прогнози) дає підстави для висновку про підвищення значущості цифрової освіти у XXI ст. із позиції цифрової безпеки як її складової. При цьому пандемія COVID-19 посилила започатковану тенденцію й прискорила темпи розвитку ЦТ (рис. 1).

Перелік технологій на світовому ринку кібербезпеки, 2021 р.					
Web- і email-безпека	Аналітика вразливостей та безпеки	Антивірусні системи	Керування доступом до особистих даних	Безпека мереж	Data-безпека
Оптимістичний прогноз					
+12,5	+11,0	+10,4	+10,4	+8,0	+6,6
Песимістичний прогноз					
+8,8	+7,5	+6,2	+8,1	+4,2	+4,2
Відхилення					
+3,7	+3,5	+4,2	+2,3	+3,8	+1,8

Рис. 1. **Тенденції розвитку технологій на світовому ринку кібербезпеки у 2021 р.: аналіз ретроспективного прогнозу,** *%*

Побудовано авторами за: [11].

Сьогодні громадяни й держава активно опановують віртуальне середовище, що стає важливою частиною їхнього повсякденного життя та впливає на швидкість прийняття рішень. У цих умовах задоволення ЖВІ громадянина, суспільства та держави здійснюється переважно завдяки участі в цифровому просторі. Бізнес, реалізуючи свої моделі, теж передбачає використання ЦТ у всіх підсистемах організації управлінського процесу, під час взаємодії з клієнтами й стейкхолдерами. Проте це супроводжується зростанням кількості онлайн-шахрайств і кібератак, що потребує відповідного рівня цифрової безпеки. Тобто збільшення переваг, які отримують користувачі, бізнес та держава від використання ЦТ, залежить від рівня їхньої професійної й спеціальної компетентності, цифрових навичок і знань, що водночас зумовлює збитки внаслідок кібератак. При цьому метою зловмисників не завжди є кошти, здебільшого це отримання інформації, а саме персональних баз даних. Наприклад, в Україні з моменту початку військових дій Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, що діє при Держспецзв'язку, зареєструвала 1 123 кібератаки [10].

Згідно з дослідженням NewsGuard, вебсайту з відстеження дезінформації в Інтернеті, новим користувачам можуть рекомендувати неправдивий контент про Україну протягом 40 хв. після приєднання до мережі [12]. Тому Центр протидії дезінформації при Раді національної безпеки і оборони України на постійній основі інформує суспільство про фейкові наративи, щодня поширювані агресором (таблиця).

Таблиця

Основні фейкові новини, поширювані в українському суспільстві під час дії воєнного стану

№ з/п	Фейк
1	Зеленський оголосив про капітуляцію
2	В Україні не війна, а «спецоперація»
3	Росія «звільняє» лише Схід України
4	В Україні при владі нацисти, тому потрібна «денацифікація»
5	Якщо змінити владу в Україні, то все налагодиться
6	Українці ненавидять росіян, тому хочуть їх убивати
7	Якби не Путін, то в Україну прийшло б НАТО
8	Україна сама себе обстрілює
9	Росія хоче домовлятись, а Україна не хоче
10	Росія все витримає
11	Санкції не працюють
12	Телебачення України повідомляє про капітуляцію й підписання мирного договору з рф
13	Україна збирається виготовляти ядерну зброю
14	Україна планувала напасти на Білорусь
15	Україна вдарила по Донецьку ракетою «Точка-У»
16	Маріупольський «Азов» закликав українців до повалення влади
17	Керівник російської розвідки заявив про плани Польщі на приєднання до свого складу західних земель України

Закінчення таблиці

№ з/п	Фейк
18	Міноборони рф повідомило, що «в Лимані підрозділи ЗСУ з околиць обстрілюють житлові квартали з артилерійських гармат, при цьому журналісти з безпечних місць здійснюють відеозйомку зруйнованих об'єктів цивільної інфраструктури»
19	Українська влада «використовує як живий щит» жителів Лисичанська, тому «не проводить» евакуацію
20	У Сєвєродонецьку НАТО «будував військову базу»
21	В Україні «заборонили» російські книжки
22	Іноземці, які воюють в українській армії, – «злочинці», й Росія «не має» використовувати норми Женевської конвенції щодо них
23	Захід багато років начебто «штовхав Україну до конфлікту» з Росією
24	Україна «блокує» в портах десятки іноземних цивільних суден
25	Проти зс рф у Запорізькій області був застосований ботулотоксин типу «В», російські військові доставлені до шпиталю з ознаками сильного отруєння… Режим Зеленського санкціонував теракти із застосуванням хімічних отруйних речовин проти російських військових
26	Виникнення протистояння Генерального штабу Збройних Сил України з Офісом Президента та Міністерством оборони
27	Неможливо отримати права людині, яка приїхала з тимчасово захоплених територій
28	Байден вимагає продовження військових дій в Україні для утримання влади, при цьому сама Україна перебуває на межі саморозпаду

Складено авторами за: [13–18].

Дієвим засобом протидії поширенню фейкової інформації та підвищення рівня безпеки в процесі використання ЦТ є знання, а саме володіння цифровими навичками (ЦН). Тому проаналізуємо стан і проблеми цифрової освіти України. Так, у 2019 р. було проведено перше комплексне дослідження знань та навичок українців щодо цифрової грамотності [19]. При цьому рівень володіння ЦН включав у себе чотири основні сфери компетенцій: інформаційні, комунікаційні, навички розв'язання проблем і навички програмного забезпечення. Результати дослідження показали, що у 2019 р. 53 % населення України мали базовий рівень ЦН. У 15,1 % населення ЦН взагалі відсутні, серед них люди, старші 60 років, які проживають поза обласними центрами, у селах та містах області, переважно не працюють і ніколи не користувались Інтернетом; у 37,5 % українців рівень володіння ЦН нижчий від середнього, зокрема це люди віком 31–50 років; у 21,5 % – середній рівень; у 25,5 % – вищий за середній [19].

У 2021 р. виконано аналогічне дослідження, результати якого свідчать про *підвищення рівня цифрової грамотності громадян України,* що дає можливість успішніше протистояти новим інформаційним загрозам (рис. 2 і 3).

Так, частка українців, чиї ЦН нижчі від позначки «базовий рівень», скоротилася на 5,2 %, або на 1,42 млн осіб, та наразі становить 47,8 %. При цьому частка українців, які не мають жодних ЦН (No skills), зменшилася на 4 %, або на 1,09 млн осіб. Більш розвиненими з 2019 р. залишаються комунікаційні й інформаційні навички: комунікаційні навички (рівень вищий від базових навичок) мають 79,2 % громадян, інформаційні (рі-

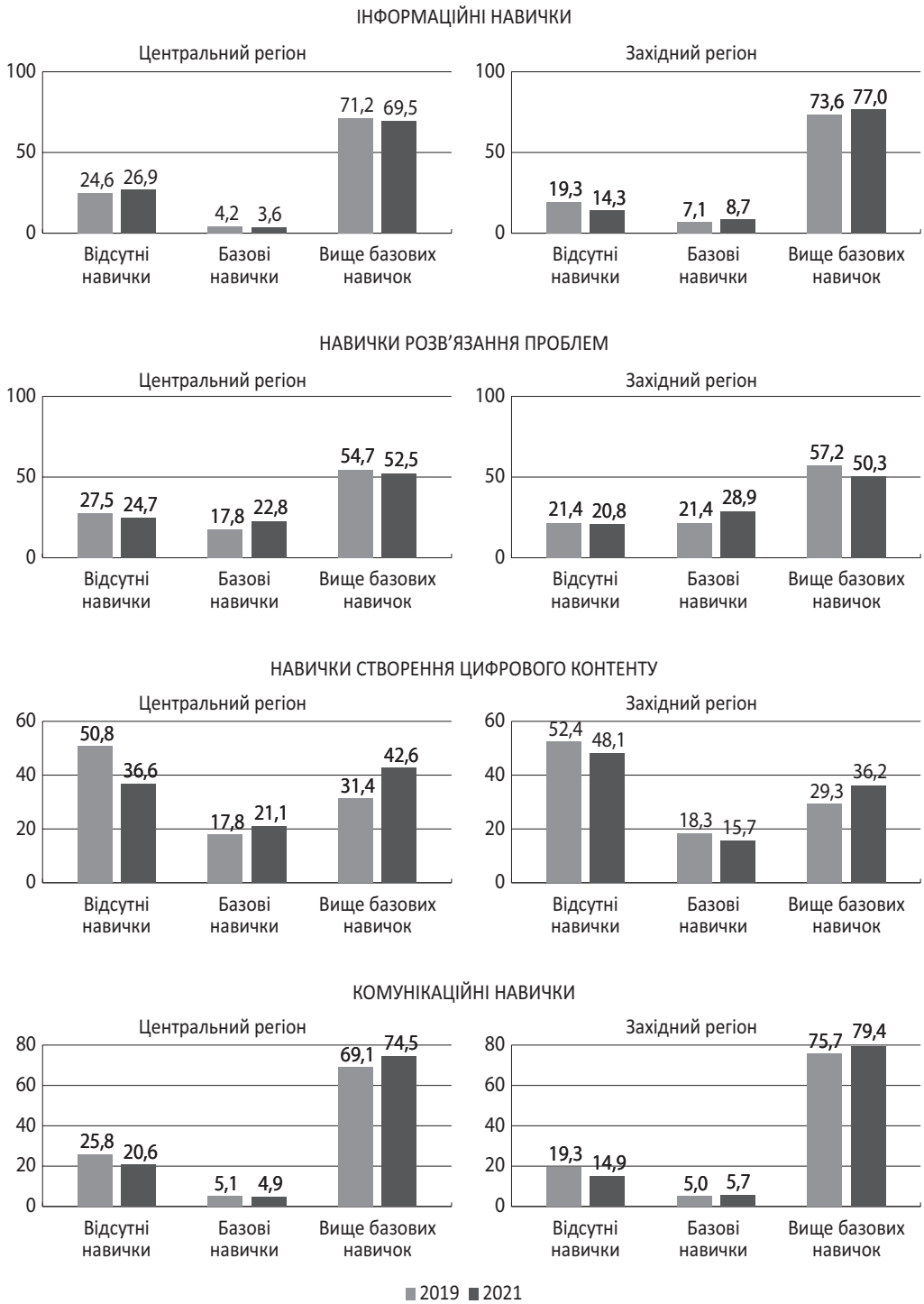

Рис. 2. **Цифрова грамотність українців у 2019 та 2021 рр. у регіональному розрізі: Центральний і Західний регіони,** *%*

Побудовано авторами за: [1].

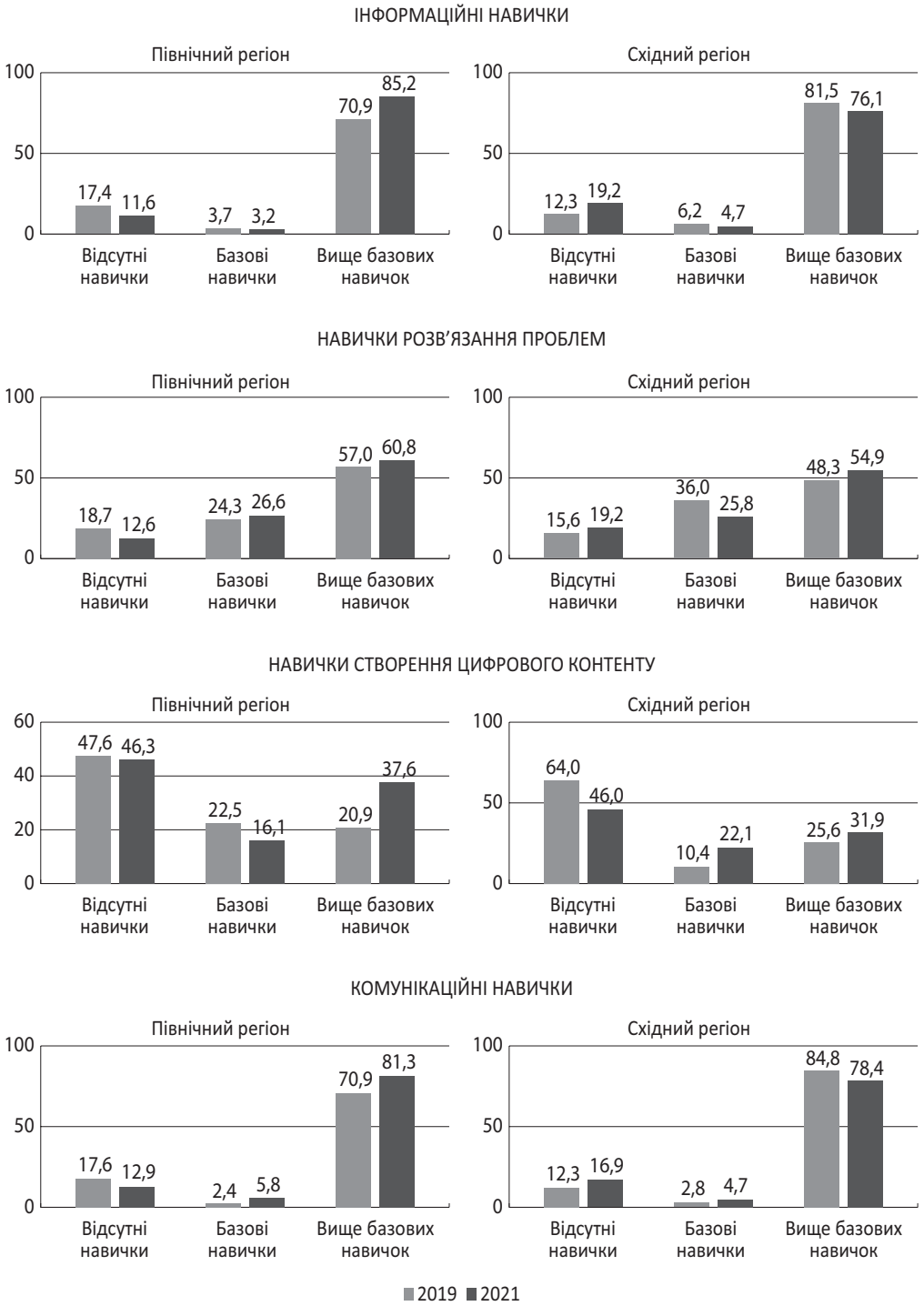

Рис. 3. **Цифрова грамотність українців у 2019 та 2021 рр. у регіональному розрізі: Північний і Східний регіони,** *%*

Побудовано авторами за: [1].

вень вищий від базових навичок) – 78,9 % громадян. Водночас рівень володіння навичками розв'язання життєвих проблем є недостатнім – 55,8 % громадян (рівень вищий від базових навичок).

88 % українців користувалися мережею Інтернет протягом останніх трьох місяців 2019 р., при цьому 93 % із них робили це щодня або практично кожного дня. Популярним місцем користування мережею Інтернет із 2019 р. залишається дім (89 % українців). Другим за популярністю місцем виходу в мережу є місце роботи чи навчальний заклад. Серед пристроїв, котрими користуються для доступу до Інтернету, лідерство зберігається за смартфонами.

Поряд із цим 52 % українців зазначили, що вперше спробували онлайн-інструменти під час пандемії COVID-19. Серед них купівля товарів онлайн, відслідковування новин в Інтернеті та дистанційна робота. Третина опитаних українців зауважили, що в період пандемії стали більше часу проводити в мережі Інтернет, ніж раніше [1].

Водночас із 2019 р. почастішали випадки шахрайських дій у мережі Інтернет. Так, число осіб, які за останніх 12 місяців зазнавали проблем, пов'язаних із безпекою, через використання Інтернету, збільшилось у середньому на 11 %. Окрім того, 45,7 % мешканців України у віці 18–70 років за останній рік ставали об'єктом хоча б одного виду шахрайських дій у мережі Інтернет, серед них 45,9 % населення непідконтрольних територій, 58,7 % людей із порушенням слуху, 40,2 % молоді віком 10–17 років.

При цьому найпоширенішими неправомірними діями в мережі Інтернет у 2021 р., як і в 2019 р., було отримання шахрайських повідомлень, перенаправлення на підроблені вебсайти із запитом особистої інформації та шахрайське використання кредитної чи дебетової карти [19].

Таким чином, цифрова грамотність українців як індикатор цифрової освіти зростає, але досить повільно, тимчасом як використання ЦТ у бізнесі та з метою надання державних послуг відбувається прискореними темпами. Так, від початку пандемії COVID-19 й дотепер в Україні було створено понад 120 цифрових послуг. Зокрема, проєкт «Дія», котрий дав змогу оцифрувати значну частину документів і надавати послуги громадянам швидко й без корупції; у 2021 р. запущено 12 нових послуг на порталі та в застосунку «Дія», такі як призначення/перерахунок пенсії, оформлення субсидії, автоматична реєстрація ФОП, зміна місця реєстрації онлайн у форматі бета-тестування на всю країну. Загалом на порталі «Дія» вже доступно 72 послуги, а в застосунку – 9 послуг і 15 цифрових документів [20].

У зв'язку з веденням активних бойових дій і тимчасовою окупацією окремих регіонів України постала гостра потреба в збереженні цілісності й конфіденційності інформації, недопущенні несанкціонованого втручання та викривлення даних, а також випадків рейдерства. Тому в Україні з початком війни доступ до державних реєстрів через застосунок «Дія» було відключено, особливо в зонах активних бойових дій. Залишилися тільки послуги «єПідтримка», «Допомога армії» та «ДіяTV». Проте вже в березні 2022 р. в окремих регіонах країни доступ до реєстрів було відновлено,

що стало життєво важливим для громадян і бізнесу. Крім того, цифрові сервіси доповнено новими послугами у воєнний час, як-от «Пенсійне посвідчення», «Посвідка на тимчасове або постійне проживання», «Автоматичний дозвіл на будівництво», «Довідка про несудимість», «Грошова допомога переселенцям без зміни даних», «Шеринг паспорта», «Заявка на пошкоджене майно», «єДекларація для бізнесу», «Автоматична реєстрація ТОВ», «Переказ грошей для армії» [21].

Цифрові сервіси у воєнний час уможливили забезпечення ЖВІ громадян, суспільства, держави та стали ключовими інструментами для відновлення бізнесу. Зокрема, держава з метою відновлення економіки на платформі «Дія» запропонувала низку нових послуг для підтримки бізнесу під час війни. Це компенсація за працевлаштування внутрішньо переміщених осіб, тимчасове переміщення підприємств із постраждалих під час війни регіонів, єдина платформа цифрової взаємодії для допомоги бізнесу в процесі його релокації, єРобота, мікрофінансування ветеранського бізнесу; також створено різноманітні державні платформи для кредитування, консалтингових послуг тощо [21].

Отже, ЦТ допомагають не лише підтримати бізнес, а й перезапустити його в умовах воєнної економіки. При цьому інформація стає зброєю, оскільки дає змогу керувати настроєм громадян, моделювати їхню поведінку, управляти їхньою довірою до державних органів.

Роль і значення інформації в умовах гібридної війни в Україні посилюють ІКТ, що дають можливість керувати «довірою до легітимності держави», збільшувати розбіжності на національному й міжнародному рівнях. На думку Хуссейна Халіфи [22], «довіру не можна розуміти як явище одного рівня чи виміру», це результат довготривалого впливу на суспільство через ЦТ.

Аналіз публікацій [23; 24] дав можливість виокремити особливості гібридної війни проти українського народу в контексті застосування ІКТ, а саме:

– здійснення російської агресії без оголошення війни;

– широке використання підготовлених «п'ятої колони» та нерегулярних озброєних формувань;

– нехтування росією міжнародними нормами ведення бойових дій;

– відкрите невиконання чинних угод і досягнутих Мінських домовленостей;

– заходи політичного й економічного тиску на Україну;

– приховування російським керівництвом безпосередньої участі рф у збройному конфлікті;

– масова антиукраїнська пропаганда та контрпропаганда із застосуванням брудних інформаційних технологій;

– використання методів психологічного тиску;

– широке використання дезінформації та створення численних фейків через ЗМІ й соціальні мережі;

– невизначеність «меж війни», що є розмитими, важко ідентифікованими й неоднозначними;

– здійснення кібератак на постійній основі щодо об'єктів критичної інфраструктури та органів влади;

– підміна культурних і соціальних цінностей;

– підрив легітимності держави, а саме розмивання довіри між державними інституціями й людьми.

Усвідомлюючи важливість ЦТ у період війни та післявоєнної розбудови національної економіки, варто запропонувати комплексний підхід щодо створення системи цифрової освіти для молоді, дорослих і людей похилого віку на основі формування навичок використання ЦТ і сервісів, що сприятиме задоволенню ЖВІ людини, суспільства, держави та підвищенню якості й комфортності життя населення. Виконати завдання із формування необхідних компетентностей у громадян покликана система освіти, яка завдяки включенню їх в освітньо-професійні програми сприятиме становленню та розвитку цивілізованого діджитал-суспільства.

Проведене дослідження дало змогу дійти таких висновків:

1. Цифрова освіта – це ключовий чинник розвитку національної економіки, що дає можливість громадянам отримувати інформацію шляхом здобуття ЦН і знань щодо вільного й безпечного користування сучасними ЦТ. Саме цифрова освіта покликана забезпечити зростання добробуту громадян і держави в умовах інформаційної (цифрової) економіки, де основним товаром є інформація. Цифрова освіта є вразливою до кіберзагроз, які стають невід'ємною частиною віртуального середовища, що потребує конкретних знань і вмінь щодо цифрової безпеки.

2. Цифрова освіта перебуває на стадії формування, про що свідчать тенденції зростання ЦН громадян у всіх регіонах України протягом 2019–2021 рр. Зокрема, молодь може набути окремі ЦН у закладах освіти, а можливості дорослих і людей похилого віку обмежені. При цьому цифрова грамотність українців як індикатор цифрової освіти зростає, але досить повільно, тимчасом як використання ЦТ у бізнесі та з метою надання державних послуг відбувається прискореними темпами. Рівень володіння ЦН обумовлений віковою категорією, доступністю до Інтернету й цифровою безпекою.

3. Запропоновано комплексний підхід щодо створення системи цифрової освіти для молоді, дорослих і людей похилого віку, котрий ґрунтується на формуванні навичок використання ЦТ та сервісів, що сприятиме задоволенню ЖВІ людини, суспільства, держави й підвищенню якості та комфортності життя населення.

4. ЦН студентів доцільно формувати під час їх навчання в закладах вищої освіти в межах загальних і спеціальних компетентностей освітньо-професійних програм. Здобуті в межах цих програм ЦК сприятимуть підвищенню конкурентоспроможності фахівців на ринку праці не лише України, а й інших країн світу.

Список використаних джерел

1. Цифрова грамотність населення України: звіт за результатами загальнонаціонального опитування. 2021. *Міністерство цифрової трансформації*. URL: https://osvita.diia.gov.ua/uploads/0/2625-doslidzenna_2021_ukr.pdf (дата звернення: 15.01.2023).

2. Формування концептуальних засад цифрової трансформації освіти та науки України / О. Ф. Новікова та ін. *Вісник економічної науки України*. 2021. № 1(40). С. 190–198. DOI: https://doi.org/10.37405/1729-7206.2021.1(40).190-198 (дата звернення: 15.01.2023).

3. Bondar-Pidhurska O., Glebova A. Information security as a digital technology's development factor of innovative sociallyoriented economy. *Advances in Economics, Business and Management Research* : Proceedings of the 2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020). 2020. DOI: https://doi.org/10.2991/aebmr.k.201205.051.

4. *Бондар-Підгурська О. В., Глєбова А. О.* Професійна освіта як інструмент і шлях до задоволення життєво важливих інтересів жителів об'єднаних територіальних громад. *Трансформація моделей управління освітою в територіальних громадах у процесі децентралізації: стан, проблеми, перспективи* : кол. моногр. Київ : ТОВ НВП «Росток А. В. Т.», 2022. С. 336–359. URL: https://www.airo.com.ua/wp-content/uploads/2022/12/monografiya-imzo-monu-2022-verstk.pdf (дата звернення: 15.01.2023).

5. *Краус К. М.* Імперативи формування цифрової освіти в Україні. *Управління соціально-економічними трансформаціями у сучасному місті* : матеріали Всеукр. наук.-практ. конф., м. Київ, 27 лют. 2018 р. Київ : КУБГ, 2018. С. 49–51. URL: http://dspace.puet.edu.ua/handle/123456789/6059 (дата звернення: 15.01.2023).

6. *Ляхоцька Л. Л., Ляхоцький В. П.* Цифрова освіта і наука – запорука національної безпеки України. *Національна безпека України у викликах новітньої історії* : кол. моногр. Київ : ДП «Експрес-об'ява», 2019. Ч. ІІ. С. 277–289. URL: https://cutt.ly/S4zTAAG (дата звернення: 15.01.2023).

7. *Малицька І.* Цифрова освіта країн Європейського Союзу під час пандемії COVID-19. *Педагогічна компаративістика і міжнародна освіта – 2021: інновації в освіті в контексті європеїзації та глобалізації* : матеріали V Міжнар. наук.-практ. конф., м. Київ, 27–28 трав. 2021 р. Тернопіль : Крок, 2021. С. 65–67. URL: https://undip.org.ua/wp-content/uploads/2021/08/Comparative_2021_w.pdf (дата звернення: 15.01.2023).

8. Digital education. *European Commission*. 2022. URL: https://education.ec.europa.eu/focus-topics/digital-education (дата звернення: 15.01.2023).

9. Symposium on Advances in Educational Technology. *AET*. 2020. November 12-13. URL: https://aet.easyscience.education/2020/ (дата звернення: 15.01.2023).

10. Цьогоріч російські хакери атакували українську інфраструктуру понад 1300 разів. *LB.UA.* 2022. URL: https://lb.ua/society/2022/07/13/522985_tsogorich_rosiyski_hakeri_atakuvali.html (дата звернення: 15.01.2023).

11. Global cybersecurity 2021 forecast. *Canalys.* 2021. URL: https://canalys.com/newsroom/canalys-cybersecurity-2021-forecast (дата звернення: 15.01.2023).

12. *Сардаризаде Ш.* Як фейки про війну в Україні збирають мільйони переглядів у TikTok. *BBC*. 2022. URL: https://www.bbc.com/ukrainian/features-61220423 (дата звернення: 15.01.2023).

13. *Прищепа Я.* Розвінчування російських фейків 4 квітня. *Суспільне Новини.* 2022. URL: https://suspilne.media/225215-rozvincuvanna-rosijskih-fejkiv-4-kvitna/ (дата звернення: 15.01.2023).

14. Розвінчування російських фейків 23 червня. *Суспільне Новини.* 2022. URL: https://suspilne.media/253509-rozvincuvanna-rosijskih-fejkiv-23-cervna/ (дата звернення: 15.01.2023).

15. *Терещенко О.* Війна Росії проти України: спростовуємо 30 фейків окупантів. *24 канал*. 2022. URL: https://24tv.ua/viyna-rosiyi-proti-ukrayini-sprostovuyemo-feyki-okupantiv-onovlyuyetsya_n1889316 (дата звернення: 15.01.2023).

16. Новини. *Міністерство цифрової трансформації України*. 2022. URL: https://thedigital.gov.ua/news (дата звернення: 15.01.2023).

17. Фейки. *Укрінформ.* 2022. URL: https://www.ukrinform.ua/tag-fejk (дата звернення: 15.01.2023).

18. *Білал А.* Гібридна війна – нові загрози, складність і «довіра» як антидот. *NATO Review*. 2021. URL: https://www.nato.int/docu/review/uk/articles/2021/11/30/gbridna-vjna-nov-zagrozi-skladnst-dovra-yak-antidot/index.html (дата звернення: 15.01.2023).

19. Цифрова грамотність населення України: звіт за результатами загальнонаціонального опитування. *Міністерство цифрової трансформації України*. 2019. URL: https://osvita.diia.gov.ua/uploads/0/585-cifrova_gramotnist_naselenna_ukraini_2019_compressed.pdf (дата звернення: 15.01.2023).

20. Цифрові паспорти, COVID-сертифікати, єПідтримка: 100 перемог Дії та Мінцифри. *Дія.* 2021. URL: https://diia.gov.ua/news/cifrovi-pasporti-sovid-sertifikati-yepidtrimka-100-peremog-diyi-ta-mincifri (дата звернення: 15.01.2023).

21. Підтримка бізнесу в умовах війни. *Дія. Бізнес*. 2022. URL: https://business.diia.gov.ua/wartime (дата звернення: 15.01.2023).

22. *Khalifa H., Al-Absy M., Badran Sh., Almaamari T. A. Q., Nagi M.* COVID-19 Pandemic and Diffusion of Fake News through Social Media in the Arab World. *ARAb Media&Societe.* 2021. URL: https://www.arabmediasociety.com/covid-19-pandemic-and-diffusion-of-fake-news-through-social-media-in-the-arab-world/ (дата звернення: 15.01.2023).

23. *Гетьманчук М. П.* «Гібридна війна» Росії проти України: інформаційний аспект. *Військово-науковий вісник.* 2017. № 27. С. 296–307. URL: http://nbuv.gov.ua/UJRN/vnv_2017_27_23 (дата звернення: 15.01.2023).

24. *Шутяк Л.* Соціальні мережі як середовище фейків: що треба знати про Facebook. *Explainer.* 2021. URL: https://explainer.ua/sotsialni-merezhi-yak-seredovishhe-fejkiv-shho-treba-znati-pro-facebook/ (дата звернення: 15.01.2023).

Oksana Bondar-Pidhurska
Dr. Sc. (Economics), Associate Professor, Poltava University of Economics and Trade, Poltava, Ukraine, bondarpodgurskaa@gmail.com
ORCID ID: https://orcid.org/0000-0001-7792-4023

Alla Glebova
Ph. D. (Economics), Associate Professor, National University «Poltava Polytechnic named after Yury Kondratyuk», Poltava, Ukraine, alliaglebova@gmail.com
ORCID ID: https://orcid.org/0000-0002-7030-948X

THE STATE, PROBLEMS AND PROSPECTS OF DIGITAL EDUCATION DEVELOPMENT IN UKRAINE DURING THE WAR AND POST-WAR PERIOD

Abstract. *The relevance of the study lies in the need to resolve the contradiction between the rapid pace of development of digital technologies in the world and the low level of digital skills of the Ukrainian population, which should be eliminated through education. The purpose of the study is to examine the state, problems and prospects for the development of digital education in Ukraine, as well as to develop recommendations for intensifying this process during the wartime and post-war period. The methods of analysis and synthesis, generalization, and visualization were used. The scientific novelty of the obtained results is the development of theoretical foundations and practical recommendations for solving the problem of digital education development in Ukraine. The authors consider the concept of "digital education" as providing citizens with knowledge and skills for the easy and safe use of digital technologies. The results of the analysis of the development of digital education of the population in all regions of Ukraine during 2019–2021 showed that it is at the stage of formation, as evidenced by the trends of the gradual growth of citizens' digital skills. It was emphasized that the level of digital skills is determined by age group, Internet access and digital security. A comprehensive approach to the creation of a digital education system for youth, adults and the elderly is proposed, based on the formation of skills in the use of digital technologies and services, which will contribute to the satisfaction of the vital interests of a person, society and the state. For the first time, the article highlights the expediency of forming students' digital skills while studying in higher education institutions within the framework of general and special competencies of educational and professional programs, which will increase the level of specialists' competitiveness in the labor market.*

Keywords: *digital education, digital competencies, digital technologies, information and communication technologies, cyber threats, vital interests.*

References

1. Ministry of Digital Transformation. (2021). *Digital literacy of the population of Ukraine: a report based on the results of a nationwide survey*. Retrieved from https://osvita.diia.gov.ua/uploads/0/2625-doslidzenna_2021_ukr.pdf [in Ukrainian].

2. Novikova, O. F., Antoniuk, V. P., Liashenko, V. I., Azmuk, N. A., Ostafiichuk, Ya. V., Shamileva, L. L., ...& Kasperovych, O. Y. (2021). Formation of Conceptual Bases of Digital Transformation of Education and Science of Ukraine. *Bulletin of economic science of Ukraine, 1(40),* 190-198. DOI: https://doi.org/10.37405/1729-7206.2021.1(40).190-198 [in Ukrainian].

3. Bondar-Pidhurska, O. V., & Glebova, A. O. (2020). Information security as a digital technology's development factor of innovative socially oriented economy. *Advances in Economics, Business and Management Research,* Proceedings of the 2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020). DOI: https://doi.org/10.2991/aebmr.k.201205.051.

4. Bondar-Pidhurska, O. V., & Glebova, A. O. (2022). Vocational education as a tool and a way to satisfy the vital interests of residents of united territorial communities. In *Transformation of education management models in territorial communities in the process of decentralization: state, problems, prospects*. Kyiv. Retrieved from https://www.airo.com.ua/wp-content/uploads/2022/12/monografiya-imzo-monu-2022-verstk.pdf [in Ukrainian].

5. Kraus, K. M. (2018). Imperatives of the formation of digital education in Ukraine. *Management of socio-economic transformations in the modern city*, Proceedings of the All-Ukrainian Scientific and Practical Conference. Kyiv. Retrieved from http://dspace.puet.edu.ua/handle/123456789/6059 [in Ukrainian].

6. Liakhotska, L. L., & Liakhotskyi, V. P. (2019). Digital education and science are the key to Ukraine's national security. In *National security of Ukraine in the challenges of recent history* (pp. 277-289). Kyiv. Retrieved from https://cutt.ly/S4zTAAG [in Ukrainian].

7. Malytska, I. (2021). Digital education of the countries of the European Union during the COVID-19 pandemic. *Pedagogical comparative studies and international education - 2021: innovations in education in the context of Europeanization and globalization*, Proceedings of the 5th International Scientific and Practical Conference. Ternopil. Retrieved from https://undip.org.ua/wp-content/uploads/2021/08/Comparative_2021_w.pdf [in Ukrainian].

8. European Commission. (2022). *Digital education*. Retrieved from https://education.ec.europa.eu/focus-topics/digital-education.

9. AET. (2020). *Symposium on Advances in Educational Technology*. Retrieved from https://aet.easyscience.education/2020/.

10. LB.UA. (2022). *This year, russian hackers attacked Ukrainian infrastructure more than 1,300 times*. Retrieved from https://lb.ua/society/2022/07/13/522985_tsogorich_rosiyski_hakeri_atakuvali.html [in Ukrainian].

11. Canalys. (2021). *Global cybersecurity 2021 forecast*. Retrieved from https://canalys.com/newsroom/canalys-cybersecurity-2021-forecast.

12. Sardaryzade, Sh. (2022). *How fakes about the war in Ukraine collect millions of views on TikTok*. Retrieved from https://www.bbc.com/ukrainian/features-61220423 [in Ukrainian].

13. Pryshchepa, Ya. (2022). Debunking russian fakes on April 4. *Social News.* Retrieved from https://suspilne.media/225215-rozvincuvanna-rosijskih-fejkiv-4-kvitna/ [in Ukrainian].

14. Social News. (2022). *Debunking russian fakes on June 23*. Retrieved from https://suspilne.media/253509-rozvincuvanna-rosijskih-fejkiv-23-cervna/ [in Ukrainian].

15. Tereshchenko, O. (2022). Russia's war against Ukraine: we refute 30 fakes of the occupiers. *Channel 24.* Retrieved from https://24tv.ua/viyna-rosiyi-proti-ukrayini-sprostovuyemo-feyki-okupantiv-onovlyuyetsya_n1889316 [in Ukrainian].

16. Ministry of Digital Transformation of Ukraine. (2022). *News*. Retrieved from https://thedigital.gov.ua/news [in Ukrainian].

17. Ukrinform. (2022). *Fake*. Retrieved from https://www.ukrinform.ua/tag-fejk [in Ukrainian].

18. Bilal, A. (2021). Hybrid warfare – new threats, complexity and "trust" as an antidote. *NATO REVIEW.* Retrieved from https://www.nato.int/docu/review/uk/articles/2021/11/30/gbridna-vjna-nov-zagrozi-skladnst-dovra-yak-antidot/index.html [in Ukrainian].

19. Ministry of Digital Transformation of Ukraine. (2019). *Digital literacy of the population of Ukraine: a report based on the results of a nationwide survey*. Retrieved from https://osvita.diia.gov.ua/uploads/0/585-cifrova_gramotnist_naselenna_ukraini_2019_compressed.pdf [in Ukrainian].

20. Diia. (2021). *Digital passports, COVID certificates, eSupport: 100 victories of Diia and the Ministry of Digital Transformation of Ukraine*. Retrieved from https://diia.gov.ua/news/cifrovi-pasporti-sovid-sertifikati-yepidtrimka-100-peremog-diyi-ta-mincifri [in Ukrainian].

21. Diia. (2022). *Business support in wartime*. Retrieved from https://business.diia.gov.ua/wartime [in Ukrainian].

22. Khalifa, H., Al-Absy, M., Badran, Sh., Almaamari, T. A. Q., & Nagi, M. (2021). COVID-19 Pandemic and Diffusion of Fake News through Social Media in the Arab World. *ARAb Media&Societe.* Retrieved from https://www.arabmediasociety.com/covid-19-pandemic-and-diffusion-of-fake-news-through-social-media-in-the-arab-world/.

23. Hetmanchuk, M. P. (2017). "Hybrid war" of russia against Ukraine: information aspect. *Military-scientific bulletin, 27,* 296-307. Retrieved from http://nbuv.gov.ua/UJRN/vnv_2017_27_23 [in Ukrainian].

24. Shutiak, L. (2021). Social networks as an environment of fakes: what you need to know about Facebook. *Explainer*. Retrieved from https://explainer.ua/sotsialni-merezhi-yak-seredovishhe-fejkiv-shho-treba-znati-pro-facebook/ [in Ukrainian].