УДК 338: 330.34.011+004 DOI https://doi.org/10.35546/kntu2078-4481.2024.1.48

С. А. ГОРБАЧЕНКО
доктор економічних наук, професор,
завідувач кафедри кібербезпеки
Національний університет «Одеська юридична академія»
ORCID: 0000-0001-8442-9581

Н. А. КЛЄВЦЄВИЧ
кандидат економічних наук, доцент,
старший науковий співробітник відділу розвитку підприємництва
ДУ «Інститут ринку і економіко-екологічних досліджень
Національної академії наук України»
ORCID: 0000-0002-2010-4814

РОЛЬ КІБЕРБЕЗПЕКИ У ВПРОВАДЖЕННІ ЦИРКУЛЯРНИХ ЕКОНОМІЧНИХ МОДЕЛЕЙ: АНАЛІЗ РИЗИКІВ ТА МОЖЛИВОСТЕЙ

Методичну основу даної наукової роботи складають висновки щодо аналізу і теоретичного узагальнення наукових підходів до координації економічного розвитку в умовах цифрової циркулярної економіки, що наведені в роботах теоретичного та практичного характеру. Для досягнення поставленої мети в статті використані методи графічної інтерпретації результатів аналізу та узагальнення, методи теоретичного аналізу, синтезу. У статті встановлено, що останнім часом світова економіка функціонувала в лінійному форматі. Автори дійшли висновку, що такий тип економічного розвитку створює певні ризики для нормального існування всього світу, який споживає більше ресурсів, ніж може відновити. Доведено, що циркулярна економіка це змінює. Визначено, що для реалізації таких світоглядних рішень у глобальному вимірі важливо створити відповідну цифрову основу. Встановлено, що впровадження цифрових технологій належить до засобів забезпечення переходу до замкнутої економіки. Зроблено висновок, що нові технології та бізнес-моделі, а також високі темпи їх впровадження несуть нові ризики (втрата даних, неякісне програмне забезпечення, технічне відставання, недостатній рівень компетенцій, порушення конфіденційності втрата робочих місць, технічні збої), але кібербезпека робить швидкі цифрові зміни безпечнішими. Зазначається, що для мінімізації цих ризиків важливо впроваджувати ефективні заходи кібербезпеки, регулярно оновлювати системи та програмне забезпечення, налагоджувати навчання персоналу та дотримуватись етичних стандартів використання технологій. Зрештою, брак впевненості користувачів у безпеці онлайн-сервісів та захисті конфіденційності ставить під загрозу можливість використання повного потенціалу інформаційно-комунікаційних технологій для стимулювання інновацій, циркулярного економічного зростання та прогресу в напрямку таких трансформаційних змін. Встановлено, що з розвитком цифровізації та комп'ютеризації як у виробничих процесах, так і в повсякденному житті масштаби кіберзагроз будуть зростати пропорційно збільшенню набору циркулярних продуктів і послуг, що використовують інформаційні технології, та кількості їх споживачів. Зважаючи на це, забезпечення кібербезпеки є актуальним завданням державного та приватного секторів, а розробка адекватних заходів протидії таким викликам і загрозам стає важливим вектором державної політики. Доведено, що проблема кібербезпеки стає надзвичайно гострою та важливою, з цього випливає, що подальший розвиток циркулярної економіки в умовах цифровізації та отримання її переваг людством нерозривно пов'язане з одночасним розвитком відповідної системи кібербезпеки.

Ключові слова: *економіка замкнутого циклу, кругова економіка, циркулярна економіка, інформаційні технології, інструменти кібербезпеки.*

S. A. HORBACHENKO
Doctor of Economics, Professor,
Head of the Cyber Security Department
National University "Odesa Law Academy"
ORCID: 0000-0001-8442-9581

N. A. KLEVTSYEVYCH
PhD, Associate Professor,
Senior Research Fellow at the Department of Entrepreneurship Development
State Organization "Institute of Market and Economic & Ecological Researches
of the National Academy of Sciences of Ukraine"
ORCID: 0000-0002-2010-4814

THE ROLE OF CYBERSECURITY IN THE IMPLEMENTATION OF CIRCULAR ECONOMIC MODELS: RISK AND OPPORTUNITY ANALYSIS

The methodological basis of this scientific work consists of conclusions regarding the analysis and theoretical generalization of scientific approaches to the coordination of economic development in the conditions of a digital circular economy, which are given in works of a theoretical and practical nature. To carry out this scientific work and achieve the set goal, the article uses methods of graphic interpretation of the results of analysis and generalization, methods of theoretical analysis, synthesis. The article established that recently the world economy functioned in a linear format. The authors concluded that this type of economic development creates certain risks for the normal existence of the whole world, which consumes more resources than it can restore. The circular economy is proven to change this. It was determined that for the implementation of such worldview solutions in a global dimension, it is important to create an appropriate digital basis. It has been established that the implementation of digital technologies belongs to the means used to ensure the transition to a closed-loop economy. It was concluded that new technologies and business models, as well as the high pace of their implementation, carry new risks (loss of data, low-quality software, technical lag, insufficient level of competence, violation of confidentiality and privacy, dependence on IT, loss of jobs, technical failures), but cybersecurity makes rapid digital change safer. It is noted that in order to minimize these risks, it is important to implement effective cyber security measures, regularly update systems and software, provide staff training and adhere to ethical standards of technology use. After all, the lack of confidence of users in the security of online services and the protection of privacy threatens the possibility of using the full potential of information and communication technologies to stimulate innovation, circular economic growth and progress in the direction of such transformational changes.It has been established that with the development of digitization and computerization both in production processes and in everyday life, the scale of cyber threats will grow in proportion to the increase in the set of circular products and services that use information technologies and the number of their consumers. Taking this into account, ensuring cyber security is an urgent task for the public and private sectors, and the development of adequate countermeasures against such challenges and threats is becoming an important vector of public policy. It has been proven that the problem of cyber security is becoming extremely acute and important, from this it follows that the further development of the circular economy under the conditions of digitalization and the obtaining of its benefits by humanity is inextricably linked with the simultaneous development of the relevant cyber security systems.

Key words: *closed cycle economy, circular economy, circular economy, information technologies, cyber security tools.*

Постановка проблеми

Протягом останніх років світова економіка діяла за принципами лінійного виробництва, де ресурси з природного середовища використовувалися для створення продукції та викидалися як відходи. Однак ця модель, що базується на масовому виробництві та споживанні, стає загрозою для сталого майбутнього, оскільки людство витрачає природні ресурси набагато швидше, ніж вони можуть відновитися. Концепція економіки замкнутого циклу, також відома як циркулярна економіка чи кругова економіка, принесла зміни у глобальному розумінні ефективного використання ресурсів. На світовому рівні вона розглядається як можливість функціонування економіки, де ресурси використовуються, але не витрачаються. У цій економічній системі передбачається здійснення економічного зростання шляхом переходу від лінійних виробничих практик. Але не дивлячись на те, що перехід від лінійної моделі до моделі економіки замкнутого циклу все ще знаходиться на етапі становлення, потенціал таких змін доволі високий. Впровадження цифрових технологій належать до інструментів, що застосовуються для забезпечення переходу до економіки замкнутого циклу. Разом із цим нові технології та інтенсивна динаміка їх впровадження несуть нові ризики, проте кібербезпека робить швидкі цифрові зміни безпечнішими. Адже непевність користувачів щодо безпеки онлайн-сервісів та захисту конфіденційності гальмує використання потенціалу цифрових технологій у сприянні інноваціям, циркулярному економічному рості та загальному прогресі в напрямку значущих трансформацій. Подібним загрозам піддаються усі без виключення країни світу, а проблема кібербезпеки набуває неабиякої гостроти і важливості. З цього слідує, що подальший розвиток циркулярної

економіки на умовах цифровізації і отримання суспільством її переваг нерозривно пов'язаний із одночасною розбудовою відповідних систем кібербезпеки.

Аналіз останніх досліджень і публікацій

Дослідженню аспектів циркулярної економіки присвячено чимало робіт вітчизняних та закордонних науковців. Потапенко В., Корнатовський Р., Шилкіна О., Харічков С., Батова Н., Сачек П., Точицька І. концентрують увагу в своїх працях саме на цих питаннях. В останні роки все більшої актуальності набирають наукові публікації про необхідність та неминучість цифровізації, свої наукові розробки цьому питанню присвячують Січкаренко К. О., Гончар С. Ф., Грановський М. В., Грабар І. Г. Вивченню важливості забезпечення кібербезпеки для розвитку цифрової економіки циркулярного типу присвячено ряд зарубіжних досліджень, зокрема Wilts H., Moşteanu N., Faccia A., Cavaliere L., Antikainena M., Uusitaloa T., Kivikyto-Reponena P., Scarpellini S., Portillo-Tarragona P., Aranda-Uson A., LlenaMacarulla F. В них відзначається, що важливим аспектом позитивного розвитку таких економічних систем є забезпечення надійного цифрового середовища, становлення якого потребує змін та доповнення відповідного правового поля і публічних дій у сфері кібербезпеки. Їх увага зосереджується на тому, що кіберзагрози гальмують темпи розвитку цифрової економіки, а значить не створюють умов у напрямку циркулярних трансформацій. Проте їх дослідження здебільшого зосереджені на сфері нормативно-правового регулювання та формуванні системи інформаційної безпеки держави, тоді як мало дослідженим торкаються питань впливу кібербезпеки на формування та розвиток цифрової економіки циркулярного типу.

На думку авторів статті, відкритим залишається питання про вигоди та ризики одночасного цифрового та циркулярного розвитку економіки, що зумовлює актуальність вибраної теми дослідження та його мету.

Формулювання мети дослідження

Метою дослідження є визначення ролі інструментів кібер безпеки в циркулярних бізнес моделях, аналіз їх ризиків та можливостей з якими пов'язане їх використання.

Виклад основного матеріалу дослідження

Сутність економіки замкнутого циклу полягає у її прагненні повторити закриту природну систему, де все, що вироблено чи використано, повністю переробляється всередині системи так, що не виникає екологічних проблем. Її мета – забезпечення максимальної ефективності від кожного процесу у життєвому циклі товару чи послуги. Циркулярна економіка впливає на розподільну систему, пріоритетним ресурсом у якій є вторинні ресурси [1].

Перехід до циркулярного типу розвитку економіки обумовлений перш за все суттєвим тиском на довкілля та ризиковістю усталених протягом багатьох років бізнес-моделей, що здійснюються в рамках лінійної економіки. Між циркулярною та лінійною моделями економіки існує низка суттєвих відмінностей. Циркулярна модель економіки відрізняється від лінійної способом створення та підтримки цінності у ланцюжку. Лінійна економіка передбачає: «видобуток – виробництво – утилізація», в якому основна увага у створенні вартості приділяється якомога більшим обсягам виробництва та продажу товарів (рис. 1).

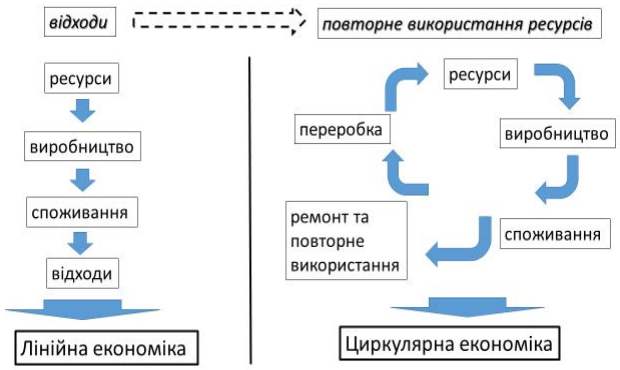

Рис. 1. Порівняння моделей лінійної та циркулярної економіки

Джерело: складено авторами.

Переформатування економіки у напрямку циркулярності вимагає використання прогресивних інноваційних рішень на всіх стадіях життєвого циклу товарів, основна частина з яких передбачає інтенсивне використання цифрових технологій. З цього випливає, що цифровізація може надати імпульс та зробити результативнішим перехід в напрямку економіки замкнутого циклу, замикаючи ланцюжок ресурсів та демонструючи повну інформацію про їхню наявність та стан тощо. Цифрові технології мають великий потенціал для забезпечення переходу до циркулярної економіки, тому що тільки завдяки її нововведенням можливо кардинально змінити існуючий стан справ до більш екологічного (рис. 2). Саме вони можуть забезпечити переформатування існуючих процесів,

оскільки являють собою механізми, які здатні збільшувати економічну значущість і при цьому зменшуючи існуючі витрати [2].

Наразі існує велика кількість практик, що свідчать про перші кроки до реалізації ідей циркулярної економіки. Багато компанії вже використовують нові технології для виключення відходів та забруднення з ланцюжків створення вартості, надаючи при цьому позитивний екологічний та соціальний вплив [3].

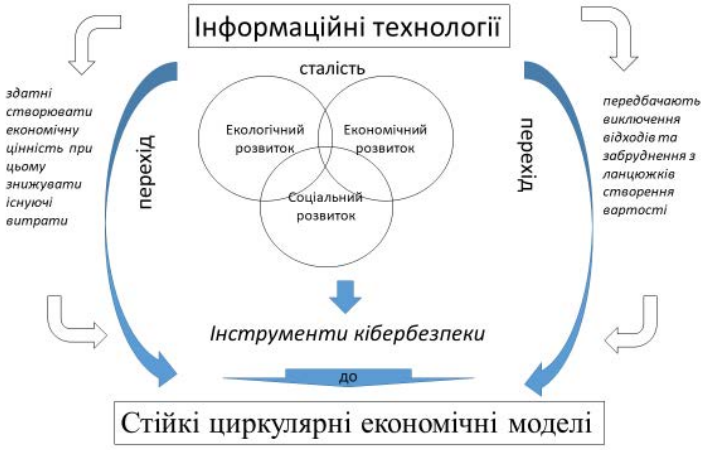

Рис. 2. Взаємозв'язок ціфровізації та циркулярної економіки для досягнення цілей сталого розвитку

Джерело: складено авторами.

Проте суб'єктам господарювання необхідно не тільки визначитися з напрямком впровадження ідей циркулярної економіки, а й розуміти, за допомогою яких інструментів можливо безпосередньо здійснити таку трансформацію. Існуючі цифрові технологічні рішення представлені на рис. 3.

Впровадження інформаційних технологій в сучасне суспільство та бізнес-середовище приносить численні можливості, але також несе і певні ризики, які варто прораховувати.

Серед основних можемо виділити [3]: втрата конфіденційної інформації (втрата даних може суттєво впливати на бізнес); ненадійне програмне забезпечення (використання неякісного програмного забезпечення може сформувати умови для можливих атак); технічне відставання (швидкий темп змін в ІТ може суттєво збільшувати вартість оновлення обладнання та програмного забезпечення); недостатній рівень компетентності (неспроможність персоналу ефективно працювати з новими технологіями може призвести до зниження продуктивності їх праці та збитків); порушення приватності (можливість незаконного доступу до особистої інформації може порушити конфіденційність користувачів); залежність від ІТ (збільшена залежність від ІТ може призвести до проблем, якщо системи вийдуть з ладу чи стануть недоступними); втрата робочих місць (може відбуватися втрата робочих місць через автоматизацію багатьох процесів); технічні збої (збої в роботі ІТ-інфраструктури можуть призвести до значних перерв у роботі бізнесу).

Рис. 3. Цифрові технології, що використовуються для переходу на циркулярні рейки економічного розвитку

Джерело: складено авторами

Для зменшення цих негативів важливо впроваджувати заходи кібербезпеки, проводити постійне оновлення систем та програмного забезпечення, здійснювати навчання персоналу та дотримуватися етичних стандартів використання цифрових технологій.

В узагальненому вигляді під кібербезпекою розуміють сукупність спеціальних правових, організаційних, і технічних заходів, реалізація яких дозволяє забезпечити захист інформаційних комп'ютерних систем, мереж і різних програмних додатків від кібернетичних атак зловмисників [3]. Такі атаки можуть завдати значних матеріальних збитків як підприємствам, внаслідок втрати коштів, активів або розкриття важливої конфіденційної інформації, так і публічному секторові – спричинити збитки для цивільної, фінансової, енергетичної та військової інфраструктури.

Основними видами кібератак є [4]: фішинг – зловмисники надсилають електронні листи або повідомлення представлені законні, і виманюють грошові кошти або важливу інформацію. Також вони можуть замінювати URL-адресу; боти та автоматичні атаки – найчастіше кібератаки здійснюють автоматизовані боти, які можуть сканувати системи на наявність вразливостей, вираховуючі паролі та підсаджувати у системи шкідливими програмами; DDoS-атаки – передбачають направлення великих обсягів фальшивого трафіку до комп'ютерної системи доти, доки обсяг трафіку не переповнить її, позбавивши доступу звичайних користувачів; шкідливе програмне забезпечення – програмне забезпечення, створене для допомоги чи проведення кібератак або заподіяння шкоди комп'ютерним системам. Зазвичай воно здатне поширюватись і заражати додаткові комп'ютерні системи.

З розвитком цифровізації масштаби кіберзагроз зростатимуть пропорційно збільшенню набору циркулярних продуктів і послуг, у яких застосовуються інформаційні технології, та кількості їх споживачів. Беручі до уваги це твердження, забезпечення кібербезпеки є надважливим завданням для публічного та приватного секторів, а впровадження адекватних заходів протидії подібним загрозам стають важливим напрямком публічної політики.

Якщо підприємці, що намагаються здійснити перехід на циркулярні рейки розвитку та застосовують при цьому цифрові інновації не роблять кроків із захисту цифрових активів бізнесу, вони безперечно ризикують.

Існує безліч інструментів, які можуть захистити від переважної більшості потенційних кібер атак.

Інструменти для пароля [5]: паролі є однією з найбільших точок вразливості у бізнесі. Вибір надійних паролів, ефективне управління ними та їх зміна часто є одними з найкращих способів запобігти будь-якій кіберзлочинності.

VPN [5]: віртуальна приватна мережа (VPN), яка може шифрувати весь мережний трафік. Єдина вразливість в мережі – це все, що потрібно для того, щоб зловмисник міг отримати доступ до всіх даних. Рішення забезпечує безперервний моніторинг локальних та віддалених мережевих пристроїв, хмарних середовищ незалежно від типу підключення: дротове, бездротове, VPN. Дуже важливою з огляду на це є наявність програми шифрування. Шифрування забезпечує безпеку даних, перетворюючи інформацію на комп'ютері на коди, що не читаються.

Антивірусна програма [6]: антивірусне програмне забезпечення не є надійною ставкою для захисту від хакерів, але воно триматиме в курсі, якщо комп'ютер заражений шкідливими програмами, і сканує вкладення електронної пошти, щоб переконатися, що вони не є шкідливими. Хороша та надійна антивірусна програма – обов'язковий елемент будь-якої системи кібербезпеки. Вона виявляє та видаляє віруси та шкідливі програми.

Брандмауер [7]: брандмауер контролює вхідний та вихідний трафік, відфільтровує певні загрози і навіть блокує деякі сайти в цілому. Брандмауер не захистить від усіх загроз в Інтернеті, але це додатковий рівень страхування, від якого не варто відмовлятися. Брандмауер блокує чи утримує віруси від проникнення у мережу, тоді як антивірус націлюється на програмне забезпечення, яке вже уражене вірусом. Інакше кажучи, вони добре працюють разом. Установка брандмауера допомагає захистити мережевий трафік малого бізнесу як вхідний, так і вихідний. Це може завадити хакерам атакувати мережу, заблокувавши певні вебсайти. Його також можна налаштувати так, щоб обмежити відправлення службових даних та конфіденційних електронних листів із мережі вашої компанії.

Найкраще обладнання [6]: старі комп'ютери, сервери та інші апаратні засоби можуть бути менш дорогими, але створюють набагато серйозніші ризики для безпеки. Вони, як правило, використовують більш старе програмне забезпечення і мають дірки в галузі безпеки, які відомі та експлуатуються протягом багатьох років. Тому експерти пропонують оновлювати обладнання регулярно, кожні кілька років.

Найкраще програмне забезпечення [8]: фахівці пропонують також звернути пильну увагу на те, яке програмне забезпечення та програми використовуються для таких завдань, як зберігання даних, зв'язок та управління проєктами. Кожна окрема платформа має свої сильні та слабкі сторони, тому потрібно обирати постачальників, до яких є довіра, із довгою історією захисту даних клієнтів.

Ігнорування підозрілих електронних листів та повідомлень [6]: через фішингові електронні листи хакер намагається отримати особисті та фінансові дані. Для більшої безпеки необхідно змінювати пароль електронної пошти кожні 60–90 днів. Крім того, важливо не використовувати один і той ж пароля скрізь.

Створення резервних копій даних [7]: потрібно або вручну створювати резервні копії всіх даних на зовнішньому жорсткому диску або хмарі, або просто запланувати автоматичне резервне копіювання, щоб забезпечити безпечне зберігання інформації. Таким чином, навіть якщо системи будуть скомпрометовані, інформація, як і раніше, буде в безпеці.

Освіта [9]: експерти пропонують інвестувати кошти на навчання та поінформованість співробітників. Більшість хаків пояснюються людськими помилками, тому більш освічені співробітники зможуть їх запобігти. Необхідно виділяти час кожного місяця для перевірки оновлень, і нагадування співробітникам про важливість звичок, таких як регулярна зміна паролів та уникнення підозрілих посилань.

Висновки

Після проведення дослідження можна зазначити, що впровадження економіки замкнутого циклу може призвести до поліпшення екологічної ситуації у світі, оскільки така модель орієнтована на більш раціональне використання обмежених природних ресурсів. Важливо врахувати, що такий перехід передбачає трансформацію природних процесів виробництва та споживання. Для підтримки цих ідей можуть бути використані цифрові технології. Розвиток яких, у свою чергу, неможливий без впровадження кібербезпеки, як на загально національному рівні, так і на рівні окремих суб'єктів господарювання. Усвідомлення і представниками влади і представниками бізнес середовища того факту, що кібер загрози та їх наслідки є дуже небезпечними є вкрай необхідним для створення відповідного цифрового середовища, яке стане основою подальших циркулярних трансформацій в нашій країні. Результати проведеного дослідження свідчать, що існує тісний зв'язок між рівнями кібербезпеки та цифрового розвитку: підвищення першої неминуче веде до прискорення другого і, як наслідок, досягнення сталого розвитку. Тому кібербезпека повинна посісти чільне місце у загальній візії розвитку нашої країни та окремо взятих компаній.

Список використаної літератури

1. Wilts H. The digital circular economy: can the digital transformation pave the way for resource-efficient materials cycles? In Brief: Sustainability Impulses from Wuppertal 04/2017 / H. Wilts, H. Berg, Wuppertal Institut. Wuppertal Institut. 2017. URL: https://wupperinst.org/fa/redaktion/downloads/publications/In_Brief_20174_en.pdf (дата обращения 20.01.2024).

2. Moşteanu N., Faccia A., Cavaliere L. Digitalization and Green Economy – changes of business perspectives. ICCBDC '20: Proceedings of the 4th International Conference on Cloud and Big Data Computing. August 2020. P. 108–112.

3. Green and digital transition: More resilience and sustainable jobs for the EU. 2022.

4. Семеног А.Ю. Екосистеми цифрових платформ як фактор трансформації бізнесу в умовах цифрової економіки. Вісник КНУТД. 2019. № 4 (137). С. 39-50.

5. Що таке кібербезпека? Заходи забезпечення кібербезпеки. Навчальний центр з підготовки IT спеціалістів. DAN.IT. 2023. URL: https://dan-it.com.ua/uk/blog/chto-takoe-kiberbezopasnost-mery-obespechenija-kiberbezopasnosti/ (дата звернення 20.01.2024).

6. Розвиток ринку кібербезпеки: інструменти і спільнодія. Громадський простір. URL: https://www.prostir.ua/?news=rozvytok-rynku-kiberbezpeky-instrumenty-i-spilnodiya-vidbuvsya-praktychnyj-dialoh-seminar-v-mezhah-prohramy-dialoh-pro-kiberbezpeku (дата звернення 24.01.2024).

7. Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія. / С. Ф. Гончар. Київ, 2019. 175 с.

8. Грановський М.В. Державна політика у сфері запобігання та протидії кібернетичним загрозам – досвід Республіки Польща / М. В. Грановський. Теорія та практика державного управління. 2019. Вип. 4. С. 212–220.

9. Грабар І.Г. Безпекова синергетика: кібернетичний та інформаційний аспекти : монографія. / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька. Житомир, 2019. 279 с.

References

1. Wilts H. (2017). The digital circular economy: can the digital transformation pave the way for resource-efficient materials cycles? In Brief: Sustainability Impulses from Wuppertal / H. Wilts, H. Berg, Wuppertal Institut. Wuppertal Institut. URL: https://wupperinst.org/fa/redaktion/downloads/publications/In_Brief_20174_en.pdf (accessed 20.01.2024).

2. Moşteanu N., Faccia A., Cavaliere L. (2020). Digitalization and Green Economy – changes of business perspectives. ICCBDC '20: Proceedings of the 4th International Conference on Cloud and Big Data Computing. (August 2020). pp. 108-112.

3. Green and digital transition: More resilience and sustainable jobs for the EU. (2022). Available at: https://www.openaccessgovernment.org/digital-transiti on-sustainable-jobs-eu/92904 (accessed 24.01.2024).

4. Semenoh A. Yu. (2019). Ekosystemy tsyfrovykh platform yak faktor transformatsii biznesu v umovakh tsyfrovoi ekonomiky. [Ecosystems of digital platforms as a factor of business transformation in the conditions of the digital economy] *Visnyk KNUTD*. no. 4 (137). pp. 39-50.

5. Shcho take kiberbezpeka? Zakhody zabezpechennia kiberbezpeky. (2023). [What is cyber security? Cyber security measures]. Navchalnyi tsentr z pidhotovky IT spetsialistiv. DAN.IT. URL: https://dan-it.com.ua/uk/blog/chto-takoe-kiberbezopasnost-mery-obespechenija-kiberbezopasnosti/(accessed 20.01.2024).

6. Rozvytok rynku kiberbezpeky: instrumenty i spilnodiia. (2023). Hromadskyi prostir. [Development of the cyber security market: tools and cooperation]. Hromadskyi prostir. URL: https://www.prostir.ua/?news=rozvytok-rynku-kiberbezpeky-instrumenty-i-spilnodiya-vidbuvsya-praktychnyj-dialoh-seminar-v-mezhah-prohramy-dialoh-pro-kiberbezpeku(accessed 24.01.2024).

7. Honchar, S.F. (2019). Otsiniuvannia ryzykiv kiberbezpeky informatsiinykh system obiektiv krytychnoi infrastruktury. [Assessment of cyber security risks of information systems of critical infrastructure objects] monohrafiia. / S. F. Honchar. Kyiv, 175 p.

8. Hranovskyi, M.V. (2019). Derzhavna polityka u sferi zapobihannia ta protydii kibernetychnym zahrozam – dosvid Respubliky Polshcha. [State policy in the field of prevention and countermeasures against cyber threats – the experience of the Republic of Poland]. Teoriia ta praktyka derzhavnoho upravlinnia, Issue 4, 212–220 pp.

9. Hrabar, I.H., Hryshchuk, R.V.,& Molodetska, K.V. (2019). Bezpekova synerhetyka: kibernetychnyi ta informatsiinyi aspekty. [Security synergy: cybernetic and informational aspects]. monohrafiia. / I. H. Hrabar, R. V. Hryshchuk, K. V. Molodetska. Zhytomyr, 279 p.