ISSN 2786-5827
Електронне наукове видання
НАУКОВИЙ ВІСНИК МІЖНАРОДНОЇ АСОЦІАЦІЇ НАУКОВЦІВ.
Серія: економіка, управління, безпека, технології
SCIENTIFIC BULLETIN OF INTERNATIONAL ASSOCIATION OF SCIENTISTS
Series: Economy, Management, Security, Technology
Том 2, № 1, 2023 **Volume 2, Issue 1, 2023** www.man.org.ua
Наказом МОН України від 10.10.2022 р. №894 видання включено до **категорії «Б»** за спеціальностями:
051 – економіка; 072 – фінанси, банківська справа та страхування; 073 – менеджмент;
076 – підприємництво, торгівля та біржова діяльність; 292 – міжнародні економічні відносини
DOI: 10.56197/2786-5827/2023-2-1-3
УДК 330:004

Кушніренко Оксана Миколаївна,
доктор економічних наук, доцент,
старший науковий співробітник відділу промислової політики,
Державна установа "Інститут економіки та прогнозування НАН України"
вул. Панаса Мирного, 26, м. Київ, 01000, Україна,
email: kushnksena@gmail.com,
ORCID ID: 0000-0002-3853-584X

Кушніренко Євгенія Володимирівна,
студентка факультету автоматизації і комп'ютерих систем,
Національний університет харчових технологій
вул. Володимирська, 68, м. Київ, 01000, Україна,
email: siel98765@gmail.com,
ORCID ID: 0000-0002-8197-3909

Kushnirenko Oksana,
Doctor of Economic Sciences, Senior Researcher,
Senior Researcher Department of Industrial Policy,
State Organization "Institute for Economics and Forecasting, NAS of Ukraine",
Panasa Myrnoho str., 26, Kyiv, Ukraine, 01011
email: kushnksena@gmail.com,
ORCID ID: 0000-0002-3853-584X

Kushnirenko Yevheniia,
Student of the Faculty of Automation and Computer Systems,
National University of Food Technology,
Volodymyrska street, 68, Kyiv, Ukraine, 01000,
e-mail: siel98765@gmail.com,
ORCID ID: 0000-0002-8197-3909

ДОСЯГНЕННЯ ЦИФРОВОЇ АВТОНОМІЇ УКРАЇНИ ЯК СТРАТЕГІЧНИЙ ВЕКТОР ІНТЕГРАЦІЇ З ЄС

UKRAINE'S DIGITAL AUTONOMY ACHIEVING AS A STRATEGIC VECTOR FOR EU INTEGRATION

Вступ. У статті обґрунтовано шляхи зміцнення цифрової й технологічної автономії України для інтеграції з ЄС в контексті трансформації стратегічних пріоритетів ЄС. Узагальнено етапи ухвалення стратегічних документів ЄС щодо цифрової автономії. Визначено складові європейської стратегічної автономії. Обгрунтовано значення цифрової й технологічної сфери в

зміцненні стійкості європейської економіки. Систематизовано концептуальні засади досягнення цифрової автономії в ЄС, ідентифіковано фактори, що обумовили необхідність впровадження даного пріоритету у стратегуванні економічного розвитку країн. Виокремлено основні компоненти цифрової автономії, а саме кібербезпека; підвищення обізнаності, розбудова потенціалу та набуття цифрових навичок; промислова політика, дослідження, інвестиції та зміцнення ланцюгів поставок; створення альянсів й сприяння міжнародній співпраці. Виявлено перешкоди цифрового розвитку в Україні в умовах військових дій. Визначено можливості подолання перешкод при формуванні цифрової автономії в Україні та окреслено шляхи консолідації з європейськими засадами формування цифрового простору.

Матеріали і методи. Досягнення мети статті здійснено за допомогою методів системного, критичного та наукового аналізу, методів наукового узагальнення, індукції та дедукції. Теоретико-методологічну базу дослідження склали інформаційні та статистичні матеріали міжнародних, європейських та українських інформаційних агенцій, нормативно-правові акти, зокрема регламенти ЄС, національні програми розвитку та стратегічні документи відновлення України, наукові праці зарубіжних та вітчизняних вчених.

Результати і обговорення. В статті аргументовано, що важливим чинником підвищення економічної й технологічної конкурентоспроможності, здатності захищати суспільні інтереси й визначати правила та стандарти в епоху цифрових технологій є досягнення стратегічної автономії. Це доводить досвід ЄС, який протягом тривалого періоду впроваджує підходи досягнення стратегічної автономії та цифрового суверенітету в широкому спектрі сфер: оборона, безпека та торгівля, а також у промисловій, цифровій, економічній, міграційній та фінансовій політиках на основі фундаментальних європейських цінностей – демократії, верховенства права, поваги до прав людини, стандартів європейської системи безпеки, а також створення умов для розвитку нових високотехнологічних виробництв та інноваційних екосистем з урахуванням Цілей сталого розвитку. В статті доведено, що Україні як кандидату на вступ до ЄС важливо інтегрувати стратегічні принципи європейського співтовариства, зокрема в частині цифрового переходу, до стратегічних документів відновлення економічного розвитку.

Висновки. Досягнення цифрової автономії в Україні в короткостроковому періоді залежить від розв’язання критично важливих проблем, обумовлених військовими діями, а саме відновлення зруйнованих телекомунікаційних потужностей, реконструкції інфраструктури для модернізації мереж зв'язку, доступу до мережі інтернет, створенні стимулів для інноваційного підприємницького розвитку, активізації спільних проектів щодо розробки і впровадження сучасних цифрових продуктів. Прискорення європейських інтеграційних процесів в сфері цифрової автономії для України залежить від ухвалення стратегічних документів, дорожніх карт, інших нормативних актів у сфері покращення кібербезпеки; підвищенні обізнаності та набутті цифрових навичок громадян; промислової, інноваційної та фінансової політики, сприянні дослідженням, інвестиціям та зміцненню ланцюгів поставок; сприянні міжнародній співпраці.

Ключові слова: стратегічна автономія, цифровізація, європейська інтеграція, обороноздатність, відновлення економіки, стійкість.

JEL Classification: F02, O38, O52

Introduction. The article substantiates directions for achieving digital and technological autonomy of the Ukraine for integration with the EU in the context digital transformation of the EU's strategic priorities. The authors systematized the phases of adoption the strategic documents on EU digital autonomy. The components of European strategic autonomy were identified. The importance of the digital and technological sphere in strengthening the sustainability of the European economy was substantiated. The conceptual foundations for achieving digital autonomy in the EU are the factors that have led to the need to implement this priority in the strategic development of countries were identified. The main components of digital autonomy are highlighted, namely cybersecurity; awareness raising, digital skills acquisition; industrial policy, research, investment and supply chain strengthening; building alliances and promoting international cooperation. The obstacles to digital development in Ukraine in the context of military operations were identified. Possibilities of overcoming the threats to the formation

of digital autonomy in Ukraine were identified and ways of consolidation with the European principles of digital space formation are outlined.

Materials and methods. The purpose of the article was achieved using the methods of systematic, critical and scientific analysis, methods of scientific generalization, induction and deduction. The theoretical and methodological basis of the study is formed by information and statistical materials of international, European and Ukrainian statistic agencies, regulations, in particular EU regulations, national development programs and strategic documents for the restoration of Ukraine, scientific works of foreign and domestic scholars.

Results and discussion. The authors defined that an important factor in enhancing economic and technological competitiveness, the ability to protect the public interest and define rules and standards in the digital age is the achievement of strategic autonomy. This is proved by the experience of the EU, which has been implementing approaches to achieving strategic autonomy and digital sovereignty in a wide range of areas: defense, security and trade, as well as in industrial, digital, economic, migration and financial policies based on fundamental European values –
democracy, the rule of law, respect for human rights and standards of the European security system, as well as creating conditions for the development of new high-tech industries and innovative ecosystems, taking into account the Sustainable Development Goals. The article proves that it is important for Ukraine, as a candidate for EU integration, to implement the strategic principles of the European community, in particular in terms of digital transition, into the strategic documents for the economic recovery.

Conclusions. Achieving digital autonomy in Ukraine in the short term depends on solving critical problems caused by the hostilities, namely, restoring destroyed telecommunications capacities, reconstructing infrastructure to modernize the communication network, access to the Internet, creating incentives for innovative entrepreneurial development, and intensifying joint projects to develop and implement modern digital products. Acceleration of European integration processes in the field of digital autonomy for Ukraine depends on the adoption of strategic documents, roadmaps, and other regulations in the field of improving cybersecurity; raising awareness and acquiring digital skills of citizens; industrial, innovation, and financial policies; promoting research, investment, and strengthening supply chains; and facilitating international cooperation.

Keywords: strategic autonomy, digitalization, European integration, defense capability, economic recovery, sustainability.

JEL Classification: F02, O38, O52

Вступ. Військова агресія росії виявила зростаючу актуальність питань, пов'язаних з безпекою та стійкістю соціально-економічного розвитку суспільства не тільки в Україні, а в усьому світі, а також важливість прийняття стратегічних управілнських рішень щодо реагування на існуючі та майбутні загрози для демократичних країн. Відповіддю демократичних країн світу, зокрема країн ЄС є посилення стратегічної автономії для забезпечення вищого ступеню європейського суверенітету та набуття нових функціональних ознак. Як зазначив Ж. Боррель, верховний представник ЄС у зовнішніх справах та політики безпеки, віце-президент Європейської Комісії: "Стратегічна автономія – це не чарівна паличка, а довгостроковий процес, спрямований на те, щоб європейці все більше брали на себе відповідальність. Стратегічна автономія не обмежується безпекою та обороною, а стосується широкого кола питань, включаючи торгівлю, фінанси та інвестиції економічного та технологічного характеру"[1]. Ця концепція містить значний потенціал для незалежності, самозабезпечення та стійкості в широкому спектрі сфер, таких як оборона, безпека та торгівля, а також у промисловій, цифровій, економічній, міграційній та фінансовій політиці.

Обгрунтуванню методичних та практичних аспектів формування стратегічних напрямів забезпечення стійкості економіки в умовах цифрового переходу посвячено праці багатьох

[1] Borrell J. Why European strategic autonomy matters. High Representative of the European Union for Foreign Affairs and Security Policy. The European External Action Service (EEAS). 2020. URL: https://www.eeas.europa.eu/eeas/why-european-strategic-autonomy-matters_en (дата звернення 02.02.2023 р.)

вітчизняних вчених. Системні узагальнення щодо характеру трансформації соціальної реальності під впливом дедалі більш широкого і проникливого застосування інформаційно-комунікаційних технологій, яка у своїй основі має ряд фундаментальних викликів, що формують глибинного змісту суперечність між людиною та її свободами і суспільством провів В. М. Геєць (Геєць, 2022). У працях А. А. Гриценка визначені шляхи забезпечення взаємопов'язаного і взаємодоповнюючого розвитку інформаційно-цифрових і соціально-економічних перетворень (Гриценко, 2021). В роботах Єгорова І. Ю., Никифорук О. І. та інших науковців Інституту економіки та прогнозування НАНУ досліджені методичні та практичні аспекти використання цифрових технологій для реалізації потенціалу України в різних сферах – енергетичній, транспортній тощо та виявлені наслідки для подальшої інтеграції України у світову економіку на якісно новій основі (Єгоров, 2020). Водночас розробка концептуальних підходів, принципів та механізмів досягнення цифрової автономії України, особливо в контексті імплементації європейських принципів при стратегуванні повоєнного відновлення залишаються недостатньо розробленими.

Більшість держав світу розглядають доступ до цифрових технологій як необхідність для забезпечення свого суверенітету як у фізичному, так і в цифровому просторі. Можливості впровадження й застосування цифрових інструментів і технологій вже давно стали ключовими засадами стратегічної конкуренції, а володіння новими технологіями формує майбутній глобальний порядок. Конкурентоспроможність і зростання економіки залежить від досягнення технологічного лідерства, що підтверджує досвід країн "Великої сімки" (Bakardjieva, 2020).

Для України зміцнення цифрової та технологічної спроможності в контексті досягнення стратегічної автономії має подвійне значення. Перш за все, це обумовлено ключовими стратегічними пріоритетами українського майбутнього – зміцнення національної безпеки та прискорення європейської інтеграції як головними векторами відновлення України[2]. Потужна підтримка України державами-членами ЄС у гуманітарній, науково-технічній, торгівельній, військовій та інших сферах доповнилася історичною подією – наданням Україні 23 червня 2022 року статусу країни-кандидата на вступ до ЄС, що має історичне значення як для охопленої війною України, так і для Європи. Адже, як зазначають фахівці Центру європейської політики: "Надання Україні статусу країни-кандидата в ЄС без умов є обов'язковим для того, щоб зробити ЄС більш релевантним і надійним глобальним гравцем. Це також моральний обов'язок Європи перед усіма українцями, які пролили сльози, кров і життя за свою європейську мрію"[3].

Стратегічну автономію в Європейському Союзі визнано стратегічним вектором розвитку як концепцію, яка спочатку застосовувалася у сфері зовнішньої політики та політики безпеки, а наразі стала актуальною для інших політик, таких як торгівля та фінансове регулювання. Отже, для України важливим є наближення соціально-економічних цілей до загальноєвропейських, що потребує удосконалення законодавства з врахуванням європейських принципів, а саме розвиток доступних публічних послуг для громадян та бізнесу, доступ до високошвидкісного інтернету, відновлення та розвиток цифрової інфраструктури, цифрових рішень та електронної ідентифікації, посилення кібербезпеки та стійкості цифрової інфраструктури, створення умов для розвитку нових високотехнологічних виробництв та інноваційних систем з урахуванням Цілей сталого розвитку До того ж посилення цифрової й технологічної стратегічної автономії в України матиме значний синергетичний ефект для зміцнення безпеки й прискорення відновлення промисловості. Війна в Україні підтверджує те, що навіть в умовах нападу значно переважаючого за потужністю та ресурсами агресора застосування цифрових технологій (штучного інтелекту, робототехніки, віртуальної та доповненої реальності) посилює обороноздатність країни, а протидія військовим загрозам залежить від спроможності держави забезпечити безпеку населення та цілісність території, де найбільшу роль відіграє потужний промисловий комплекс.

---

[2] Головні вектори відновлення України – національна безпека та європейська інтеграція. Міністерство з питань стратегічних галузей промисловості України. 2022. URL: https://mspu.gov.ua/news/premier-ministr-holovni-vektory-vidnovlennia-ukrainy-natsionalna-bezpeka-ta-ievropeiska-intehratsiia (дата звернення 02.02.2023 р.)

[3] EU candidate status for Ukraine is a geopolitical and moral imperative. European Policy Centre. 2022. URL: https://www.epc.eu/en/publications/EU-candidate-status-for-Ukraine-is-a-geopolitical-and-moral-imperative~497c80 (дата звернення 02.02.2023 р.)

Метою статті є оцінка рівня узгодженості та координації концептуальних підходів, принципів та механізмів досягнення цифрової й технологічної спроможності України відповідно європейських підходів, а також обґрунтування інструментів щодо формування цифрової автономії як важливого принципу у стратегуванні повоєнного відновлення України.

Матеріали і методи. Досягнення мети статті здійснено за допомогою методів системного, критичного та наукового аналізу, методів наукового узагальнення, індукції та дедукції. Теоретико-методологічну базу дослідження склали інформаційні та статистичні матеріали міжнародних, європейських та українських інформаційних агенцій, нормативно-правові акти, зокрема регламенти ЄС, національні програми розвитку та проекти планів відновлення України, наукові праці зарубіжних та вітчизняних вчених.

Результати і обговорення. Щоб подолати загрозливі виклики для розвитку демократичного суспільства, зміцнити спроможність ЄС захищати своїх громадян та інфраструктуру в часи невмотивованої агресії росії проти України, Європейська Комісія ухвалила програму Цифрового десятиліття з конкретними цілями та завданнями до 2030 року. Метою є підтримання дій Європейського Союзу щодо зменшення стратегічної залежності, просування європейських цінностей та формування середовища, в якому європейські компанії зможуть конкурувати на регіональному та глобальному рівнях. Це закладено в ухваленій Європейською комісією в травні 2020 року Концепції "відкритої стратегічної автономії", яка стала центральною частиною дій ЄС у внутрішньому та зовнішньому вимірах. Важливе значення даного підходу та його вирішальний плив на розвиток інших країн підтверджується так званим "брюссельським ефектом", тобто визначальним впливом європейської міжінституційної та багаторівневої політики, яка відповідає високим стандартам правової визначеності та є ефективним інструментом для спонукання інших держав до впровадження європейських засад і принципів. Іншими словами, брюссельський ефект проявляється як дифузія європейських принципів, правил та регламентів, які прямо чи опосередковано трансформують стратегічні вектори розвитку багатьох інших країн (Cervi, 2022).

Стратегічна автономія спочатку застосовувалася у сфері оборонної промисловості і тривалий час зводилася до питань оборони та безпеки. Європейська Рада застосувала цю концепцію в листопаді 2013 року у Спільній політиці безпеки та оборони[4]. Практичним втіленням концепції став Стратегічний компас ЄС, метою якого є "закріплення основ спільного бачення держав-членів ЄС щодо питань безпеки та оборони", а цілями – "введення в дію стратегічної автономії ЄС з тим, щоб покращити рівень його амбіцій і краще пов'язати його стратегічні та оперативні потреби, а також потреби в можливостях[5]".

Стратегічна автономія, цифровий суверенітет і кіберстійкість знаходяться в центрі суспільних дискусій не тільки в ЄС, а й в усьому світі. Так, аналітичний інструмент Google Trends показує стабільно високий (більше середнього, а у лютому 2022 року – максимальну кількість балів щодо популярності запиту в системі пошуку Google) рівень популярності запиту "Стратегічна автономія" протягом останніх п'яти років[6]. Стратегічна автономія в ЄС – це формування такого союзу, який більш спроможний діяти разом з партнерами, коли можливо, і самостійно, коли необхідно. У звіті "Впровадження Глобальної стратегії ЄС" підкреслюється необхідність поглибити роботу щодо збору та обміну даними, стратегічної культури, взаємосумісності, командування та контролю, оборонного співробітництва, кібербезпеки та доступу до комунікацій та мереж[7]. Райан Е. обгрунтував вплив європейської стратегічної автономії на посилення енергетичної безпеки (Ryon, 2020). Іншими словами, поняття

---

[4] The Common Security and Defence Policy. The European External Action Service (EEAS). 12.08.2021. URL: https://www.eeas.europa.eu/eeas/common-security-and-defence-policy_en (дата звернення 02.02.2023 р.)

[5] Europe's Digital Decade: digital targets for 2030. The European Commission. 02.2023. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en (дата звернення 02.02.2023 р.)

[6] European strategic autonomy. Google. Trends. 15.02.2022. https://trends.google.com/trends/explore?date=today%205-y&q=European%20strategic %20autonomy, Digital%20autonomy (дата звернення 02.02.2023 р.)

[7] The European Union's global strategy three years on, looking forward. Strategy. The European External Action Service. 2019. URL: https://www.eeas.europa.eu/%20sites/default/files/eu_global_strategy_2019.pdf (дата звернення 02.02.2023 р.)

стратегічної автономії, з одного боку, вказує на імперативність досягнення стратегічної автономії, а з іншого – окреслює коло сфер, у яких ЄС наближається до неї.

Факторами, які визначають актуальність досягнення стратегічної автономії в ЄС, а також країн, що спрямовують свої зусилля на зближення з ЄС, є:

– зміна впливу геополітичних центрів, тенденціями секторального відокремлення та фрагментованого регулювання, що характеризується зростанням конкуренції, протистояннями ключових економічних гравців (США, Китаю, ЄС). Адже, за словами Ж. Борреля: "Важко назвати себе політичним союзом, здатним діяти як глобальний гравець і як геополітична комісія, не будучи автономним[1]". У цій перспективі стратегічна автономія є процесом політичного виживання;

– "Чорні лебеді сучасності" – пандемія COVID-19 та повномасштабна війна в Україні посилюють значення стратегічної автономії для подолання викликів завдяки обєднанню зусиль та застосуванню цифрових технологій. Вплив пандемії коронавірусу – зрив поставок та пошук замінників, скорочення довжини ланцюгів доданої вартості, порушення операційної діяльності, дефіцит оборотних коштів, зниження прибутковості, погіршення фінансової стійкості та платоспроможності, зростання ймовірності банкрутства, особливо вдарив по секторах машинобудування, зокрема виробництва електроніки, обчислювальної техніки, текстильній, хімічній галузях. З початком невмотивованої агресії росії проявився потужний вплив цифрових технологій, коли цифрові технології широко використовувалися як зброя для дезінформації, інформаційно-психологічних операцій, хакерства та руйнування стратегічної інфраструктури (Дейнеко, 2022);

– зростання впливу таких інструментів як наука, технології, торгівля, дані, інвестиції на конкурентоспроможність. Конкурентоспроможність промислових компаній сьогодні базується на двох основних факторах: зростанні ефективності всіх бізнес-процесів, оптимізації витрат та впровадженні цифрових технологій у виробничий цикл, вертикальною і горизонтальною інтеграцію процесів й зміну ролі людини як учасника виробничого процесу. Розвиток цифрової економіки та Індустрії 4.0 характеризується інтеграцією різних областей знань, галузей промисловості, сфер людського життя. Мова йде не про локальне застосування тих чи інших технологій, а про їх злиття, об'єднання в мережу, що тягне за собою глибокі структурні трансформації, які проявляються на глобальному рівні практично у всіх країнах, галузях і в суспільстві в цілому;

– зростання зв'язку та залежності від цифрових послуг і ключових компонентів для розвитку цифрових технологій, які вважаються критичними. Прикладом є виробництво напівпровідників й мікросхем для забезпечення базових потреб цифровізації, що є частиною глобальних ланцюгів доданої вартості і включає високий ступінь розподілу праці, значні капіталовкладення, спеціальні знання та тривалий час виробництва.

В цих умовах пріоритетами Єврокомісії визнано необхідність просування до стратегічної автономії та досягнення цифрового суверенітету. Президент Європейської комісії Урсула фон дер Ляєн наголосила про важливість цифрового суверенітету у зв'язку з підключенням та цифровою інфраструктурою у своїй промові ще у 2020 році[8], а роком пізніше наголошувалося про технологічний суверенітет[9], що стало передумовою ухвалення Європейського закону "Про мікросхеми", за допомогою якого ЄС прагне відновити 20% частку світового виробництва мікросхем до 2030 року. Німеччина зробила цифровий суверенітет одним із своїх чотирьох пріоритетів у цифровому секторі під час свого головування в ЄС у другій половині 2020 року[10]. В лютому 2021 року Шарль Мішель, президент Ради ЄС заявила: "Немає стратегічної автономії

---

[8] Leyen U. The six policy priorities of the von der Leyen Commission. State of play as the Commission approaches mid-term. European Parliamentary Research Service. March 2022. URL: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/729351/EPRS_IDA(2022)729351_EN.pdf. (дата звернення 02.02.2023 р.)

[9] Leyen U. State of the Union Addresses by President Ursula von der Leyen at the European Parliament Plenary. Speech15. September 2021. Strasbourg. URL: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701 (дата звернення 02.02.2023 р.)

[10] Independent, inclusive and innovative: Four goals of the German Presidency for the digital sector. 24 October 2020. Germany's Presidency of the Council of the EU. URL: https://www.eu2020.de/eu2020-en/news/article/digitalziele-eu2020/2405548 (дата звернення 02.02.2023 р.)

без цифрового суверенітету”[11]. Стратегічна автономія передбачає співпрацю країн-партнерів на принципах взаємодоповнюваності, що вимагає додаткових зусиль з виконання зобов’язань, взятих на себе державами-членами. Місце цифрової автономії в системі стретегічної автономії ЄС показано в табл. 1.

Таблиця 1

Характеристика основних складових поняття стратегічної автономії

Види автономії	Характеристика	Майбутні тренди розвитку
Політична	Можливість приймати рішення щодо політики безпеки	Зміцнення позицій у сфері захисту демократичних прав і цінностей
Операційна	Здатність самостійно планувати та проводити цивільні та/або військові дії	Зміцнення стратегічних альянсів з країнами-партнерами, посилення згуртованості для спільних дій у питаннях оборони та безпеки
Індустріальна/ економічна	Можливості досягнення операційної автономності	Розвиток технологічних можливостей ЄС через інновації та промислову конкурентоспроможність
Цифрова	Здатність безпечно взаємодіти в цифровому світі за допомогою захисних механізмів, дієвих інструментів і співпраці	Досягнення цифрового суверенітету ЄС залежить від масштабування стартапів у сприятливих для інновацій екосистемах і розробки технічних правил таким чином, щоб сприяти розвитку інновацій відповідно до цінностей і стандартів ЄС
Екологічна	Здатність прискорити зелений перехід шляхом модернізації промисловості та розвитку технологій відновлюваної енергії та циркулярної економіки	Основою для екологічно орієнтованих інновацій та циркулярних екосистем є обов’язкові зобов’язання щодо обміну даними для постачальників, виробників і операторів шляхом скоординованої розробки Європейського цифрового паспорта та регулювання даних для стандартизованого збору пов’язаних із продуктом екологічних даних
Торгівельна	Запобігання перебоям у постачанні та забезпечити стійкість ланцюгів доданої вартості	Зміцнення європейських виробничих потужностей та вдосконалення європейської торговельної політики для забезпечення доступу до основних ресурсів, коли зовнішні ринки закриті

Джерело: складено за даними Joint Research Centre (Cagnin, 2021)

Оскільки цифровізація відіграє все більшу роль у геополітичному вимірі щодо забезпечення безпеки й досягнення економічних інтересів, зміцнення цифрової автономії стає ключовим компонентом стратегічної автономії ЄС[12]. Ваховуючи трансформаційні особливості цифрових технологій, Т. Гаєвський ставить їх на центральне місце в концепції стратегічної автономії (Gajewski, 2022), а європейські дослідники з Науково-дослідного інституту економіки промисловості ЄС обгрунтовують значення цифрової автономії у формуванні нового європейського порядку перекалібрування своєї політики та дій у різних сферах (Bakardjieva, 2020). Узагальнюючи різні нормативні вимоги до цифрової автономії, можна зазначити, що

[11] Charles M. Digital sovereignty is central to European strategic autonomy. Speech by President Charles Michel at “Masters of digital 2021” online event. 03.02.2021. URL: https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/ (дата звернення 02.02.2023 р.)

[12] Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence. The European Political Strategy Centre. 19.02.2020. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273 (дата звернення 02.02.2023 р.)

цифрова автономія означає спроможність діяти незалежно в цифровому світі за допомогою захисних механізмів, дієвих інструментів і співпраці з ключовими учасниками, одночасно сприяючи цифровим інноваціям та доступу до цифрових технологій. Дослідники Берлінського центру соціальних наук Ю. Поле та Т. Тіль довели, що сьогодні цю концепцію застосовують більше як дискурсивну практику в політиці та державному управлінні, ніж як правову чи організаційну концепцію (Pohle, 2020).

Послідовність реалізації європейських принципів цифрової автономії представлена низкою нормативно-правових документів, хронологію ухвалення яких показано в табл. 2.

Таким чином, процес досягнення стратегічної цифрової автономії триває по теперішній час, хоч в ЄС уже розроблені численні нормативні та регулятивні рамки у сферах захисту даних, етичних і орієнтованих на людину підходів до технологій, зобов'язання онлайн-платформ або боротьби з дезінформацією. Однак одне лиш регулювання не може гарантувати європейську технологічну незалежність, тому і в подальшому зусилля спрямовуватимуться на зменшення залежності та забезпечення безпеки поставок, а також на розширення досліджень, розвиток потенціалу та спрямування інвестицій у ключові стратегічні сфери для інновацій, цифровізації та безпеки. Європейські дослідники Ж. Погорел, А. Несторас, Ф. Каппеллетті обґрунтували такі важелі, що впливають на досягнення стратегічної цифової автономії: наука та дослідження; навчання, утримання та залучення талантів; гармонізовані правила та оновлена конкурентна політика для економічно інтегрованої Європи; розвиток конкурентних екосистем, об'єднання підприємців і стартапів, налагодження партнерства з дослідницькими центрами (Pogorel, 2022). Практичним інструментом реалізації цифрової автономії в ЄС є Цифровий компас 2030, який містить набір конкретних цифрових цілей у сферах навичок, інфраструктури, бізнесу та державних послуг (рис. 1).

Рис. 1. Елементи програми Цифрового десятиліття ЄС

Джерело: складено за даними: The European Commission[13]

[13] Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030. 09.03.2021. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_983 (дата звернення 02.02.2023 р.)

Таблиця 2

Хронологія ухвалення стратегічних документів ЄС щодо цифрової автономії

Дата	Подія / ухвалення документу	Короткий опис
19.02.2020	Порядок денний для формування цифрового майбутнього Європи, Стратегії даних та Білої книги штучного інтелекту	Нормативно-правова основа для розвитку цифрових технологій на основі європейських принципів: розвиток надійних технологій для сприяння демократичному суспільству та стійкій економіці для боротьби зі зміною клімату й досягнення екологічного переходу.
10.03.2020	Нова індустріальна стратегія	Оновлення європейської промислової політики на основі подвійного переходу до кліматичної нейтральності та цифрового лідерства. Пакет ініціатив встановлює низку заходів для підтримки всіх гравців європейської промисловості, включаючи великі та малі компанії, інноваційні стартапи, дослідницькі центри, постачальників послуг і соціального партнерства.
24.09.2020	Стратегія цифрового фінансування та законодавчі пропозиції щодо криптоактивів і цифрової стійкості	Ухвалення набору правил щодо цифрових фінансів і роздрібних платежів, а також законодавчих пропозицій щодо криптоактивів; управління інноваціями у фінансовому секторі ЄС, захист інвесторів, боротьба з відмиванням грошей і кіберзлочинністю з метою зростання конкурентоспроможності ЄС та ухвалення глобальних стандартів у сфері фінансових послуг[14].
01.12.2020	Правила податкової прозорості на цифрових платформах	Узгоджена пропозиція щодо адміністративної співпраці й автоматичного обміну державами-членами інформацією про доходи, отримані продавцями на цифрових платформах. Це дозволяє національним органам влади визначати ситуації, коли податки повинні бути сплачені, зменшує адміністративне навантаження на платформи, які співпрацюють з різними національними вимогами звітності[15].
15.12.2020	Закон про цифрові послуги; Закон про цифрові ринки	Реформа цифрового простору, комплексний набір нових правил для цифрових послуг, включаючи соціальні медіа, онлайн-ринки та інші онлайн-платформи, які діють у ЄС[16].
16.12.2020	Стратегія кібербезпеки	Захист відкритого Інтернету для забезпечення безпеки та основних прав людини. Містить пропозиції щодо регуляторних, інвестиційних і політичних ініціатив у трьох сферах діяльності ЄС: стійкість, технологічний суверенітет і лідерство (правила безпеки мережевих та інформаційних систем в ЄС); розбудова оперативного потенціалу для запобігання, стримування та реагування на зловмисну кібердіяльність; посилення співпраці, сприяння міжнародній безпеці та стабільності в кіберпросторі[17].
09.03.2021	Курс на розвиток цифрової Європи до 2030 року	Бачення, цілі та шляхи до 2030 року: цифрові навички, безпечна цифрова інфраструктура, цифрова трансформація бізнесу[18].
03.06.2021	Регламент № 910/2014 щодо електронної ідентифікації та	Впровадження Європейської цифрової ідентифікації громадянам, резидентам і підприємствам в ЄС (eIDAS)[19].

[14] Digital Finance Package: Commission sets out new, ambitious approach to encourage responsible innovation to benefit consumers and businesses. 24.09.2020. The European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1684 (дата звернення 02.02.2023 р.)

[15] Fair Taxation: Member States agree on new tax transparency rules on digital platforms 01.12.2020. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2253 (дата звернення 02.02.2023 р.)

[16] The Digital Markets Act: ensuring fair and open digital markets. European Commission. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en (дата звернення 02.02.2023 р.)

[17] New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. 16.12.2020. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391 (дата звернення 02.02.2023 р.)

[18] Europe fit for the Digital Age: Commission proposes new rules for digital platforms. 15.12.2020. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347 (дата звернення 02.02.2023 р.)

[19] Commission proposes a trusted and secure Digital Identity for all Europeans. 03.06.2021. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663 (дата звернення 02.02.2023 р.)

	довірчих послуг для транзакцій на внутрішньому ринку	
26.01.2022	Декларація про європейські цифрові права та принципи	Закріплення основних цифрових прав людини, зокрема поставлення інтересів людини у центр цифрової трансформації; підтримка солідарності та інклюзивності; забезпечення свободи вибору онлайн; сприяння участі в цифровому публічному просторі; сприяння стійкості цифрового майбутнього[20].
08.02.2022	Європейський закон про мікросхеми	Вирішення проблеми дефіциту напівпровідників шляхом мобілізації 43 млрд євро державних і приватних інвестицій; підготовки, передбачення та швидкого реагування на майбутні збої в ланцюзі поставок разом з міжнародними партнерами[21].
23.02.2022	Закон про дані	Стимулювання конкурентного ринку даних, відкриття можливостей для інновацій, забезпечення доступності даних у цифровому середовищі, що призведе до появи інноваційних послуг більш конкурентоспроможних цін на післяпродажне обслуговування та ремонт підключених об'єктів до 2030 року[22].
11.05.2022	Європейська стратегія “Кращий Інтернет для дітей”	Бачення цифрового десятиліття для дітей та молоді, яке базується на принципах безпечного цифрового досвіду, захисту дітей від шкідливого та незаконного онлайн-контенту; розширення цифрових можливостей для здобуття навичок; повага до дітей, надання їм права голосу в цифровому середовищі для сприяння інноваційному та творчому безпечному цифровому досвіду[23].
15.09.2022	Закон про кіберстійкість	Загальноєвропейське законодавство, яке запроваджує обов’язкові вимоги до кібербезпеки для продуктів із цифровими елементами протягом усього життєвого циклу[24].
14.12.2022	Спільна заява президента фон дер Ляєн і прем’єр-міністра Лі щодо цифрового партнерства ЄС-Сінгапур	Співпаця з усього спектру цифрових питань, включаючи сприяння торгівлі, довірені потоки даних та інновації даних, цифрову довіру, стандарти, цифрові навички для працівників, а також цифрову трансформацію бізнесу та державних послуг[25]
06.02.2023	Створення Ради з торгівлі та технологій ЄС-Індія	Формування спільних робочих груп з питань: 1. Стратегічні технології, цифрове управління та цифрові зв’язки (спільні проекти в сфері штучного інтелекту, 5G/6G, високопродуктивні та квантові обчислення, напівпровідники, хмарні системи, кібербезпека, цифрові навички. 2. Зелені та чисті енергетичні технології: інвестиції та стандарти, дослідження та інновації в сферах енергетики, циркулярної економіки, управління відходами, пластику і сміття в океані. 3. Торгівля, інвестиції та стійкі ланцюжки створення вартості (стійкість ланцюгів постачання та доступу до критичних компонентів, енергії та сировини; спрощення торговельних бар’єрів; просування міжнародних стандартів.

Джерело: складено за даними: The European Commission[26]

[20] European Digital Rights and Principles. European Commission. URL: https://digital-strategy.ec.europa.eu/en/policies/digital-principles (дата звереннння 02.02.2023 р.)
[21] European Chips Act. European Commission.URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en(дата звереннння 02.02.2023 р.)
[22] Data Act: Commission proposes measures for a fair and innovative data economy. 23.02.2022. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113 (дата звереннння 02.02.2023 р.)
[23] New EU strategy to protect and empower children in the online world. 11.05.2022. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2825 (дата звереннння 02.02.2023 р.)
[24] State of the Union: New EU cybersecurity rules ensure more secure hardware and software products. 15.09.2022. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5374 (дата звереннння 02.02.2023 р.)
[25] Joint statement by President von der Leyen and Prime Minister Lee on the EU-Singapore Digital Partnership 14.12.2022. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_7743 (дата звереннння 02.02.2023 р.)
[26] Making Europe's businesses future-ready: A new Industrial Strategy for a globally competitive, green and digital Europe. The European Commission. 10.03.2020. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_416. (дата звереннння 02.02.2023 р.)

До компонентів, які формують цифрову стратегічну автономію можна віднести:

1. Кібербезпеку;
2. Підвищення обізнаності, розбудова потенціалу та набуття цифрових навичок;
3. Набуття лідерства у регулюванні;
4. Промислову політику, дослідження, інвестиції та зміцнення ланцюгів поставок;
5. Створення альянсів і сприяння міжнародній співпраці.

Для з'ясування, наскільки Україна успішно вирішує внутрішні проблеми готовності до цифрової автономії та виявити "вузькі" місця для подолання технологічних викликів необхідно охарактеризувати вищеназвані компоненти більше детально та порівняти українські досягнення з європейськими.

1. Кібербезпека.

Зміцнення кібезбезпеки є одним з ключових завдань сьогодення, адже кібрезлочини, тобто руйнування інформаційних мереж, викрадення даних, розповсюдження шкідливого програмного забезпечення, крадіжка номерів кредитних карт і банківських рахунків, злом паролів, порушення авторських прав призводять до катастрофічних наслідків. Війна росії проти України довела критично важливе значення забезпечення кіберстійкості. Ще до війни кібератаки викликали значні збитки для приватного й державного секторів (наприклад, кібератака на німецький Бундестаг у 2021 році). Атаки ворожих програм відбувалися кожні 11 секунд у 2021 році, а до 2031 року очікується, що вони прискориться до 2 секунд, що призведе до втрати близько 10,5 трлн дол. США щороку. Трагічним прикладом є кіберзлочини 22.06.2021 року проти найбільшого у світі виробника нафти "Saudi Aramco", коли кібер-злочинці розмістили у даркнеті 1терабайт інсайдерських даних та вимагали від компанії 50 млн дол. США викупу, що викликало перебої на глобальному нафтовому ринку. Також кібератаки портової інфраструктури Бельгії, Німеччини та Нідерландів 02.03.2022 року порушили роботу нафтових терміналів, не даючи танкерам доставляти енергоносії. Це наочно показує, що одна держава може загрожувати безпеці іншої держави, не перетинаючи її кордонів. Кіберзлочинці завдають значних збитків, що сягають 1–2% ВВП розвинутих країн[29] і ці збитки щорічно зростають (рис. 2). За прогнозами європейського статистичного бюро до 2026 року річні витрати на кіберзлочинність у всьому світі можуть перевищити 20 трлн дол. США, збільшившись майже на 150 % порівняно з 2022 роком.

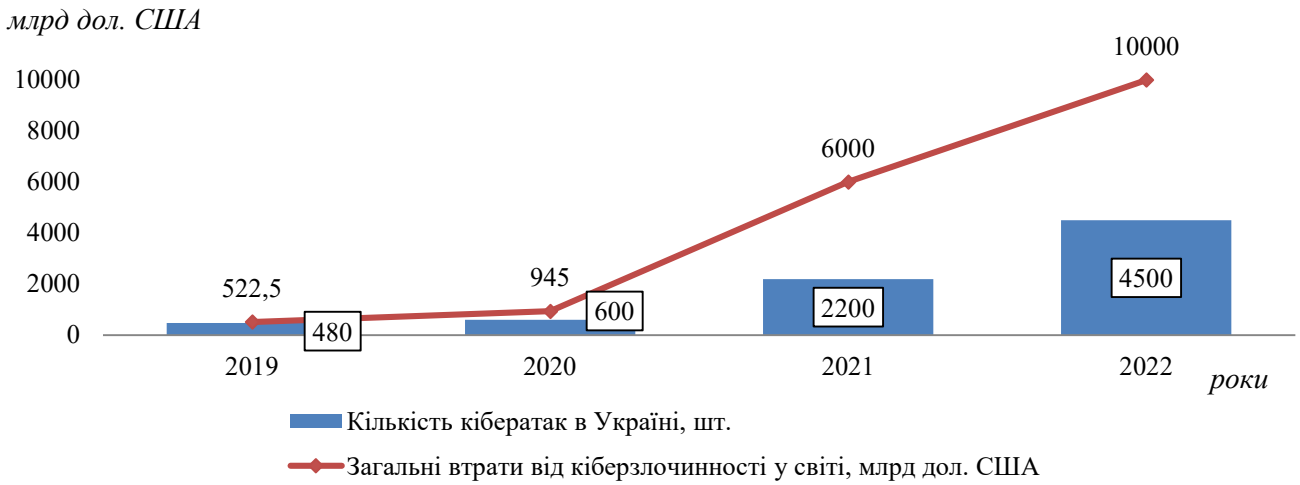

Рис. 2. Динаміка кількості кібератак в Україні та втрати від кіберзлочинності в світі, млрд дол. США

Джерело: складено за даними Європейської служби статистики [27]

[27] Estimated cost of cybercrime worldwide from 2016 to 2027. Statista. 02.12.2022. URL: https://www.statista.com/statistics/1280009/cost-cybercrime-worldwide (дата звернення 02.02.2023 р.)

Агресія росії проти України провокує зростання кібезлочинності та посилення інформаційних провокацій, зростання кількості кібератак на критично важливу інфраструктуру, таку як енергетика, охорона здоров'я та фінанси, які стають все більше цифровими і одночасно, вразливими. Особливо шкідливими є зростаючі можливості зловмисників, які використовують кібератаки проти ланцюгів поставок та атаки на об'єкти критичної інфраструктури. Гібридний підхід росії, який поєднує фізичні та кібератаки, продемонстрував, що збій у роботі основних послуг є реальною загрозою для не тільки для України, а і для інших країн ЄС. Наприклад, атака на провайдера супутникового зв'язку лише за годину до атаки росії на Україну вплинула на інтернет-сервіси та вітрові електростанції по всій Європі.

В ЄС здійснені заходи протидії для захисту критичної інфраструктури. Директива про стійкість критично важливих об'єктів разом із Директивою про безпеку мережевих та інформаційних систем безпосередньо відповідають на цей виклик. Однак масштаб загроз, що швидко зростають, вимагають прискореного впровадження оновленої правової бази. У 2022 році Рада ЄС ухвалила рекомендації щодо активізації зусиль, спрямованих на захист критичної інфраструктури та сприяння співпраці. Зокрема, подальша політика ЄС щодо кіберзахисту має на меті підвищити спроможності кіберзахисту і взаємодію між військовими та цивільними кіберспільнотами. Підключення критичної інфраструктури забезпечуватиме інфраструктура стійкості, взаємозв'язку та безпеки за допомогою супутника Iris², космічної безпечної системи підключення, яка буде функціонувати на орбіті до 2024 року[28]. Підвищення оперативної спроможності в ЄС посилюється створенням мережі організацій на кшталт CyCLONe, координацією кризового менеджменту у випадку масштабних транскордонних кіберінцидентів, а Об'єднаний кіберпідрозділ забезпечуватиме скоординовану реакцію між цивільними, правоохоронними, дипломатичними відомствами. Нарощування потенціалу ЄС у сфері кібербезпеки здійснюватиметься в рамках Європейського центру компетенції з кібербезпеки, який разом із мережею національних центрів сформує щит кібербезпеки на базі технологій штучного інтелекту та інфраструктури суперкомп'ютерів (Willett, 2019).

Трагічний досвід України продемонстрував можливості держави-агресора використовувати кібератаки, щоб загрожувати критичній національній інфраструктурі: фінансовим установам, трубопроводам, атомним електростанціям, електромережам і комунікаційним маршрутизаторам. Так, за кілька годин до запуску ракет 24 лютого 2022 року Центр розвідки загроз Microsoft виявив низку аступальних та руйнівних кібератак включно з виявленням нового пакета шкідливого програмного забезпечення FoxBlade, спрямованих проти інфраструктури України[29]. Відбулися напади на цілі, включаючи українські військові установи, ОПК та декілька інших українських державних установ. Цілями кіберзлочинів були:

- контроль за об'єктами критичної інфраструктури (електростанціями, системами тепло- та водопостачання);
- крадіжка та збір розвідувальних даних, у тому числі інформації з обмеженим доступом;
- інформаційно-психологічний вплив;
- блокування інформаційних систем.

Такі загрози визначаютьє важливість синхронізації політики кібербезпеки України з міжнародними підходами, зокрема ЄС та Північно-антлантичного альянсу (табл. 3).

Вразливість української системи кібербезпеки обумовлена також існуючими і до війни проблемами: відсутність реєстру об'єктів критичної інфраструктури; відсутність передумов для стрімкого зростання вітчизняного виробництва конкурентоспроможних засобів захисту; постійно зростаюча кількість кібератак на системи державних інформаційних ресурсів; використання російського програмного забезпечення органами державної влади, громадянами та бізнесом, що потенційно може містити шпигунський або іншого роду шкідливий програмний

[28] Commission welcomes political agreement on new rules on cybersecurity of network and information systems. Press release13 May 2022. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985(дата звернення 02.02.2023 р.)
[29] Smith B. Digital technology and the war in Ukraine. Blog post 28.02.2022. Microsoft. URL: https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/ (дата звернення 02.02.2023 р.)

Таблиця 3

Заходи посилення кібербезпеки в Україні

Завдання	Проект в рамках завдання	Необхідні нормативно-правові акти
Посилення захисту державних інформаційних ресурсів	Створення реєстру заборонених до використання програмних продуктів	Постанова КМУ щодо унормування використання сервісів захисту від DDoS, очищення трафіку та CDN ; Проєкт Закону України "Про внесення змін до деяких законів України щодо невідкладних заходів із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури".
Зростання рівня кібербезпеки в органах державної влади, місцевого самоврядування, об'єктах критичної інфраструктури	Оновлення кваліфікаційних вимог відповідно до Європейської рамки кваліфікації, розробка професійних стандартів	Постанова Кабінету Міністрів України "Про затвердження Порядку пошуку та виявлення потенційних вразливостей інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж на підставі публічної пропозиції (оферти)".
Оцінка захищеності критичної інфраструктури (перелік пріоритетних об'єктів)	Створення реєстру об'єктів критичної інформаційної інфраструктури	Внесення змін до до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури.

Джерело: складено за даними Національної ради з відновлення України від наслідків війни [30]

код. За останні два роки найчастіше атакують офіційні вебпредставництва Президента України, сайти СБУ, Державного бюро розслідувань та Національного антикорупційного бюро України, Київської міської держадміністрації, Державної служби з надзвичайних ситуацій та Міністерство внутрішніх справ[31].

2. Підвищення обізнаності, розбудова потенціалу та набуття цифрових навичок

Підвищення обізнаності, розбудова потенціалу та набуття навичок є ключовими викликами для Цифрового переходу ЄС. У 2021 році лише 54% людей у ЄС віком від 16 до 74 років мали базові цифрові навички. Пріоритетом подальшого розвитку має бути доступ до апаратного та програмного забезпечення та розвиток навичок використання кіберпростору та Інтернету таким чином, щоб розширити можливості громадян і категорій окремих громадян, які мають обмежені можливості доступу до інтенету, а саме населення з низькими доходами або люди, які проживають у сільській місцевості. Крім того, підвищення обізнаності та набуття цифрових навичок надають можливості для вдосконалення законодавства в цифровій сфері. Ці інструменти можуть сприяють залученню громадян до процесу прийняття рішень, використовуючи переваги демократичної участі для створення змістовної та ефективної політики щодо цифрової стратегічної автономії ЄС. Такі інструменти як онлайн-обговорення, онлайн-залучення та участь громадян, можуть бути включені процеси публічного управління, включаючи ідентифікацію проблем, встановлення порядку денного, ухвалення політики або оцінку результативності.

В Україні формування цифрових навичок стало пріоритетом держави ще у 2021 році, коли Кабінет Міністрів України схвалив Концепцію розвитку цифрових компетентностей до 2025 року. У тому ж році Міністерство цифрової трансформації України проводило місяць

[30] Ukraine's National Recovery Plan. National Recovery Council. 2022. URL: https://uploads-ssl.webflow.com/621f88db25fbf24758792dd8/62c166751fcf41105380a733_NRC%20Ukraine%27s%20Recovery%20Plan%20blueprint_ENG.pdf (дата звернення 02.02.2023 р.)

[31] Щиголь Ю. Важко захищати об'єкти критичної інфраструктури без прямого впливу на процес захисту інформації. Інтерв'ю. Інтерфакс-Україна. 01.11.2021. URL: https://ua.interfax.com.ua/news/interview/777637.html (дата звернення 02.02.2023 р.)

цифрової грамотності, рівень якої не задовольняв потреб світової цифрової економіки. Так, за результатами дослідження Міністерства цифрової трансформації за 2019 рік 53% українців перебувають нижче позначки "базовий рівень" у навичках з цифрової грамотності, 15,1% українців не володіють ними взагалі, а низький рівень навичок мають 37,9% громадян. Щоб навчити українців цифрової грамотності, у лютому 2020 року Мінцифри запустило національну онлайн-платформу з цифрової грамотності Дія.Цифрова освіта. За рік платформу відвідали майже 2 млн українців, з них майже 500 тисяч зареєструвались на навчання, створені близько 2000 офлайн-хабів цифрової освіти по всій Україні[32]. Під час війни продовжується формування цифрових навичок населення, хоч і в скорочених обсягах через економне споживання електроенергії.

Наступним показником цифрової автономії є доступ населення до Інтернету, що розраховується як відсоток осіб, які користувалися Інтернетом з будь-якого місця незалежно від використовуваного пристрою та мережі (рис. 3).

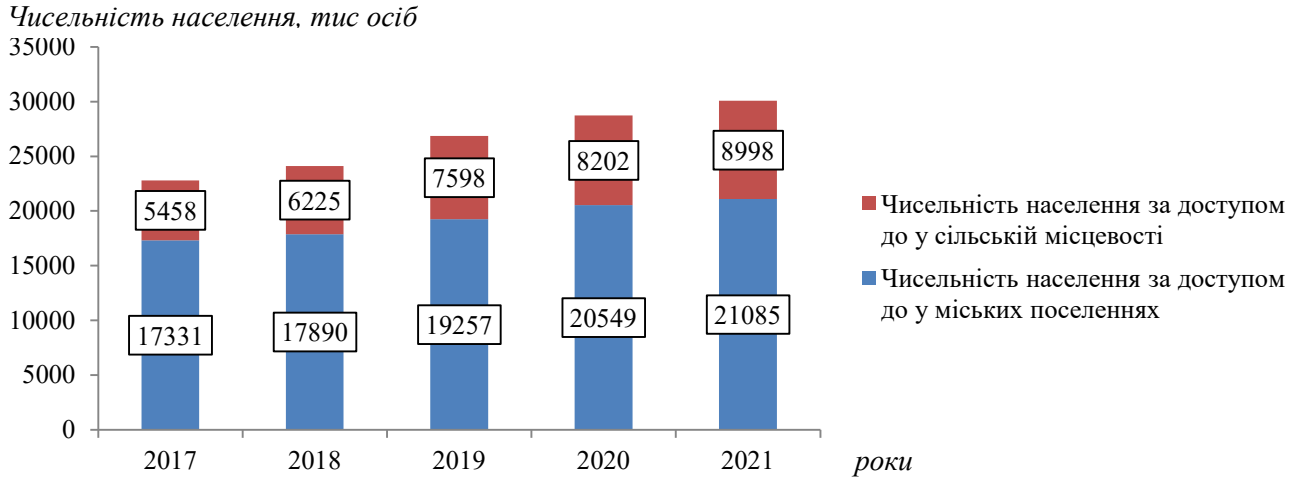

Рис. 3. Доступ населення України до Інтернету у 2017-2021 рр.
Джерело: складено за даними Держстату України[33]

Аналіз умов доступу до глобальної мережі Інтернет висвітлює перешкоди, що ускладнюють процеси адаптації до цифрових викликів. Дійсно, за останні роки кількість користувачів Інтернету в Україні щорічно зростає і сягає 79,5% населення на кінець 2021 року, що хоч і нижче середньозваженого значення по Європі (87,7%), проте вище середнього значення в світі (58,8%). Водночас, в Україні спостерігається значна розбіжність щодо кількості користувачів Інтернету в міських та сільських поселеннях (83,7 у міській місцевості, 71,3% користувачів у сільських місцевості). За останні роки диспропорції проникнення Інтернету в населених пунктах різної величини помітно згладилися. На даний момент значно відстає у поширенні Інтернету сільська місцевість, мешканці якої частіше посилаються на обмеження в технічних можливостях підключення малонаселених пунктів. Варто також зауважити, що розвиток Інтернет породжує ще один вид соціальної диференціації (а можливо і інформаційної дискримінації) в Україні: сільське населення, особи з низьким рівнем доходу і старші вікові групи користуються Інтернетом значно менше, ніж інші. Через масовий обстріл української енергетичної інфраструктури в деяких містах тривали аварійні та планові відключення електроенергії. І в цих умовах виникали проблеми з доступом до стаціонарного і мобільного інтернету. Крім цього, одна з актуальних потреб операторів – це заміна батарей базових станцій на літієві. Це дозволить швидше заряджати та підтримувати роботу станції, а отже довше

[32] Мінцифри збирається навчити 6 мільйонів українців цифрових навичок за 3 роки. Міністерство цифрової трансформації України. 22.03.2021. URL: https://www.kmu.gov.ua/news/mincifri-zbirayetsya-navchiti-6-miljoniv-ukrayinciv-cifrovih-navichok-za-3-roki (дата звернення 02.02.2023 р.)
[33] Доступ домогосподарств України до Інтернету (за даними вибіркового опитування домогосподарств, проведеного у січні 2022 року). Статистичний збірник. Державна служба статистики України. URL: https://ukrstat.gov.ua/druk/publicat/kat_u/2022/zb/07/zb_dd_internet_21.pdf (дата звернення 02.02.2023 р.)

забезпечувати зв'язок під час вимкнення електрики. Отже, учасниками ринку потрібно повністю оновити й модернізувати власну мережу, що вимагає значних інвестицій. Виникає потреба переглянути законодавчі вимоги до стійкості мереж, вирішення якого залежить від державних органів: Мінцифри, Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв`язку та Держспецзв'язку, передбачене в проєкті плану з відновлення цифрової інфраструктури.

3. Розробка норм регулювання для цифрових технологій

Важливою складовою формування цифрової автономії в ЄС є регулювання й налаштування стандартів і норм в цифровому посторі. Таке регулювання виходить за рамки технічних складових і стає важливою геополітичною можливістю для поширення норм, які базуються на європейських цінностях, правах людини. Ці нормативні акти стосуються таких сфер як: боротьба з дезінформацією, запровадження обмежень для великих технологічних компаній, створення Єдиного простору даних у ЄС на основі конвергенції; нові технічні стандарти для проривних технологій; а популяризація спільної позиції щодо застосування міжнародного права в кіберпросторі може допомогти ЄС посилити свою роль цифрового лідера. Розробка норм регулювання для цифрових технологій визнає стратегічну важливість посилення співпраці Ради з торгівлі та технологій ЄС з ключовими гравцями на світовій арені – США, Індією, Японією, Південною Кореєю, Сінгапуром.

В Україні, яка у 2022 році стала членом програми "Цифрова Європа" продовжується робота з наближення норм регулювання до європейських норм. На засіданні Ради асоціації Україна – ЄС, яке відбулося 05 вересня 2022 року у Брюсселі, де Україна вперше взяла участь у статусі кандидата на членство у Європейському Союзі, високо оцінено залученість України до відбудови та швидкого розвитку в напрямі зелених, стійких до клімату та цифрових перетворень і входження сектору телекомунікаційних послуг до режиму внутрішнього ринку[34]. Наступними кроками у досягненні прогресу на 2023 рік визнано такі сфери вдосконалення регулювання:

- забезпечення громадян якісним зв'язком (удосконалення Закону України "Про електронні комунікації");
- завершення реформи державних реєстрів (приведення законодавства у відповідність до Закону України "Про публічні електронні реєстри");
- розвиток цифрової інфраструктури регіонів, їх швидке післявоєнне відновлення шляхом можливості об'єднання ресурсів органів місцевого самоврядування та суб'єктів господарської діяльності (робота над проектом Закону "Про спільне фінансування розвитку цифрової інфраструктури");
- продовження інтеграції законодавства України з питань цифрової трансформації до положень права ЄС та виконання міжнародно-правових зобов'язань України у сфері європейської інтеграції України до цифрового ринку ЄС.

4. Промислова політика, дослідження, інвестиції та зміцнення ланцюгів поставок

ЄС розглядає формування промислової політики, орієнтованої на технології, щоб зменшити недоліки в технологічних можливостях в поєднанні з інвестиційними зобов'язаннями для посилення розробки альтернатив для ключових цифрових послуг, таких як хмарні технології або нові обчислювальні ресурси квантових технологій. Ключове значення матиме інвестування в дослідження та створення державно-приватного партнерства для залучення, підтримки та утримання кваліфікованих працівників для сприяння інноваціям. Саме тому ЄС спрямовує значні інвестиції, щоб впровадити інноваційні цифрові технології.

В Україні подібні процеси також знаходять своє відображення. Так, 17.01.2018 року було схвалено Концепцію розвитку цифрової економіки та суспільства України на 2018–2020 рр. та затверджено план заходів щодо її реалізації. Водночас, механізми підтримки адаптації української промисловості до викликів цифрового переходу тільки починають формуватися. В Україні хоч і ухвалені нормативно-правові засади впровадження цифрових технологій, водночас,

---

[34] Департамент комунікацій Секретаріату Кабінету Міністрів України. Спільна прес-конференція Д. Шмигаля, Ж. Борреля, О. Варгеї. 05 вересня 2022. URL: https://www.kmu.gov.ua/events/5-veresnia-spilna-pres-konferentsiia-denysa-shmyhalia-zhozepa-borrelia-olivera-varhei (дата звернення 02.02.2023 р.)

слід відмітити, що головну увагу в програмних документах приділено електронному урядуванню, що вказує на початковий етап формування стратегічних документів та недостатню увагу сприяння розвитку діджиталізації саме в промисловості. Створене у 2019 р. Міністерство цифрової трансформації також визначає одним з пріоритетів формування та реалізацію державної політики у сфері цифровізації, цифрової економіки, цифрових інновацій, електронного урядування та електронної демократії, розвитку інформаційного суспільства. А представлений у липні 2022 року План заходів з післявоєнного відновлення та розвитку України з переліком пропозицій щодо пріоритетних реформ та стратегічних ініціатив Національної ради з відновлення України від наслідків війни відповідно до Указу Президента від 21 квітня 2022 р. № 266/2022 р. пропонує заходи з розвитку електронних публічних послуг, що сприятимуть відновленню цифрової економіки України та її інтеграції в світовий цифровий простір. Водночас відсутність обґрунтування стратегічних ініціатив зі сприяння адаптації української промисловості до технологічних цифрових викликів нарощує розрив між Україною та розвинутими країнами світу й тільки посилює ефект деіндустріалізації економіки країни. Для реалізації поставлених у Плані відновлення завдань за даним напрямом важливо синхронізувати матеріали відповідно європейського стратегічного курсу. Зокрема, згідно з галузевою ініціативою ЄС "Цифровізація європейської промисловості в рамках пакета "Єдиний цифровий ринок", забезпечити, щоб підприємства всіх розмірів, розташування й секторів могли повною мірою використовувати переваги цифрових інновацій. Для цього на етапі відновлення – "Відновлення, перезапуск економіки та інститутів" додати завдання "Сприяння до цифрових трансформацій в промисловості".

Цифрова економіка та ІТ-сектор в Україні переживали стрімке зростання в роки, що передували війні, залучаючи висококваліфікованих українців та інвестиції транснаціональних компаній. В часи війни дистанційна робота та хмарні сервери, розташовані як у країні, так і за її межами, дозволяли багатьом підприємствам продовжувати діяльність. Широкомасштабна агресія росії проти України спричиняє серйозні порушення підключення до Інтернету, що є передумовою для стійкості та подальшого розвитку цифрової економіки, а цифрові технології відіграють вирішальну роль у зміцненні обороноздатності нашої країни. Доступ до Інтернету та якість передачі даних знизилися з початком війни як через кібератаки, так і через фізичні атаки на цифрову інфраструктуру країни. Водночас слід відмітити стійкість цифрової системи, адже не зважаючи на військові виклики продовжується розвиток цифрового надання державних послуг. Так, платформа та додатки "Дія" дозволяють підтримувати надання державних послуг, але міграція та залучення фахівців до військової служби загострюють кадровий дефіцит у країні. Крім того, необхідно вирішити структурні проблеми, такі як відновлення потужностей критичної інфраструктури, мереж електропостачання та засобів зв'язку.

5. Створення альянсів і сприяння міжнародній співпраці

ЄС підтримує міжнародну співпрацю із багатьма зацікавленими сторонами, включаючи наукові кола, громадянське суспільство, промисловість і технологічні компанії, а також інші уряди та міжнародні організації для досягнення цифрової стратегічної автономії та забезпечення координації в багатьох сферах, таких як регулювання та стандартні налаштування, а також безпеки ланцюга поставок, створення безпечних потоків даних. Міжнародні зв'язки є основою багатьох виробничих і операційних процесів у ключових цифрових технологіях, таких як виробництво напівпровідників та мікросхем, робота з даними та хмарні сховища.

Для України наразі посилюється значення міжнародного співробітництва, завдяки якому можна протистояти військовим викликам, адже міжнародна допомога сприяє отриманню необхідних засобів для економічного й гуманітарного відновлення, що включає покращення доступу до таких ресурсів як: матеріальні (промислове обладнання й устаткування, сировина, матеріали), фінансові, інтелектуальні (ноу-хау, трансферт технологій), навчальні та консультаційні (висококваліфіковані спеціалісти), інформаційні (консалтинг, тренінги, програми навчання) та ін. До того ж можливості міжнародної допомоги, що пропонують міжнародні організації-донори, здатні прискорити приєднання українського бізнесу до глобальних ланцюгів доданої вартості. Водночас, погоджуємося з Ю. Кіндзерським, який наголошує, що категорично

не варто робити ставку на відновлення лише на основі іноземної допомоги у вигляді постачання промислових товарів в Україну замість відбудови чи створенні підприємств для виробництва аналогічних товарів в середині країни (Кіндзерський, 2022). Пи цьому критично важлива роль у повоєнному відновленні економіки належить державі як інституту, який повинен забезпечити дієві стимули для налагодження ефективної взаємодії між бізнесом і наукою. Держава, акумулюючи в одному джерелі значні ресурси, є субєктом відповідальності за стан і долю країни, рівень конкурентоспроможності економіки, її місце в глобальному економічному і технологічному просторі, за національну безпеку суб'єктів господарювання (Промисловість України, 2022). Саме тому, післявоєнна структурна перебудова української промисловості повинна проводитися не лише як відновлення зруйнованих війною промислових та інфраструктурних потужностей, а педбачатиме стратегічне планування структурної модернізації промисловості на вищому технологічному рівні з урахуванням збереження її можливостей до самозабезпечення, експортної орієнтації та включення до глобальних ланцюгів створення вартості з урахуванням необхідності відповіді на виклики щодо низьковуглецевого розвитку, Цілей сталого розвитку та досягнення перспектив євроінтеграції (Відновлення та реконструкція, 2022). Промисловість України у повоєнному періоді повинна стати драйвером створення високорозвиненої індустріальної економіки, спроможної забезпечувати як відбудову, так і реконструкцію економіки країни, підтримувати її обороноздатність у довгостроковому періоді та здатність швидко реагувати як на потреби захисту держави, так на потреби внутрішнього і зовнішніх ринків.

Висновки. Загрозливі виклики сьогодення – війна в центрі Європи, пандемія, глобальні загрози демократичному розвитку суспільства підкреслили ключову роль цифрових технологій для розвитку сталого та процвітаючого майбутнього. Проте, війна росії проти України трансформує розуміння того, що означає бути захищеним у цифрову епоху. Перший повномасштабний військовий конфлікт на європейській землі за десятиліття демонструє зростаючу роль цифрових технологій у реаліях міждержавного конфлікту, оскільки росія має намір знищити український суверенітет. Відповіддю ЄС на ці події є посилення стратегічної автономії – розробка і впровадження політики та інструментів для підвищення економічної та технологічної конкурентоспроможності Європи та сприяння здатності захищати свої суспільні інтереси, визначати правила та стандарти в епоху цифрових технологій. Практично це проявляється в ухвалених стратегічних документах: Порядку денного цифрового десятиліття ЄС, Стратегічного й Цифрового компасу ЄС; спільних позицій держав-членів ЄС щодо кібербезпеки та цифрової дипломатії; а також заходи промислової політики, що керуються стратегічною автономією, наприклад Закон ЄС про мікросхеми.

Прискорення інтеграційних процесів України як кандидата на членство в ЄС залежить від стратегічного планування відновлення з врахуванням принципів цифрового переходу ЄС. Це передбачає низку заходів консолідації українського законодавства з європейськими регламентами, зокрема ухвалення стратегічних документів, дорожніх карт у сфері політики, спрямованої на зменшення розбіжностей у цифровому розвитку. Водочас досягнення цифрової автономії в Україні в короткостроковому періоді залежить і від розв'язання критично важливих проблем, обумовлених військовими діями. Мова йде перш за все про доступ громадян України до мережі інтернет. Для цього першочерговим є забезпечення безпечної роботи інтернет провайдерів, створення умов для модернізації сфери ІТ послуг, розвиток цифрових навичок населення, стимулювання науково-технічних розробок та співпраці з міжнародними розробниками, захист права власності та сприяння розвитку інноваційної інфраструктури з метою зростання кількості інноваційних стартапів. Важливе місце при цьому посідає забезпечення платоспроможності населення та подолання бідності, адже користування інтернетом та цифровими послугами залежать від можливості користуватися сучасними засобами зв'язку. Тому в подальших наукових дослідженнях доцільно акцентувати увагу на поєднанні інструментів всіх рівнів управління, а саме держави, бізнесу і суспільства для модернізації мереж відповідно до зростаючого попиту та усуненні перешкод, пов'язаних із низьким рівнем доходу населення та формування цифрових навичок.

Список використаних джерел.

1. Геєць В.М. Соціальна реальність у цифровому просторі. *Економіка України*. 2022. № 1. С. 3-28. https://doi.org/10.15407/economyukr.2022.01.003

2. Гриценко А.А. Комплементарність інформаційно-цифрових і соціально-економічних перетворень як умова стабільного розвитку суспільства : монографія. Київ: ДУ "Ін-т. екон. та прогнозув. НАН України", 2021. 400 с.

3. Єгоров І.Ю., Никифорук О.І., Лір В.Е. та ін. Цифрові технології в інноваційній трансформації економіки України : колективна монографія. Київ : ДУ "Ін-т. екон. та прогнозув. НАН України", 2020. 308 с.

4. Bakardjieva E., Bremberg N., Michalski A., Oxelheim L. The European Union in a Changing World Order: What Is at Stake? Interdisciplinary European Studies. New York: Palgrave Macmillan, 2020. Pp. 23-46. https://doi.org/10.1007/978-3-030-18001-0

5. Cervi G. V. The Brussels Effect in Digital Policy: Why Does It Matter? *The Ventotene Lighthouse*. 2022. Pp. 1121-1144. URL: https://www.theventotenelighthouse.eu/the-brussels-effect-in-digital-policy-why-does-it-matter/

6. Ryon E. European strategic autonomy: Energy at the heart of European security? *European View*, 2020. № 19 (2). Pp. 238-244. URL: https://doi.org/10.1177/1781685820968302/

7. Дейнеко Л.В., Кушніренко О.М., Ципліцька О.О., Гахович Н.Г. Наслідки повномасштабної воєнної агресії РФ для української промисловості. *Економіка України*. 2022. № 5. С. 3-25. https://doi.org/10.15407/economyukr.2022.05.003

8. Cagnin C., Muench S., Scapolo F., Stoermer E., Vesnic A. Shaping and securing the EU`s Open Strategic Autonomy by 2040 and beyond. JRC Publications Repository. Luxembourg: Publications Office of the European Union. 2021. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC125994

9. Gajewski T. Digital Technologies and the Prospects of the European Union's Strategic Autonomy. *Athenaeum Polskie Studia Politologiczne*. 2022. № 76 (4). pp. 127-148. https://doi.org/10.14763/2020.4.1532

10. Pohle J., Thiel T. Digital sovereignty. *Internet Policy Review*. 2020. № 9 (4). URL: https://policyreview.info/pdf/policyreview-2020-4-1532.pdf

11. Pogorel G., Nestoras A., Cappelletti F. Decoding EU Digital Strategic Autonomy: Sectors, Issues, and Partners. *Techno-Politics Series. European Liberal Forum EUPF*. 2022. № 1. URL: https://www.researchgate.net/publication/361736581_Decoding_EU_Digital_Strategic_Autonomy_Sectors_Issues_and_Partners

12. Willett M. Cyber instruments and international security. Analysis. *The International Institute for Strategic Studies*. 2019. URL: https://www.iiss.org/blogs/analysis/2019 /03/cyber-instruments-and-international-security

13. Кіндзерський Ю. Повоєнне відновлення промисловості України: виклики та особливості політики. *Економічний аналіз.* 2022. Том 32. № 2. С. 101-117.

14. Промисловість України перед викликами майбутнього: у пошуках відповідей та рішень: колективна монографія. Київ : ДУ "Ін-т. екон. та прогнозув. НАН України". 2022. 346 с.

15. Відновлення та реконструкція повоєнної економіки України : наукова доповідь. Київ: ДУ "Ін-т. екон. та прогнозув. НАН України". К., 2022. 305 с. URL: http://ief.org.ua/wp-content/uploads/2022/12/Vidnovlennja-ta-reconstrukcsja-povojennoji-economiky.pdf

References.

1. Heyets, V. (2022), "Social reality in the digital space", *Ekonomika Ukrainy*, 2022, vol. 1, pp. 3-28. https://doi.org/10.15407/economyukr.2022.01.003

2. Hrytsenko, A. (2021), Komplementarnist informatsiino-tsyfrovykh i sotsialno-ekonomichnykh peretvoren yak umova stabilnoho rozvytku suspilstva [Complementarity of information-digital and socio-economic transformations as a condition for stable development of

society], Institute of the Economy and Forecasting of the National Academy of Sciences of Ukraine, Kyiv.

3. Yehorov, I.Iu., Nykyforuk, O.I., Lir, V.E. (2020), Tsyfrovi tekhnolohii v innovatsiinii transformatsii ekonomiky Ukrainy [Digital technologies in the innovative transformation of the economy of Ukraine], Institute of the Economy and Forecasting of the National Academy of Sciences of Ukraine, Kyiv.

4. Bakardjieva, E., Bremberg, N., Michalski, A., Oxelheim, L. (2020), The European Union in a Changing World Order: What Is at Stake? Interdisciplinary European Studies. Palgrave Macmillan, New York, USA.

5. Cervi, G. V. (2022), "The Brussels Effect in Digital Policy: Why Does It Matter?" *The Ventotene Lighthouse,* pp. 1121-1144. URL: https://www.theventotenelighthouse.eu/the-brussels-effect-in-digital-policy-why-does-it-matter/.

6. Ryon, E. (2020), "European strategic autonomy: Energy at the heart of European security?" *European View*, vol. 19 (2), pp. 238-244. URL: https://doi.org/10.1177/1781685820968302.

7. Deineko, L.V., Kushnirenko, O.M., Tsyplitska, O.O., Gakhovich N.G. (2022), "Consequences of full-scale military aggression of the Russian Federation for Ukrainian industry", *Ekonomika Ukrainy*, vol. 5, pp. 3-25. https://doi.org/10.15407/economyukr.2022.05.003

8. Cagnin, C., Muench, S., Scapolo, F., Stoermer, E., Vesnic, A. (2021). Shaping and securing the EU`s Open Strategic Autonomy by 2040 and beyond. JRC Publications Repository. Publications Office of the European Union, Luxembourg, European Union. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC125994.

9. Gajewski, T. (2022), "Digital Technologies and the Prospects of the European Union's Strategic Autonomy". *Athenaeum Polskie Studia Politologiczne*, vol. 76 (4), pp. 127-148. URL: DOI: 10.15804/athena.2022.76.07.

10. Pohle, J., Thiel, T. (2020), "Digital sovereignty". *Internet Policy Review*, vol. 9, issue 4. URL: https://policyreview.info/concepts/digital-sovereignty.

11. Pogorel, G., Nestoras, A., Cappelletti, F. (2022), "Decoding EU Digital Strategic Autonomy: Sectors". *Techno-Politics Series. European Liberal Forum EUPF,* vol. 1, pp. 152-158. URL: https://www.researchgate.net/publication/361736581_Decoding_EU_Digital_Strategic_Autonomy_Sectors_Issues_and_Partners.

12. Willett, M. (2019), "Cyber instruments and international security". *Analysis. the International Institute for Strategic Studies (IISS).* URL: https://www.iiss.org/blogs/analysis/2019/03/cyber-instruments-and-international-security.

13. Kindzerski, Yu. (2022), "Post-war recovery of Ukrainian industry: difficulties and peculiarities of the policy". *Ekonomichnyi analiz*, vol. 32 (2), pp. 101-117.

14. Promyslovist Ukrainy pered vyklykamy maibutnoho: u poshukakh vidpovidei ta rishen (2022), [Industry of Ukraine facing the challenges of the future: in search of answers and solutions], Institute of the Economy and Forecasting of the National Academy of Sciences of Ukraine, Kyiv.

15. Recovery and reconstruction of the post-war economy of Ukraine: scientific report (2022), Institute of the Economy and Forecasting of the National Academy of Sciences of Ukraine, Kyiv, Ukraine. 305 p. URL: http://ief.org.ua/wp-content/uploads/2022/12/Vidnovlennja-ta-reconstrukcsja-povojennoji-economiky.pdf.

Стаття надійшла до редакції 10.02.2023 р.
Рецензовано 25.02.2023 р.
Опубліковано 28.02.2023 р.