https://www.bloomberg.com/news/articles/2023-09-22/russia-plans-huge-defense-spending-hike-in-2024-as-war-drags-on?embedded-checkout=true [Accessed: 25/1/2024].

3. Memorandum on security assurances in connection with Ukraine's accession to the Treaty on the Non-Proliferation of Nuclear Weapons. 1994. Budapest. Available at: https://treaties.un.org/doc/Publication/UNTS/Volume%203007/Part/volume-3007-I-52241.pdf [Accessed: 25/3/2024].

УДК 338.2

Онищенко Світлана Володимирівна*[8]*,
доктор економічних наук, професор
Глушко Аліна Дмитрівна,
кандидат економічних наук, доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)

ЄВРОПЕЙСЬКА ПАРАДИГМА БЕЗПЕЧНОГО ЦИФРОВОГО СВІТУ ДЛЯ ПІДВИЩЕННЯ СТІЙКОСТІ ЕКОНОМІКИ

Глобальні виклики останніх років – пандемія COVID-19, війна росії проти України, геополітична криза, кардинально змінили роль і сприйняття процесів цифровізації для забезпечення безпеки та стійкості національних економік [1]. У сучасних умовах цифрові технології виступають головним джерелом підвищення якості життя, розвитку бізнесу та впровадження інновацій [2]. Запровадження цифрових рішень є базисом переходу до кліматично нейтральної, замкнутої та більш стійкої економіки. Цифрові технології сприяють підвищенню рівня екологічності процесів у сільському

[8] Тези підготовлено в межах виконання проєкту Жана Моне Erasmus+ 101127395–EEEISEUEU–ERASMUS-JMO-2023-HEI-TCH-RSCH «Забезпечення екологічної, економічної та інформаційної безпеки: досвід ЄС для України».

господарстві, енергетиці, будівництві, промисловості, сприяючи, таким чином, формуванню «зеленої» економіки. Забезпечення зростання енерго- та ресурсоефективності цифрових інфраструктур та технологій дозволить зміцнити економічну та екологічну безпеку країн. Цифрові технології визнані ключовими активами для економічного успіху та стійкості Європейського Союзу.

Водночас, підвищення вразливості цифрового простору до зростаючих кіберзагроз, вплив дезінформаційних кампаній на демократичні суспільства, загострення «цифрових розривів» між територіями та суб'єктами господарювання, виникнення «цифрової бідності» – це ті актуальні проблеми, які потребують вирішення в аспекті побудови безпечного цифрового простору.

Європейська парадигма безпечного цифрового світу для підвищення стійкості та процвітання економіки включає в себе такі ключові аспекти як захист прав і свобод людини в цифровому середовищі; забезпечення кібербезпеки та стійкості критичної інфраструктури; стимулювання інновацій та цифрового розвитку; підвищення цифрової грамотності та інклюзії; розвиток міжнародного співробітництва. Цифрова трансформація ЄС ґрунтується на принципі людиноцентризму, який передбачає захист прав та свобод людей у цифровому просторі, включаючи право на приватність, свободу слова та доступ до інформації, недопущення дискримінації [3]. Невід'ємним елементом формування безпечного цифрового світу є зміцнення кібербезпеки через посилення заходів з протидії кіберзагрозам і кіберзлочинності, розвиток компетенцій та можливостей реагування на кіберінциденти. Підвищення цифрових компетенцій громадян, особливо вразливих груп, забезпечення рівного доступу до цифрових послуг та інфраструктури дозволить сформувати суспільство, яке довірятиме цифровим продуктам і онлайн-сервісам, зможе

виявляти дезінформацію та протидіяти кібершахрайству. Цифрове лідерство та глобальна конкурентоспроможність Європи залежать також від спільної політики країн-членів ЄС та розвитку міжнародної взаємодії. Особливий акцент на сьогоднішній день робиться на посиленні співпраці ЄС з Україною у сфері протидії гібридним загрозам і дезінформації, зміцненні кібербезпеки [4].

З метою забезпечення безпеки та стійкості цифрової екосистеми на рівні Європейського Союзу прийнято ряд нормативно-правових документів, які регулюють питання етичного використання штучного інтелекту, безпечної цифрової ідентичності, вдосконалення інфраструктури даних, захисту персональних даних, впровадження ефективних систем безпеки інформаційно-комунікаційних технологій тощо [5, 6]. Серед них доцільно відмітити Стратегію кібербезпеки ЄС (EU Cybersecurity Strategy), Стратегічний план з кібербезпеки ЄС (EU Cybersecurity Strategic Plan), Загальний регламент з захисту персональних даних (GDPR), Закон про штучний інтелект (Artificial Intelligence Act, AI Act).

Уряди країн Європейського Союзу відіграють ключову роль у зміцненні інформаційної безпеки на національному рівні та в межах ЄС. Водночас залишається ряд пріоритетних напрямів щодо формування безпечного цифрового світу:

– подальше удосконалення законодавства щодо кібербезпеки, захисту даних, протидії дезінформації;

– підвищення обізнаності населення з питань кібергігієни та медіаграмотності;

– створення спеціалізованих державних органів з питань кібербезпеки та моніторингу інформпростору;

– інвестування в розвиток національних технічних можливостей кіберзахисту;

– координація та співпраця з приватним сектором у питаннях інформаційної безпеки, в тому числі кібербезпеки.

Реалізація окреслених заходів є основою для побудови цифрового суверенітету Європейського Союзу, для забезпечення стійкої та процвітаючої цифрової економіки.

Література

1. Onyshchenko, S., Hlushko, A., Yanko, A. (2020). Role and importance of information security in a pandemic environment. Economics and Region, 2 (77), 103–108.
2. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O. (2023). Economic cybersecurity of business in Ukraine: strategic directions and implementation mechanism. Economic and cyber security. Kharkiv: PC TECHNOLOGY CENTER, 30–58. doi: https://doi.org/10.15587/978-617-7319-98-5.ch2
3. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. 2030 Digital Compass: the European way for the Digital Decade. EUROPEAN COMMISSION. Brussels, 9.3.2021. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118
4. Давимука О.О. Ухвалення «Стратегічного компасу» Європейського Союзу. Національний інститут стратегічних досліджень. Центр зовнішньополітичних досліджень. 2022. URL: https://niss.gov.ua/sites/default/files/2022-04/evropeyskiy_kompas.pdf
5. Onyshchenko S., Yanko A., Hlushko A., Maslii O., Cherviak A. Cybersecurity and improvement of the information security system . Journal of the Balkan Tribological Association . 2023. 29(5). pp . 818–835.
6. Onyshchenko S., Yanko A., Hlushko A., Sivitska S. Conceptual principles of providing the information security of the national economy of Ukraine in the conditions of digitalization. International Journal of Management. 2020. № 11(12). P. 1709-1726. https://doi.org/10.34218/IJM.11.12.2020.157