УДК 327:004.056 ЄС

Абрат С. Б.
аспірант,
кафедра політології та міжнародних відносин,
НУ «Львівська політехніка»,
кім. 314, 4 н.к., вул. Митрополита Андрея, 5,
м. Львів, 79016, Україна
E-mail: serhii.b.abrat@lpnu.ua
ORCID ID: http://orcid.org/0009-0004-4378-3460
DOI https://doi.org/10.32782/2707-5206.2024.37.14

СПІВРОБІТНИЦТВО ЄС ТА КРАЇН-УЧАСНИЦЬ СХІДНОГО ПАРТНЕРСТВА У СФЕРІ КІБЕРБЕЗПЕКИ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

У статті проаналізовано особливості співробітництва ЄС та країн Східного партнерства у сфері кібербезпеки. Виокремлені основні формати співпраці між ЄС та країнами регіону у питанні кіберзахисту. Проаналізовані ключові інструменти ЄС щодо посилення системи кібербезпеки країн Східного партнерства. Серед них виокремлено Ініціативу ЄС «Східне партнерство», програму ЄС «EU4Digital», угоди про асоціацію з Україною, Молдовою та Грузією. Здійснено аналіз Глобального індексу кібербезпеки країн регіону. Встановлено, що найбільший захист кіберпростору мають Азербайджан та Грузія, а найменший – Вірменія та Білорусь. На основі аналізу Індексу кібербезпеки розроблено класифікацію за критерієм стійкості кіберзахисту, зокрема: держави із високим рівнем кібербезпеки (Азербайджан та Грузія); держави із прогресуючою системою кіберзахисту (Україна, Молдова); держави із слабкою системою кібербезпеки (Білорусь та Вірменія). Досліджено ключові внутрішні та зовнішні виклики системі кібербезпеки країнам Східного партнерства. Встановлено, що наявна низка зовнішніх викликів, зокрема геополітична складність регіону, гібридні атаки РФ, відсутність бажання частини країн Східного партнерства інтегруватись до ЄС. До внутрішніх викликів системі кібербезпеки досліджуваних держав можна віднести слабкість або відсутність імплементації стратегій кібербезпеки, застарілі системи кіберзахисту, відсутність ресурсів на покращення системи кібербезпеки, низька інтенсивність впровадження європейський стандартів. Також подані рекомендації щодо посилення співпраці між ЄС та країнами Східного партнерства у сфері кіберзахисту та протидії гібридним викликам. Зокрема варто посилити інтеграцію країн регіону до Єдиного цифрового ринку ЄС, що дасть змогу мати більш надійну систему кіберзахисту. Розглянуті перспективи та можливі сценарії щодо посилення співпраці ЄС-країни Східного партнерства у галузі кібербезпеки.
Ключові слова: ЄС, Східне партнерство, кібербезпека, кіберзагрози, співробітництво.

Актуальність теми дослідження полягає в тому, що в епоху цифрових технологій стрімко розвивається транснаціональна кіберзлочинність. В умовах ведення гібридних воєн інструмент кібератак на інформаційні системи держав став одним із найбільш популярних методів злочинності. ЄС позиціонує себе як глобальний лідер, тому одним із важливих його завдань у світі є побудова миру та безпеки у інших країнах. Регіон Східного партнерства вже давно став пріоритетом зовнішньої політики для ЄС. Одним із пріоритетів політики об'єднання щодо країн Східного партнерства є забезпечення безпеки. В контексті поширення

© Абрат С. Б., 2024

засад цифрового компасу ЄС, інтеграції країн СХП до єдиного цифрового ринку ЄС важливим є забезпечення в державах регіону стійкості системи кібербезпеки. Особливо актуальним є співпраця у цьому напрямку між ЄС та країнами регіону в контексті гібридної війни РФ та великої кількості кібератак на національні інформаційні системи досліджуваних держав.

Методологія дослідження. Методологічною основою дослідження послугували низка наукових методів. Зокрема, за допомогою порівняльного методу було співставлено ступінь розвитку кібербезпеки у країнах Східного партнерства. Інституційний метод допоміг проаналізувати ключові формати співпраці між ЄС та країна Східного партнерства у сфері кіберзахисту. Метод прогнозування сприяв формуванню ключових сценарії посилення взаємодії ЄС та країн регіону у напрямі кібербезпеки. Використання методу узагальнення допомогло сформулювати ключові висновки на основі проаналізованих даних. Також вагомим у дослідження є аналіз Глобального індексу кібербезпеки, що допомогло встановити рівень кіберзахисту країн Східного партнерства. Аналіз тематики дослідження здійснюється крізь призму трансформаційної, розумної та м'якої сили ЄС. Союз активно впливає на країни Східного партнерства з метою проведення реформ, посилення демократії та безпеки у них. За допомогою інструментів «Єдиного цифрового ринку ЄС» та «Цифрового компасу ЄС» Союз намагається інтегрувати цифрові ринки країн регіону до свого, посилити їхню безпеку у інформаційному просторі.

Мета дослідження полягаєм у комплексному аналізі особливостей співпраці між ЄС та країнами Східного партнерства у сфері кібербезпеки, виокремленні ключових викликів та виробленні рекомендацій щодо посилення кіберстійкості досліджуваних держав.

Аналіз останніх досліджень і публікацій. Дослідження питання кібербезпеки є відносно новою проблематикою, що зумовлено стрімким розвитком цифрових технологій лише в останнє десятиріччя. Наявний брак комплексних досліджень щодо особливостей співпраці між ЄС та країнами Східного партнерства у сфері безпеки. Більшість наукових праць сфокусовані на вивченні питань безпеки кіберпростору виключно ЄС чи окремої країни-учасниці Ініціативи ЄС «Східне партнерство». Зокрема комплексно досліджено особливості співробітництва та ключові виклики в рамках Східного партнерства у цифровій сфері у монографії колективу українських авторів Ярини Турчин, Ольги Івасечко, Олега Цебенка, Ірини Сухорольської, Домініки Рослонь «Перспективи розвитку Ініціативи ЄС «Східне партнерство» в умовах сучасних геополітичних викликів» (Turchyn, Ivasechko, Tsebenko, Sukhorolska, Roslon, 2022. Ключові виклики у сфері безпеки аналізують українські дослідниці Ольга Івасечко та Аліна Яблонська у статті «Загрози миру та безпеці в країнах-адресатах Східного партнерства» (Ivasechko, Yablonska, 2022). Стан та тенденції кібербезпеки в Україні та ЄС комплексно проаналізовано у Інформаційно-аналітичний дайджесті «Кібербезпека в інформаційному суспільстві» за редакцією О. Довганя (Derzhavna naukova ustanova «Instytut informatsii, bezpeky i prava NAPrN Ukrainy», 2023). Інше аналітичне дослідження «Україна і Східне партнерство: візія 2025 року», здійснене ГО «Рада зовнішньої політики "Українська призма"» розглядає перспективи співпраці України та ЄС у цифровій сфері(НО «Rada zovnishnoi polityky "Ukrainska pryzma"», Ofis Fondu Konrada Adenauera v Ukrainiб 2021). Особливості політики кібербезпеки ЄС проаналізовано у статті зарубіжних дослідників

Агнеса Каспера та Влада Вернигори «Кібербезпека ЄС: стратегічний наратив кібердержави чи заплутана політика для локального спільного ринку?» (Kasper, Vernygora, 2021). Важливою основою нашого дослідження послугувало аналітичне дослідження в рамках програми EU4Digital «Керівні принципи з кібербезпеки для Східних країн-партнерів», де проаналізовані ключові особливості та стан кібербезпеки в країнах Східного партнерства (EU4Digital, 2020).

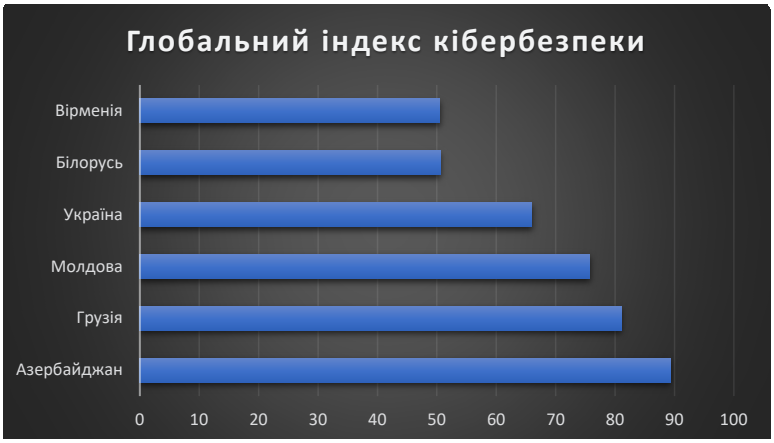
Виклад основного матеріалу. ЄС є лідером у впровадженні цифрових технологій. Ключовим пріоритетом для ЄС на сьогоднішній день є цифровізація усіх сфер суспільного життя. Варто зазначити, що ЄС має амбіції глобального лідерства, тому часто його внутрішні політики поширюються поза кордони держав-членів. В контексті глобальних амбіцій для досягнення цілей ЄС застосовує активно трансформаційну, м'яку та розумну силу для реалізації перетворень, європеїзації та демократизації країн, що не є членами об'єднання. В рамках цифрової політики об'єднання було прийнято «Цифровий компас ЄС», «Кіберстратегію ЄС», активно розвивається «Єдиний цифровий ринок» (Kasper, Vernygora, 2021). Усі ці політики активно імплементуються у зовнішній політиці ЄС. Пріоритетом для політики союзу є країни-учасниці Східного партнерство. На сьогодні регіон має надскладну геополітичну ситуацію, що впливають на європейську систему безпеки. В контексті зміцнення власної системи безпеки для ЄС важливо посилити систему кібербезпеки країн Східного партнерства. Одним із найбільших викликів є постійні кібератаки на цифрову систему ЄС та країн регіону СХП. В контексті цього важливим є пошук дієвих механізмів співпраці та посилення ролі ЄС у забезпеченні безпеки кіберпростору країн регіону.

Ключові інструменти впливу ЄС на посилення системи кібербезпеки країн Східного партнерства: 1. Безпекова ініціатива PESCO. Цифровий компас ЄС. 2. Стратегія кібербезпеки ЄС. 3. Проєкт Ради Європи CyberEast. 4. Програма EU4Digital. 5. Програма Horizon 2020. 6. Кібердипломатія ЄС. 7. Підвищення кіберстійкості в країнах Східного партнерства. 8. М'яка, трансформаційна та розумна сили ЄС в країнах Східного партнерства (Abrat, 2023; Council of Europe, 2019; EU4Digital, 2020).

Основні форми співпраці між ЄС та країнами Східного партнерства у сфері кіберзахисту: 1. Ініціатива ЄС «Східне партнерство». 2. Інтеграція країн Східного партнерства до єдиного цифрового ринку ЄС. 3. Співпраця у сфері розвитку та розбудова кіберпотенціалу. 4. Угоди про асоціацію. 5. Міжінституційна співпраця між профільними структурами. 6. Угоди про співпрацю у сфері кіберзахисту. 7. Обмін досвідом та інформацією. 8. Навчання кіберфахівців країн СХП у ЄС (Tsebenko, Ivasechko, Turchyn, Holoshchuk, 2022; Turchyn, Ivasechko, Tsebenko, Sukhorolska, Roslon, 2022).

З метою аналізу стану кібербезпеки в країнах Східного партнерства нами було проаналізовано Глобальний індекс кібербезпеки за 2021 рік (Діаграма 1) (European Commission, 2021).

Згідно аналізу даних можемо зазначити, що найбільш стійку систему безпеки кіберпростору мають Азербайджан (89,31) та Грузія (81,06). Дещо гірша система кібербезпеки в Республіки Молдова (75,78) та України (65,93). Досить слабкою є кібербезпека у Білорусі (50,57) та Вірменії (50,47). Можемо зробити висновки про значний розрив у стійкості кібербезпеки країн Східного партнерства. Варто зазначити, що рівень кібербезпеки у деяких країн регіону не завжди корелюється



Діаграма 1. Глобальний індекс кібербезпеки 2021

із євроінтеграційними досягненнями (Азербайджан). На основі аналізу Індексу кібербезпеки розроблено класифікацію за критерієм стійкості кіберзахисту, зокрема: держави із високим рівнем кібербезпеки (Азербайджан та Грузія); держави із прогресуючою системою кіберзахисту (Україна, Молдова); держави із слабкою системою кібербезпеки (Білорусь та Вірменія) (European Commission, 2021).

Цифрова сфера є пріоритетною у співпраці між ЄС та країнами Східного партнерства. Ключове місце у ній займає сфера кібербезпеки. В сучасних геополітичних умовах сфера цифровізації країн Східного партнерства має низку зовнішніх та внутрішніх викликів (таблиця 1) (Abrat, 2023; Ivasechko, Yablonska, 2022; Ratsiborynska, 2021).

Таблиця 1

Зовнішні та внутрішні виклики системі кібербезпеки держав СХП

Зовнішні виклики	Внутрішні виклики
Постійні кібератаки на країни регіону з боку Росії	Відсутність національної стратегії кібербезпеки в деяких країнах СХП
Відсутність стратегії кібербезпеки ЄС щодо цього регіону	Застарілість національного законодавства у сфері кібербезпеки
Геополітична напруженість в регіоні СХП	Стандарти країн СХП у сфері кібербезпеки не відповідають нормам ЄС
Транснаціональна кіберзлочинність	Низький рівень цифрової грамотності населення країн регіону
Швидкий розвиток кіберзлочинності	Прийняті стратегії кібербезпеки слабко імплементовуються
	Низький рівень цифровізації
Відсутність єдності країн СХП щодо інтеграції до ЄС	Брак кадрів у сфері кіберзахисту
	Обмеженість ресурсів у фінансуванні кіберзахисту
	Застарілі системи кіберзахисту

Аналіз таблиці показав, що кібербезпека країн Східного партнерства має значну кількість загроз, що зумовлює необхідність її посилення, зокрема через посилення співпраці із ЄС. Одним із найбільш загрозливих викликів є геополітична напруженість в регіоні та постійні кібератаки Росії на системи більшості країн-учасниць Східного партнерства. Не позбавлена ця сфера і внутрішніх викликів, серед яких найбільш значними є застарілість систем кіберзахисту, відсутність стратегій кібербезпеки або видимого прогресу їх імплементацій країнами Східного партнерства, відсутність фінансових ресурсів для покращення кіберінфраструктури.

Рекомендації щодо посилення співпраці між ЄС та країнами Східного партнерства у сфері кібербезпеки (Council of Europe, 2019; НО «Rada zovnishnoi polityky «Ukrainska pryzma»», 2021; Ukrainian Prism, 2022):

1. Посилення інтеграції країн регіону до ЄС.
2. Інтеграція країн регіону до Єдиного цифрового ринку ЄС.
3. Впровадження європейський стандартів та законодавства у цифровій сфері в країнах Східного партнерства.
4. Впровадження кращих практик ЄС у сфері кібербезпеки в країнах Східного партнерства.
5. Формування спільних центрів протидії кіберзагрозам.
6. Прийняття та імплементація національних стратегій кібербезпеки.
7. Спільна стратегія ЄС-країни Східного партнерства щодо протидії гібридним атакам РФ.
8. Формування за підтримки та контролю ЄС стійкої кіберполіції в країнах Східного партнерства.
9. Фінансування ЄС реформ національних систем кібербезпеки.
10. Підготовка фахівців у сфері кібербезпеки за стандартами ЄС та НАТО.

Потенційні сценарії зміцнення системи кіберзахисту країн Східного партнерства в контексті інтеграції до Єдиного цифрового ринку ЄС:

Сценарій 1. Повна інтеграція країн Східного партнерства до Єдиного цифрового ринку ЄС та включення у систему європейську систему кібербезпеки. Малоймовірний варіант, оскільки частина держав регіону не проявляє значних зрушень у євроінтеграційних бажаннях(Вірменія та Азербайджан), а Білорусь припинила у 2021 році співпрацю із ЄС.

Сценарій 2. Частина держав Східного партнерства інтегрується у цифровій сфері до ЄС. Високоймовірний варіант, оскільки країни «Асоційованого тріо» демонструють стрімке бажання інтегруватись до ЄС. В свою чергу об'єднання, в умовах сучасної гібридної війни Росії, зацікавлене у посиленні кіберстійкості та інтеграції цих країн.

Сценарій 3. Відбудуться дезінтеграційні процеси в країнах-учасницях Східного партнерства, що призведуть до зменшення впливу ЄС на цифрові ринки країн регіону. Малоймовірний варіант, оскільки Україна, Молдова та Грузія зробили значні євроінтеграційні потуги, а ЄС навряд чи дасть можливість Росії посилити свій геополітичний вплив у цих країнах.

Сценарій 4. Країни-учасниці Східного партнерства самостійно розвиватимуть власну стійку систему кібербезпеки та не потребуватимуть зовнішньої підтримки. Малоймовірний варіант, оскільки ці країни мають слабкий ресурсний потенціал та все ж залежні від зовнішньої підтримки.

Висновки дослідження. На сьогодні цифровий простір держав піддається великій кількості атак. З метою розвитку цифрових технологій кіберзлочинність стрімко зростає. ЄС є лідером у світі серед розвитку цифрових технологій, тому кібербезпека є пріоритетним напрямком їх внутрішньої та зовнішньої політики. Регіон Східного партнерства піддається постійним кібератакам, головно із сторони РФ. Посилення безпеки кіберпростору цих країн є важливим завданням для розвитку європейської системи безпеки. Пріоритетними форматами співпраці ЄС та країн Східного партнерства у сфері кібербезпеки є Ініціатива ЄС «Східне партнерство», програма EU4Digital. Аналіз Індексу кібербезпеки показав, що Азербайджан та Грузія є найбільш захищеними у сфері кібербезпеки. Найбільші проблеми із захистом цифрових даних є у Білорусі та Вірменії. Система кібербезпеки країн регіону має низку зовнішніх та внутрішніх викликів, серед яких кібератаки РФ, транснаціональна кіберзлочинність, відсутність єдності країн регіону щодо питання євроінтеграції, слабкість національних систем кіберзахисту, відсутність кіберстратегій у деяких країн СХП, відсутність ресурсів на посилення національної системи кібербезпеки. ЄС необхідно посилювати співпрацю з країнами регіону, формувати спільні координаційні структури, посилити фінансування розвитку цифрової інфраструктури в державах регіону, оскільки це напряму пов'язано із їхньою власною системою безпеки. Найбільш ймовірним варіантом є інтеграції України, Молдови та Грузії до Єдиного цифрового ринку ЄС та його кіберпростору, що в свою чергу посилить їх кібербезпеку. Перспективним виглядає також посилення співпраці ЄС із Вірменією у цьому напрямі.

References [Список використаної літератури]

Abrat, S. (2023). The security dimension of cooperation within the framework of the EU Initiative "Eastern Partnership", *International relations, public communications and regional studies,* 2(16), 6–20. Retrieved from: https://relint.vnu.edu.ua/index.php/relint/article/view/309/287 [in Ukrainian]. [Абрат С. Безпековий вимір співпраці в рамках Ініціативи ЕС «Східне парнерство». *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2023. Вип 2. Т.16. С. 6–20. URL: https://relint.vnu.edu.ua/index.php/relint/article/view/309/287 (дата звернення: 10.02.2024)].

Council of Europe (2019). *Cybercrime and cybersecurity strategies in the Eastern Partnership region.* Retrieved from: https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c [in English]. [Cybercrime and cybersecurity strategies in the Eastern Partnership region. *Council of Europe.* 2019. URL: https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c (дата звернення: 11.02.2024)].

State Scientific Institution "Institute of Information, Security and Law of the National Academy of Sciences of Ukraine (2023). *Cyber security in the information society: Informational and analytical digest* [ed. Dovhan, O.]. Kyiv. 11. 330 p. [in Ukrainian]. [Кібербезпека в інформаційному суспільстві. [за заг. Ред. О. Довганя]. *Інформаційно-аналітичний дайджест*. Київ: Державна наукова установа «Інститут інформації, безпеки і права НАПрН України». 2023. №.11. 330 с.].

EU4Digital (2020). *Cybersecurity guidelines for the Eastern Partner countries.* Retrieved from: https://eufordigital.eu/wp-content/uploads/2020/10/Cybersecurity-guidelines-for-the-Eastern-Partner-countries.pdf [in English]. [Cybersecurity guidelines for the Eastern Partner countries. *EU4Digital.* 2020. URL: https://eufordigital.eu/wp-content/uploads/2020/10/Cybersecurity-guidelines-for-the-Eastern-Partner-countries.pdf (дата звернення: 11.02.2024)].

European Commission (2021). *Global Cyber Security Index.* Retrieved from: https://composite-indicators.jrc.ec.europa.eu/explorer/explorer/indices/GCI/global-cyber-security-index [in English]. [Global Cyber Security Index. *European Commission.* 2021. URL: https://composite-indicators.jrc.ec.europa.eu/explorer/explorer/indices/GCI/global-cyber-security-index (дата звернення: 13.02.2024)].

Ukraine and the Eastern Partnership: the vision of 2025. NGO "Foreign Policy Council "Ukrainian Prism", Office of the Konrad Adenauer Foundation in Ukraine. Kyiv. 66 p. [in Ukrainian]. [Україна і Східне партнерство: візія 2025 року. *ГО «Рада Зовнішньої політики «Українська Призма»», Офіс Фонду Конрада Аденауера в Україні.* Київ. 66 с.]

Ivasechko, O., & Yablonska, A. (2022). Threats to peace and security in the recipient countries of the Eastern Partnership (2014-2022). *Regional study*. 31. 91–96. Retrieved from: http://regionalstudies.uzhnu.uz.ua/archive/31/17.pdf [in Ukrainian]. [Івасечко О., Яблонська А. Загрози миру та безпеки в країнах-адресатах Східного партнерства (2014-2022 рр.). *Регіональні студії*. №31. С. 91–96. URL: http://regionalstudies.uzhnu.uz.ua/archive/31/17.pdf (дата звернення: 15.02.2024)].

Kasper, A., & Vernygora, V. (2021). The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market? *Cuadernos Europeos de Deusto*. 65. 29–71. Retrieved from: http://dx.doi.org/10.18543/ced-65-2021pp29-71 [in English]. [Kasper A., Vernygora V. The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market? *Cuadernos Europeos de Deusto*. № 65. P. 29-71. URL: http://dx.doi.org/10.18543/ced-65-2021pp29-71 (дата звернення: 15.02.2024)].

Ratsiborynska, V. (2021). EU-NATO and the Eastern Partnership countries against hybrid threats: From the EU Global Strategy till the war in Ukraine. *Horizon Insights*. 4(4), 20–31. [in English]. [Ratsiborynska V. EU-NATO and the Eastern Partnership countries against hybrid threats: From the EU Global Strategy till the war in Ukraine. *Horizon Insights*. №4. Т.4. С. 20–31].

Tsebenko, O., Ivasechko, O., Turchyn, Y., & Holoshchuk, R. (2022). EU Digital Market: the Future of Eastern Partnership. *SCIA-2022 CEUR Workshop Proceedings*. 3296. 4–17. Retrieved from: https://ceur-ws.org/Vol-3296/paper1.pdf [in English]. [Tsebenko O., Ivasechko O., Turchyn Y., Holoshchuk R. EU Digital Market: the Future of Eastern Partnership. *SCIA-2022 CEUR Workshop Proceedings*. 2022. №3296. С. 4–17. URL: https://ceur-ws.org/Vol-3296/paper1.pdf (дата звернення: 16.02.2024)].

Turchyn, Ya., Ivasechko, O., Tsebenko, O., Sukhorolska, I., & Roslon, D. (2022). *Prospects for the development of the EU initiative «Eastern Partnership» in the conditions of geopolitical challenges: monograph*. Lviv: Lviv Polytechnic Publishing House, 224 p. [in Ukrainian]. [Турчин Я., Івасечко О., Цебенко О., Сухорольська І., Рослонь Д. Перспективи розвитку Ініціативи ЄС «Східне паротнерство» в умовах геополітичних викликів: монографія. Львів: видавництво Львівської політехніки. 2022. 224 с.]

Ukrainian Prism (2022). *Resilient digital transformation in the Eastern Partnership region: State of play in 2022 and recommendations*. Retrieved from: https://prismua.org/en/english-resilient-digital-transformation-in-the-eastern-partnership-region-state-of-play-in-2022-and-recommendations/ [in English]. [Resilient digital transformation in the Eastern Partnership region: State of play in 2022 and recommendations. *Ukrainian Prism*. 2022. URL: https://prismua.org/en/english-resilient-digital-transformation-in-the-eastern-partnership-region-state-of-play-in-2022-and-recommendations/ (дата звернення: 19.02.2024)].

Стаття надійшла до редакції 27.02.2024

Abrat S. B.
Department of Political Science and International Relations
Lviv Polytechnic National University
r. 314, 4 n.k., Mytropolyta Andreia str., 5, Lviv, 79016, Ukraine

COOPERATION OF THE EU AND EASTERN PARTNERSHIP COUNTRIES IN THE FIELD OF CYBERSECURITY: CHALLENGES AND PROSPECTS

Summary

The article analyzes the peculiarities of cooperation between the EU and the Eastern Partnership countries in the field of cybersecurity. The main formats of cooperation between the EU and the countries of the region in the field of cyber defense are highlighted. The key EU instruments for strengthening the cybersecurity system of the Eastern Partnership countries are analyzed. Among them are the EU's Eastern Partnership Initiative, the EU's "EU4Digital" program, and the Association Agreements with Ukraine, Moldova, and Georgia. The Global Cybersecurity Index of the countries of the region is analyzed. It was found that Azerbaijan and Georgia have the greatest protection of cyberspace, and Armenia and Belarus have the least. Based on the analysis of the Cybersecurity Index, a classification on the criterion of cybersecurity resilience is developed, in particular: states with a high level of cybersecurity (Azerbaijan and Georgia); states

with a progressive cybersecurity system (Ukraine, Moldova); states with a weak cybersecurity system (Belarus and Armenia). The key internal and external challenges to the cybersecurity system of the Eastern Partnership countries are analyzed. It is established that there are a number of external challenges, including the geopolitical complexity of the region, hybrid attacks by the Russian Federation, and the lack of desire of some EaP countries to integrate into the EU. The internal challenges to the cybersecurity system of the studied countries include weakness or lack of implementation of cybersecurity strategies, outdated cybersecurity systems, lack of resources to improve the cybersecurity system, and low intensity of implementation of European standards. Recommendations are also made to strengthen cooperation between the EU and the Eastern Partnership countries in the field of cyber defense and countering hybrid challenges. In particular, the integration of the countries of the region into the EU's Digital Single Market should be strengthened, which will allow for a more reliable cyber defense system. The prospects and possible scenarios for strengthening EU-Eastern Partnership countries cooperation in the field of cybersecurity have been considered.
Key words: EU, Eastern Partnership, cybersecurity, cyber threats, cooperation.