Проблеми національної економіки

УДК 330.341.1:330.47

Піжук Ольга Іванівна
кандидат економічних наук, доцент,
доцент кафедри економіки підприємства
Університет державної фіскальної служби України
Пижук Ольга Ивановна
кандидат экономических наук, доцент,
доцент кафедры экономики предприятия
Университет государственной фискальной службы Украины
Pizhuk Olga
PhD, Associate Professor,
Associate Professor of the Economics of the Enterprise Department
University of the State Fiscal Service of Ukraine
ORCID: 0000-0002-5802-1053

КІБЕРБЕЗПЕКА ЯК ФАКТОР ПРИСКОРЕННЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ УКРАЇНИ
КИБЕРБЕЗОПАСНОСТЬ КАК ФАКТОР УСКОРЕНИЯ ТЕМПОВ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ЭКОНОМИКИ УКРАИНЫ
CYBERSECURITY AS AN ACCELERATION FACTOR OF THE DIGITAL TRANSFORMATION OF UKRAINE'S ECONOMY

Анотація. *Ключовою гіпотезою даного наукового дослідження є припущення, що гарантування безпеки в кіберпросторі може пришвидшити процеси цифрової трансформації економіки в будь якій країні світу. З цією метою у статті уточнено сутність поняття кіберпростору, що розглядається як глобальне інформаційне середовище, сформоване сукупністю взаємозалежних елементів інформаційно-технічної інфраструктури, а саме інформаційних і телекомунікаційних*

мереж й комп'ютерних систем, які призначені для зберігання, обробки, модифікації й обміну даними, а також з'ясовано значення кібербезпеки у процесі цифрової трансформації економіки. Проаналізовано рівень готовності країн з різним рівнем соціально-економічного розвитку до захисту даних в кіберпросторі за «Глобальним індексом кібербезпеки» (Global Cybersecurity Index, GCI) і «Національним індексом кібербезпеки» (National Cyber Security Index, NCSI), розкрито особливості їх змісту. Проаналізовано рівень цифрового розвитку (Digital Development Level – DDL) високорозвинених країн і країн з трансформаційною економікою крізь призму Індексу розвитку ІКТ (IDI) та Індексу мережевої готовності (NRI). Визначено сильні та слабкі сторони як системи кібербезпеки так і рівня цифрового розвитку України. Зосереджено увагу на визначенні впливу кібербезпеки на збільшення можливостей для використання в економічних процесах сучасних цифрових технологій, що у підсумку може прискорити цифрову трансформацію економіки. Зроблено висновки про те, що підвищення рівня кібербезпеки є необхідним але не завжди достатнім фактором прискорення цифрової трансформації економіки. Запропоновано проведення наукових досліджень з проблем формування дієвих засобів кіберзахисту у правовому, організаційному і технічному аспектах, започаткувати інформаційні та навчальні кампанії щодо підвищення обізнаності та набуття відповідних навичок, зокрема для формування кадрового резерву у сфері кібербезпеки; а також, посилення зусиль держави у напрямі розробку та імплементації ефективних систем кібербезпеки на рівні держави, бізнесових організацій та громадян.

Ключові слова: *кіберпростір, цифровий розвиток, система кібербезпеки, кіберзахист економічних систем.*

Аннотация. *Ключевой гипотезой данного научного исследования является предположение, что обеспечение безопасности в*

киберпространстве может ускорить процессы цифровой трансформации экономики в любой стране мира. С этой целью в статье уточнена сущность понятия киберпространства, что рассматривается как глобальное информационное пространство, сформированное совокупностью взаимозависимых элементов информационно-технической инфраструктуры предназначенной для хранения, обработки, модификации и обмена данными, а также выяснено значение кибербезопасности в процессе цифровой трансформации экономики. Проанализирован уровень готовности стран с различным уровнем социально-экономического развития к защите данных в киберпространстве за «Глобальным индексом кибербезопасности» (Global Cybersecurity Index) и «Национальным индексом кибербезопасности» (National Cybersecurity Index), раскрыты особенности их содержания. Проанализирован уровень цифрового развития (Digital Development Level) высокоразвитых стран и стран с трансформационной экономикой сквозь призму «Индекса развития ИКТ» (IDI) и «Индекса сетевой готовности» (NRI). Определены сильные и слабые стороны как системы кибербезопасности, так и уровня цифрового развития Украины. Сосредоточено внимание на определении влияния кибербезопасности на увеличение возможностей для использования в экономических процессах современных цифровых технологий, что в итоге может ускорить цифровую трансформацию экономики. Сделаны выводы о том, что повышение уровня кибербезопасности необходимо, но не всегда есть достаточным фактором ускорения цифровой трансформации экономики. Предложено проведение научных исследований по проблемам формирования действенных способов киберзащиты в правовом, организационном и техническом аспектах; создание информационных и учебных кампаний по повышению осведомленности и приобретению соответствующих навыков, в частности для формирования кадрового резерва в сфере

кибербезопасности; направление усилий государства на разработку и имплементацию эффективных систем кибербезопасности на уровне государства, бизнес организаций и граждан.

Ключевые слова: *киберпространство, цифровой развитие, система кибербезопасности, киберзащита экономических систем.*

Summary. *The key hypothesis of the research is the assumption that security in cyberspace can accelerate a process of the economy's digital transformation in any country in the world. Our goal in this article to clarify the essence of cyberspace's concept, which is considered as a global information environment, formed by a set of interdependent elements of the information technology infrastructure, namely information and telecommunications networks and computer systems for storage, processing, modification, and exchange data, as well as the importance of cybersecurity in the process of the digital transformation of the economy. The degree of readiness of countries with different levels of socio-economic development to protecting data in cyberspace according to the Global Cybersecurity Index (GCI) and the National Cybersecurity Index (NCSI) is analyzed. Using the ICT Development Index (IDI) and the Network Readiness Index (NRI), the level of digital development of highly developed countries and countries with transformational economies is analyzed. The strengths and weaknesses of both the cybersecurity system and the level of digital development of Ukraine have been identified. The focus is on determining the impact of cybersecurity on increasing opportunities for the use of modern digital technologies in economic processes, which may ultimately accelerate the economy's digital transformation. It is concluded, increasing the level of cybersecurity is a necessary but not always sufficient factor in accelerating the economy's digital transformation. According to the results of the study, it is proposed: firstly, to research the formation of effective means of cyberdefense in legal, organizational, and technical aspects; secondly, to launch*

information and training campaigns to raising awareness and acquire relevant skills, in particular, to build a human resources reserve in the field of cybersecurity; thirdly, to strengthen the state's efforts to develop and implement effective cybersecurity systems at the level of the state, business organizations and citizens.

Key words: *cyberspace, digital development, cybersecurity system, cyber protection of economic systems.*

Постановка проблеми. Пришвидшення процесів цифрової трансформації економіки, де важливим ресурсом є інформація, неможливе без розвитку систем безпеки кіберпростору. Відповідно до міжнародного стандарту, кіберпростір – це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення та послуг в Інтернеті за допомогою технологічних пристроїв і мереж, що під'єднані до них, якого не існує в будь-якій фізичній формі. Якщо розглядати кіберпростір як словосполучення «кібернетичний простір», то кіберпростір – це простір (територія), який створений і працює на основі принципів, методів кібернетики (науки про загальні закони одержання, зберігання, передачі та обробки інформації) [1, с. 216]. На загальнодержавному рівні визначення кіберпростору вперше визначено в доповіді дослідницької служби конгресу США у 2001 році, де останнє визначено як «всеохоплююча множина зв'язків між людьми, створена на основі комп'ютерів і телекомунікацій незалежно від фізично визначеної географії» [2].

Аналіз останніх досліджень і публікацій. Проблемним аспектам становлення системи кібербезпеки присвятили свої наукові праці зарубіжні та вітчизняні вчені, зокрема: О. Баранов [3], В. Буряк [4], М. Гуцалюк [5], М. Гончар [6], М. Грановський, І. Грабар, Р. Грищук, К. Молодецька [7] В. Дудикевич, Г. Микитин, А. Ребець [8], Ю. Кінзерський [9], Д. Монін [10],

І. Рус [11], О. Ткаченко, К. Ткаченко [12], В. Фурашев [13], та ін. Водночас недостатньо вивченими залишаються питання впливу кібербезпеки на процеси цифрової трансформації економіки.

Формулювання цілей статті. Метою статті є виявлення впливу рівня розвитку системи кібербезпеки в країні на збільшення можливостей для використання в економічних процесах сучасних цифрових технологій, що у підсумку може прискорити цифрову трансформацію економіки.

Виклад основного матеріалу дослідження. У даному науковому дослідженні кіберпростір розглядається як глобальне інформаційне середовище, сформоване сукупністю взаємозалежних елементів інформаційно-технічної інфраструктури, а саме інформаційних і телекомунікаційних мереж й комп'ютерних систем, які призначені для зберігання, обробки, модифікації та обміну даними. У даному визначенні важливим є уточнення щодо призначення інформаційно-технічної інфраструктури, зважаючи на те, що найчастіше кібератаки проводяться з метою отримання доступу до конфіденційної інформації, її зміни або знищення. Подібні дії здатні завдати матеріальних збитків як окремим підприємствам, через втрату або спотворення стратегічно важливої інформації, так і державі – кібератаки можуть спровокувати техногенні катастрофи, збитки цивільної, фінансової та військової інфраструктури. Зважаючи на зазначене гарантування кібербезпеки є надзвичайно актуальним завданням сучасності, а заходи з протидії викликам і загрозам у цій царині є невід'ємною складовою технічного прогресу. У свою чергу, під кібербезпекою як правило розуміють сукупність заходів, реалізація яких дозволяє забезпечити захист систем, мереж і різних програмних додатків від кібератак [9].

З метою моніторингу й порівняльної оцінки ступеня готовності країн до захисту даних у кіберпросторі використовуються міжнародні рейтинги, найбільш авторитетними з яких є «Національний індекс кібербезпеки»

(National Cyber Security Index, NCSI) та «Глобальний індекс кібербезпеки» (Global Cybersecurity Index, GCI) розроблений Міжнародним союзом електрозв'язку (International Telecommunication Union, ITU). Ці індекси оцінюють рівень ризику для корпоративної, промислової та урядової інформаційної інфраструктури через певний спектр кіберзагроз. Так, базисом формування Індексу NCSI є такі ключові кіберзагрози як відмова від електронних послуг – послуги недоступні; порушення цілісності даних – несанкціоноване внесення змін; порушення конфіденційності даних – оприлюднення таємниці. Зазначені загрози безпосередньо впливають на нормальне функціонування національних інформаційно-комунікаційних систем і, через ІКТ-системи, електронних послуг (у тому числі критичних). Для управління цими кіберзагрозами країна повинна володіти можливостями для забезпечення базового рівня та розвитку кібербезпеки, а також управління інцидентами.

Рейтинг NCSI зосереджений на вимірюваних аспектах кібербезпеки, впроваджених центральними урядами країн, а саме: чинне законодавство – нормативно-правові акти (положення, накази тощо); розвиток інституцій (діючі організації, управління тощо); формати співпраці (комітети, працюючі групи тощо); результати (політики, технології, веб-сайти, програми тощо). Відмінною рисою даного індексу є те, що рейтинги країн базуються на публічних доказах, а саме: правові акти, офіційні документи, офіційні веб-сайти. Оцінка NCSI показує відсоток, отриманий країною від максимального значення показників. Максимальний показник NCSI завжди 100 (100%) незалежно від того, додаються чи знімаються показники.

Глобальний індекс кібербезпеки (Global Cybersecurity Index, GCI) [14], базується на основі відповідей респондентів про стан таких компонентів безпеки в кіберпросторі як законодавство, технічна, організаційна складові, а також можливості підвищення їх потенціалу та

кооперації. Детальний аналіз індексу дозволяє зробити висновок про те, що законодавча база є основою забезпечення кібербезпеки. Правовий аспект вимірюється на основі кількості відповідних інститутів і структур, відповідальних за кібербезпеку. Оскільки забезпечення останньої неможливо здійснити без відповідних технічних навичок для виявлення кібератаки і реагування на неї важливою є оцінка технічних елементів. Процес оцінювання здійснюється на основі цілого ряду практичних механізмів, що використовуються для боротьби з кіберзлочинністю.

Наявність національної стратегії, адекватної до вирішуваних завдань моделі управління та органів нагляду, укомплектованих фахівцями, які професійно займаються даною проблемою є важливими елементами забезпечення ефективного функціонування системи кібербезпеки. Все це є основою організаційної складової кібербезпеки на національному рівні. Можливості підвищення рівня безпеки в кіберпросторі оцінюються виходячи з кількості досліджень та розробок у даній сфері, наявності освітніх і навчальних програм, а також сертифікованих фахівців та установ державного сектора. Забезпечення ефективності в боротьбі з кіберзлочинністю також передбачає розширення співпраці. Національне та міжнародне співробітництво оцінюються на основі кількості партнерств, основаних на співпраці по обміну інформацією.

На додаток до шкали NCSI та GCI, таблиця індексів (табл. 1) відображає рівень цифрового розвитку (Digital Development Level, DDL). DDL розраховується як середній відсоток Індексу розвитку ІКТ (IDI) та Індексу мережевої готовності (NRI).

Таблиця 1

Рейтинг країн за індексами кібербезпеки та рівнем цифрового розвитку

Національний індекс кібербезпеки, 2019		Глобальний індекс кібербезпеки, 2018 [14]		Рівень цифрового розвитку (DDL)*, 2019	
Країна	Оцінка	Країна	Оцінка	Країна	Оцінка
Високорозвинені країни					
Франція	83,12	Великобританія	93,1	Швейцарія	85,13
Німеччина	80,52	США	92,6	Великобританія	83,96
США	79,22	Франція	91,8	Норвегія	83,78
Великобританія	77,92	Норвегія	89,2	Люксембург	83,06
Швейцарія	76,62	Австралія	89,2	США	82,33
Норвегія	62,34	Люксембург	89,0	Японія	82,15
Японія	62,34	Японія	88,0	Німеччина	81,95
Люксембург	62,34	Китай	82,8	Австралія	80,49
Австралія	59,74	Німеччина	84,9	Франція	79,06
Китай	35,06	Швейцарія	78,8	Китай	58,00
Країни з трансформаційною економікою					
Чехія	92,21	Грузія	85,7	Білорусь	75,5
Словаччина	83,12	Росія	83,6	Чехія	69,37
Румунія	71,43	Польща	81,5	Росія	67,49
Польща	70,13	Угорщина	81,2	Словаччина	66,73
Росія	64,94	Словаччина	72,9	Польща	66,59
Угорщина	64,94	Болгарія	72,1	Угорщина	66,08
Україна	**63,64**	**Україна**	**66,1**	Болгарія	63,59
Білорусь	53,25	Білорусь	57,8	Румунія	61,69
Грузія	53,25	Чехія	56,9	Грузія	59,66
Болгарія	51,95	Румунія	56,8	**Україна**	**58,10**

Джерело: https://ncsi.ega.ee/compare/

Порівняння високорозвинених країн і країн з трансформаційною економікою за відповідними індексами цифрового розвитку і кібербезпеки, взаємозв'язок між останніми стає очевидним. Так, згідно даних табл. 1, відповідно до рейтингу, побудованого на основі розрахунків індексу кібербезпеки NCSI-2019 Україна займає 29 сходинку. Сильними сторонами нашої країни було відзначено напрацювання у сфері запровадження політики кібербезпеки, захисту персональних даних і боротьби з кіберзлочинністю. Серед слабких слід відмітити позиції із управління інцидентами та кіберкризами, а також захисту електронних сервісів, аналізу та інформування громадськості про кіберзагрози.

Великобританія стала лідером рейтингу Глобального індексу Кібербезпеки у 2018 році зі значенням показника 0,931 бала, в той час як у 2017 році займала аж 12 сходинку. Другу сходинку рейтингу зберегли за собою США із оцінкою 0,926 бала, третю – Франція (0,918 бала), якій вдалося піднятися із восьмої позиції у порівнянні з 2017 роком. Україна за даними 2018 року посіла 54 місце з оцінкою 66,1 бала, випередивши такі країни з трансформаційною економікою як Білорусь (57,8 бала), Чехія (56,9 балів), Румунія (56,8 балів). Підвищення України у рейтингу на п'ять позицій у порівнянні із 2017 роком зумовлене ефективною роботою команди реагування на комп'ютерні надзвичайні події CERT-UA, що працює у тісній взаємодії з Cisco Talos Intelligence Group та іншими державами-членами CERT щодо питань подолання наслідків кібератак на критично важливу інформаційну інфраструктуру і виявлення причин та обставин таких інцидентів. CERT-UA також допомагає усунути загрози безпеці приватного сектору України та іноземних партнерів. Відповідно до закону «Про основні засади забезпечення кібербезпеки України», прийнятого у 2017 році, CERT-UA та Центр реагування на кіберзлочини координують заходи оперативного реагування на кібератаки, а також контролюють впровадження контрзаходів, що передбачають мінімізацію уразливості систем зв'язку. Україна бере участь у роботі Агентства ЄС з кібербезпеки, Європейського центру з досліджень і компетенції в сфері кібербезпеки, а також у навчаннях із реалізації Спільної оперативної схеми реагування ЄС і держав-членів на кібератаки [9].

Станом на 2019 рік відповідно до Індексу розвитку ІКТ (IDI), Індексу мережевої готовності (NRI) та Національного індексу цифрової трансформації головними гравцями світового ринку інформаційних технологій в умовах глобалізації є Японія, європейські країни – Норвегія, Швейцарія, Великобританія та Люксембург, а також Сполучені Штати Америки, економікам яких притаманний високий рівень цифрового

розвитку. Україна відповідно до Звіту Міжнародного союзу електрозв'язку «Вимірювання інформаційного суспільства 2019», який представляє рейтинг країн за Індексом розвитку ІКТ (ICT Development Index) посіла 79 місце із 176, за Індексом мережевої готовності (NRI) – 64 місце. Серед причин невисокого місця України у рейтингу найбільш значущою є нерівномірність розвитку та впровадження ІКТ в різних сферах життєдіяльності та окремих регіонах.

З огляду на те, що ключовою гіпотезою даного дослідження є припущення: забезпечення безпеки в кіберпросторі може сприяти підвищенню рівня цифрового розвитку в країнах, нами використано інструментарій кореляційно-регресійного аналізу, який дозволив виявити суттєвість зв'язку між національним індексом кібербезпеки та комплексним показником рівня цифрового розвитку (табл. 2).

Таблиця 2

Регресійний аналіз між індексом NCSI і DDL у розрізі розвинених країн і країн з трансформаційною економікою, 2019

Регресійна статистика		Дисперсійний аналіз			
		Критерії	*Регресія*	*Залишок*	*Всього*
Високорозвинені країни					
Множинний R	0,886738	*df*	1	8	9
R-квадрат	0,786305	*SS*	1520,149	413,1326	1933,281
Нормований R-квадрат	0,759593	*MS*	1520,149	51,64158	
Стандартна похибка	7,186207	*F*	29,43652		
Спостереження	10	*Значущість F*	0,000627		
Країни з трансформаційною економікою					
Множинний R	0,964001	*df*	1	8	9
R-квадрат	0,929298	*SS*	1439,57131	109,523334	1549,0946
Нормований R-квадрат	0,920461	*MS*	1439,57131	13,6904167	
Стандартна похибка	3,700056	*F*	105,151752		
Спостереження	10	*Значущість F*	7,03E-06		

Джерело: розраховано автором

За даними таблиці значення множинного коефіцієнта кореляції для високорозвинених країн становить 0,8867, а для країн з трансформаційною економікою – 0,9640, що свідчить про високу та дуже високу тісноту зв'язку між досліджуваними масивами даних (шкала Чеддока). Коефіцієнт детермінації (R-квадрат) для високрозвинених країн складає 0,786, або 78,6%, а для країн з трансформаційною економікою – 0,929, або 92,9%. Це означає, що розрахункові параметри моделі на 78,6% і 92,9% пояснюють залежність між досліджуваними параметрами, також демонструючи тісний зв'язок між змінними. Якщо ж розраховувати коефіцієнт детермінації для всіх досліджуваних країн, то він є значно меншим і дорівнює 0,3856 або 38,56 % (табл. 3).

Таблиця 3

Регресійний аналіз між індексом NCSI і DDL в загальній кількості респондентів по всіх досліджуваних країнах, 2019

Регресійна статистика		Дисперсійний аналіз			
		Критерії	*Регресія*	*Залишок*	*Всього*
Високорозвинені країни					
Множинний R	0,620945	*df*	1	18	19
R-квадрат	0,385572	*SS*	1344,776	2142,966	3487,742
Нормований R-квадрат	0,351437	*MS*	1344,776	119,0537	
Стандартна похибка	10,91117	*F*	11,29554		
Спостереження	20	*Значущість F*	0,00348		

Джерело: розраховано автором

Так, регресійний аналіз між національним індексом кібербезпеки NCSI і рівнем цифрового розвитку (DDL) за 2019 рік, в загальній кількості спостережень рівних 20 досліджуваних країн, за шкалою Чеддока свідчить про помітну тісноту зв'язку між досліджуваними масивами даних із значенням множинного коефіцієнта кореляції 0,6209. Разом з тим, R-квадрат, величина якого < 0,6 вказує на те, що точність апроксимації є недостатньою і модель вимагає введення нових незалежних змінних.

Тобто, підвищення рівня кібербезпеки не завжди є достатнім для забезпечення розвитку цифрової економіки.

Висновки та перспективи. Таким чином, як свідчать результати аналізу розвиток цифрової економіки неможливий без посилення кібербезпеки, а тому підвищення останньої неминуче веде до прискорення цифрової трансформації економіки. Зважаючи на це кібербезпека стає сьогодні важливим фактором розвитку цифрової економіки, розширення електронної взаємодії учасників ринку, впровадження елементів блокчейна, масштабне використання нових технологій виводить на перший план питання підвищення конкурентоспроможності вітчизняної фінансової системи, забезпечення її безпеки як об'єкта критичної інфраструктури. Важливими напрямами посилення кібербезпеки в Україні можуть бути: по-перше, проведення наукових досліджень щодо формування ефективних засобів кіберзахисту в юридичному, організаційному та технічному аспектах; по-друге, впровадження інформаційних і навчальних кампаній з метою підвищення обізнаності та набуття відповідних навичок, зокрема для формування кадрового резерву у сфері кібербезпеки; по-третє, посилити зусилля держави у напрямах розробки та впровадження ефективних систем кібербезпеки на рівні держави, бізнесових організацій та громадян.

Література

1. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності / О.В. Манжай // Право і Безпека. 2009. № 4. С. 215-219.
2. Паршин С. А., Горбачев Ю. Е., Кожанов Ю. А. Кибервойны – реальная угроза национальной безопасности. М.: Изд-во КРАСАНД, 2011.
3. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» // Правова інформатика. 2014. № 2(42). С. 54-62.

4. Буряк В.В. Цифровая экономика, хактивизм и кибербезопасность. Симферополь: ИП Зуева Т.В., 2019. 140 с.
5. Гуцалюк М.В. Оцінка реалізації стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик // Інформація і право. 2019. № 2(29). С. 90-99.
6. Грабар І. Г. Грищук Р. В., Молодецька К. В. Безпекова синергетика: кібернетичний та інформаційний аспекти : моногр. Житомир, 2019. 279 с.
7. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія. Київ, 2019. 175 с.
8. Дудикевич В. Б., Микитин Г. В., Ребець А. І. Квінтесенція інформаційної безпеки кіберфізичної системи // Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі. 2018. № 887. С. 58–68.
9. Кіндзерський Ю.В. Кібербезпека і становлення цифрової економіки: проблеми взаємозв'язку // Науковий журнал Економічний вісник Національного гірничого університету, 2020. №. С. 18-27.
10. Монін Д. Ризики й виклики нового часу // Дзеркало тижня. 2020. 5 вересня. URL: https://zn.ua/ukr/macrolevel/riziki-j-vikliki-novoho-chasu.html (Дата звернення: 7 вересня 2020 р.).
11. Rus I. Study of cybersecurity issues. Studia universitatis petru maior series oeconomica. 2017. Vol. 1. PP. 1-16.
12. Ткаченко О., Ткаченко К. Кіберпростір і кібербезпека: проблеми, перспективи, технології // Цифрова платформа: інформаційні технології в соціокультурній сфері. 2018. Вип. 1. С. 75–86.
13. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право. 2012. № 2(5). С. 162-175.

14. ITU. Global Cybersecurity Index (GCI), 2018. URL: www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_GlobalCybersecurity-Index-EV5_print_2.pdf (Дата звернення: 11.09.2020)

References

1. Manzhaj O.V. Vikoristannya kiberprostoru v operativno-rozshukovij diyalnosti / O.V. Manzhaj // Pravo i Bezpeka. 2009. № 4. S. 215-219.
2. Parshin S. A., Gorbachev Yu. E., Kozhanov Yu. A. Kibervojny – realnaya ugroza nacionalnoj bezopasnosti. M.: Izd-vo KRASAND, 2011.
3. Baranov O.A. Pro tlumachennya ta viznachennya ponyattya «kiberbezpeka» // Pravova informatika. 2014. № 2(42). S. 54-62.
4. Buryak V.V. Cifrovaya ekonomika, haktivizm i kiberbezopasnost. Simferopol: IP Zueva T.V., 2019. 140 s.
5. Gucalyuk M.V. Ocinka realizaciyi strategiyi kiberbezpeki Ukrayini z urahuvannyam dosvidu yevropejskih i svitovih praktik // Informaciya i pravo. 2019. № 2(29). S. 90-99.
6. Grabar I. G. Grishuk R. V., Molodecka K. V. Bezpekova sinergetika: kibernetichnij ta informacijnij aspekti : monogr. Zhitomir, 2019. 279 s.
7. Gonchar S. F. Ocinyuvannya rizikiv kiberbezpeki informacijnih sistem ob'yektiv kritichnoyi infrastrukturi : monografiya. Kiyiv, 2019. 175 s.
8. Dudikevich V. B., Mikitin G. V., Rebec A. I. Kvintesenciya informacijnoyi bezpeki kiberfizichnoyi sistemi // Visnik Nacionalnogo universitetu «Lvivska politehnika». Informacijni sistemi ta merezhi. 2018. № 887. S. 58–68.
9. Kindzerskij Yu.V. Kiberbezpeka i stanovlennya cifrovoyi ekonomiki: problemi vzayemozv'yazku // Naukovij zhurnal Ekonomichnij visnik Nacionalnogo girnichogo universitetu, 2020. №. S. 18-27.

10. Monin D. Riziki j vikliki novogo chasu // Dzerkalo tizhnya. 2020. 5 veresnya. URL: https://zn.ua/ukr/macrolevel/riziki-j-vikliki-novoho-chasu.html (Data zvernennya: 7 veresnya 2020 r.).
11. Rus I. Study of cybersecurity issues. Studia universitatis petru maior series oeconomica. 2017. Vol. 1. RP. 1-16.
12. Tkachenko O., Tkachenko K. Kiberprostir i kiberbezpeka: problemi, perspektivi, tehnologiyi // Cifrova platforma: informacijni tehnologiyi v sociokulturnij sferi. 2018. Vip. 1. S. 75–86.
13. Furashev V.M. Kiberprostir ta informacijnij prostir, kiberbezpeka ta informacijna bezpeka: sutnist, viznachennya, vidminnosti // Informaciya i pravo. 2012. № 2(5). S. 162-175.
14. ITU. Global Cybersecurity Index (GCI), 2018. URL: www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_GlobalCybersecurity-Index-EV5_print_2.pdf (Data zvernennya: 11.09.2020)