УДК 330.341.1:330.47 https://doi.org/10.33271/ebdut/71.018

КІБЕРБЕЗПЕКА ТА СТАНОВЛЕННЯ ЦИФРОВОЇ ЕКОНОМІКИ: ПРОБЛЕМИ ВЗАЄМОЗВ'ЯЗКУ

Ю. В. Кіндзерський, д. е. н, провідний науковий співробітник ДУ «Інститут економіки та прогнозування НАН України», vkpp@ukr.net, https://orcid.org/0000-0002-4432-6526

Методологія дослідження. Методологічною основою дослідження стали загально-наукові та спеціальні методи пізнання процесів і явищ цифрової трансформації економіки: статистичні методи – для обробки даних при оцінці рівня цифрової трансформації економіки; експертних оцінок – для визначення факторів впливу на розвиток цифрової економіки; кореляційного аналізу – при встановленні взаємозв'язку між детермінантами та масштабами цифровізації економіки.

Результати. Розкрито значення кібербезпеки у формуванні цифрової економіки. Проаналізовано рівень готовності країн до захисту даних у кіберпросторі за «Глобальним індексом кібербезпеки» (Global Cybersecurity Index, GCI) та «Національним індексом кібербезпеки» (National Cyber Security Index, NCSI), розкрито особливості їх складових. Акцентовано увагу на оцінці впливу кібербезпеки на рівень розвитку цифрової економіки. Виявлено проблему волатильності взаємозв'язку між кібербезпекою та рівнем цифрового розвитку крізь призму показників розвитку ІКТ і мережевої готовності. Виявлено, що підвищення рівня кібербезпеки неминуче веде до прискорення розвитку цифрової економіки і відповідного зростання загального добробуту. Запропоновано спрямовувати зусилля держави на розробку й впровадження дієвих систем кібербезпеки державного і корпоративного управління, на проведення наукових досліджень з розроблення засобів кіберзахисту в правовому, організаційному і технічному аспектах, на започаткування інформаційних і навчальних кампаній щодо підвищення обізнаності та формування навичок діяльності у сфері кібербезпеки.

Новизна. Встановлено взаємозв'язок між рівнями безпеки кіберпростору та цифрового розвитку. Показано, що підвищення рівня кібербезпеки є необхідною, проте недостатньою умовою для більш активного використання інформаційно-комунікаційних технологій та прискорення темпів розвитку цифрової економіки.

Практична значущість. Результати дозволяють більш гнучко підійти до формування параметрів політики держави щодо безпеки кіберпростору.

Ключові слова: цифрова економіка, кібербезпека, кіберпростір, великі дані, хмарні обчислення, інтернет речей, фішинг.

Постановка проблеми. Цифрові технології дозволяють підвищити ефективність створення суспільного продукту і задоволення потреб людини через збалансування і стійке використання виробничих, технологічних, трудових, інтелектуальних, фінансових та природних ресурсів, фізичної та інноваційної інфраструктури, що є передумовою для виникнення принципово нового укладу життя суспільства – «цифрової економіки» [1]. Її ключові технології, – «Великі дані» («Big data»), «Хмарні обчислення» («Cloud computing») та «Інтернет речей» («Internet of Things»), – дозволяють збирати, зберігати, обробляти і аналізувати великі масиви даних різного походження, повноти і характеру для подальшої оптимізації бізнес-процесів, швидкого ухвалення оперативних і стратегічних рішень окремих компаній і цілих країн, гнучкого і адекватного реагування на кон'юнктурні зміни і запити ринку при одночасному зменшенні впливу суб'єктивного людського фактору в процеси управління і ухвалення рішень в будь-якій сфері

господарської діяльності і суспільного життя [2].

Проте, поряд із перевагами цифровізація утворює ряд кіберзагроз для діяльності країн, компаній і окремих громадян. Використання ІК-технологій для несанкціонованого заволодіння даними юридичних і фізичних осіб сторонніми суб'єктами може нанести значної шкоди господарській діяльності – вивести з ладу системи управління компаній, незаконно позбавити їх майна і коштів, заблокувати виробничий процес, паралізувати економіку загалом (якщо йдеться про незаконне зовнішнє втручання у роботу стратегічних об'єктів виробництва та інфраструктури), тощо. Що стосується, наприклад України, то Рада національної безпеки і оборони нашої держави заявила, що у 2020 році в країні було виявлено понад один мільйон кіберзагроз. Найчастіше жертвами хакерів стають приватні підприємства. Кіберзлочинці активно використовують спроби мережевого сканування, мережеві атаки прикладного рівня, спроби WEB-атак, фішинг, DDoS-атаки, поширення шкідливого програмного забезпечення та інше [14]. Вони полюють за різними даними. Одні націлені вкрасти особисту закриту інформацію компанії; інші прагнуть привласнити її гроші. Водночас суть кібератаки переважно зводиться до отримання неправомірної фінансової вигоди або відразу – шляхом крадіжки грошей підприємства/клієнта, або через викрадення інформації, яка становитиме компромат на компанію, що дозволить за допомогою шантажу отримати від неї фінансову винагороду.

Подібним загрозам піддаються усі без виключення країни світу, а проблема кібербезпеки набуває неабиякої гостроти і важливості. Про це свідчить невпинне зростання розміру світового ринку кібербезпеки, який у 2020 р. оцінювався у розмірі 173 млрд дол., а до 2026 р. очікується його збільшення мало не вдвічі – до 270 млрд дол. [14]. З цього слідує, що подальший розвиток цифрової економіки і отримання людством її переваг нерозривно пов'язаний із одночасною розбудовою відповідних систем кібербезпеки..

Аналіз останніх досліджень і публікацій. Вивченню важливості забезпечення кібербезпеки для розвитку цифрової економіки в країні присвячено ряд зарубіжних досліджень. В них зокрема відзначається, що необхідною умовою успішного розвитку цифрової економіки є забезпечення надійного цифрового простору, досягнення якого можливе за умови вдосконалення відповідного законодавства і політики у сфері кібербезпеки [3], доводиться факт, що кіберзагрози уповільнюють темпи розвитку цифрової економіки [4]. Дослідження британської аудиторської компанії «Ernst & Young» [15] виявило серйозні прогалини у сфері кібербезпеки на рівні компаній по всьому світу, пов'язані як з недостатнім усвідомленням її значення керівництвом, так і з відсутністю достатньо ефективних організаційних і технічних засобів протидії кіберзагрозам.

Окремі аспекти зазначеної проблем досліджувались такими вітчизняними науковцями, як О. Баранов [5], М. Гончар [6], М. Грановський [7], І. Грабар, Р. Грищук, К. Молодецька [8], В. Дудикевич, Г. Микитин, А. Ребець[9], О. Ткаченко, К. Ткаченко [10], І. Яковів [11] та інші. Проте їх дослідження здебільшого зосереджені на сфері правового регулювання та формування системи інформаційної безпеки України, тоді як маловивченими залишились питання впливу кібербезпеки на формування та розвиток цифрової економіки.

Формулювання мети статті. Метою статті є визначення взаємозв'язку між кібербезпекою та рівнем розвитку цифрової економіки для формулювання рекомендацій щодо політики цифровізації.

Виклад основного матеріалу дослідження. Однією з ключових проблем становлення цифрової економіки, у якій інформація стає ключовим ресурсом, є забезпечення кібербезпеки. В узагальненому вигляді під кібербезпекою розуміють сукупність спеціальних правових, організаційних, і технічних заходів, реалізація яких дозволяє забезпечити захист інформаційних комп'ютерних систем, мереж і різних програмних додатків від кібернетичних атак зловмисників. Такі атаки здатні завдати значних матеріальних збитків як підприємствам, через втрату коштів, активів або розкриття важливої конфіденційної інформації, так і державі – спровокувати техногенні катастрофи, спричинити збитки для

цивільної, фінансової, енергетичної та військової інфраструктури (табл. 1). З поширенням цифровізації і комп'ютеризації як у виробництві, так і у побуті, масштаби кіберзагроз зростатимуть пропорційно розширенню спектру продуктів і послуг, у яких застосовуються інформаційні технології, та кількості їх споживачів. Уже сьогодні, за експертними оцінками, у світі налічується близько шести тисяч тіньових ринків, де продають 45 тис. продуктів або послуг для здійснення кіберзлочинів, а найшвидше зростаючим ринком у цій сфері є ринок послуг зі зламу комп'ютерних систем [16].

Таблиця 1

ТОП-10 найбільш цінних для зловмисників типів даних та найбільш актуальних для компаній кіберзагроз у світі, 2018–2019 р., відсотків у загальній кількості

	Типи даних, цінні для зловмисників	%	Кіберзагрози для компаній	%
1	Клієнтська інформація	17	Фішинг	22
2	Фінансова інформація	12	Шкідливе ПЗ	20
3	Стратегічні плани	12	Кібератаки з метою дезорганізації діяльності	13
4	Інформація про вище керівництво	11	Кібератаки з метою викрадення коштів	12
5	Паролі клієнтів	11	Шахрайство	10
6	Результати НДДКР	9	Кібератаки з метою викрадення об'єктів інтелектуальної власності	8
7	Інформація про угоди злиття та поглинання	8	Спам	6
8	Об'єкти інтелектуальної власності	6	Атаки зсередини організації	5
9	Незапатентована інтелектуальна власність	5	Стихійні лиха	2
10	Інформація про постачальників	5	Шпіонаж	2

Джерело: [15, с. 9].

З огляду на зазначене гарантування кібербезпеки є актуальним завданням для держави і бізнесу, а розробка адекватних заходів протидії подібним викликам і загрозам стають важливим напрямом науково-технічного прогресу і державної політики.

Для моніторингу та порівняльної оцінки ступеня готовності країн до захисту даних в кіберпросторі використовуються «Глобальний індекс кібербезпеки» (Global Cybersecurity Index, GCI) та «Національний індекс кібербезпеки» (National Cyber Security Index, NCSI). Ці індекси оцінюють ризики для корпоративної, промислової та урядової інформаційної інфраструктури від кіберзагроз. У формуванні Індексу NCSI ураховують такі ключові кіберзагрози як втручання в систему електронних послуг (послуги недоступні), порушення цілісності даних (несанкціоноване внесення змін), порушення конфіденційності даних (оприлюднення таємниці). Ці загрози впливають на нормальне функціонування національних комп'ютерних інформаційних систем електронних послуг, блокування надання яких може спричинити колапс в економіці і державному управлінні.

Рейтинг NCSI будується на вимірюванні тих аспектів кібербезпеки, що відображені в урядових рішеннях і стосуються спеціальних законодавчих і нормативно-правових актів, наявності і розвиненості спеціальних інституцій з протидії загрозам, організації співпраці між різними суб'єктами щодо протидії загрозам, наявності відповідних технологічних можливостей і програмного забезпечення тощо. Такий підхід дозволяє отримати чітку верифіковану основу для складання індексу і є його відмінною рисою.

Глобальний індекс кібербезпеки (Global Cybersecurity Index, GCI) розроблений Міжнародним союзом електрозв'язку (International Telecommunication Union (ITU))

[12]. Він вибудовується на основі відповідей експертів щодо стану безпеки кіберпростору у розрізі законодавчої, технічної та організаційної складових, а також оцінювання можливостей підвищення їх потенціалу та взаємодії (табл. 2).

Таблиця 2

Структура формування Глобального індексу кібербезпеки (GCI)

Складові	Зміст складових
Законодавство	Законодавство з кіберзлочинності; регулювання кібербезпеки; законодавче обмеження спаму
Технічне забезпечення	CERT / CIRT / CSIRT*; структура застосовуваних стандартів; органи стандартизації; технічні механізми і можливості, що застосовуються для боротьби зі спамом; використання хмари для забезпечення кібербезпеки; механізми захисту дітей від негативної інформації в Інтернеті
Організаційна складова	Національна стратегія кібербезпеки; відповідальні органи; показники кібербезпеки
Підвищення потенціалу	Кампанії з інформування громадськості; структура для сертифікації та акредитації фахівців з кібербезпеки; професійні тренувальні курси з кібербезпеки; освітні програми або академічні курси з кібербезпеки; програми наукових досліджень і розробок в галузі кібербезпеки тощо
Кооперація	Двосторонні угоди; багатосторонні угоди; участь в міжнародних асоціаціях; державно-приватне партнерство; міжвідомче /внутрішньовідомче партнерство тощо

* CERT - Computer Emergency Response Team; CIRT - Computer Incident Response Team; CSIRT - Computer Security Incident Response Team. Джерело: [12].

Аналіз індексу дозволяє зробити висновок, що законодавча база є ключовою у забезпеченні кібербезпеки. Юридичний контекст оцінюється на основі кількості правових інститутів і структур, відповідальних за кібербезпеку. Забезпечення останньої неможливо здійснити без відповідних технічних навичок для виявлення кібератак і реагування на них. Для забезпечення ефективного функціонування системи кібербезпеки важливими елементами є: наявність національної стратегії; моделі управління, адекватної рівню вирішуваних завдань; органів нагляду, укомплектованих відповідними фахівцями. Все це становить основу організаційної складової кібербезпеки на національному рівні. Можливості підвищення потенціалу і рівня кібербезпеки оцінюються за кількістю досліджень і розробок в даній сфері, наявністю освітніх і навчальних програм, а також сертифікованих фахівців та установ державного сектора. Для забезпечення ефективності в боротьбі із кіберзлочинністю необхідною умовою є розширення співпраці на національному та міжнародному рівні, яка оцінюється за кількістю партнерств з обміну інформацією.

Рівень цифрового розвитку (Digital Development Level – DDL) розраховується за Індексом розвитку ІКТ (IDI) та Індексом мережевої готовності (NRI). Індекс розвитку ІКТ (IDI) визначається за показниками розвиненості інфраструктури інформаційних технологій. Він призначений для моніторингу розвитку ІТ у країнах, їх позиціонування на світовому ринку ІТ і має три субіндекси: доступ, використання, навички [13, с.261]. Індекс мережевої готовності складається з чотирьох субіндексів, які оцінюють середовище для розвитку ІТ, готовність суспільства до використання ІТ, їх фактичне використання державою, бізнесом, населенням та наслідки, які ІТ породжують в економіці та суспільстві. Перші три субіндекси – це драйвери зростання, які формують передумови для четвертого субіндексу – впливу ІТ на економіку.

При порівнянні країн за відповідними індексами цифрового розвитку та кібербезпеки, взаємозв’язок між останніми стає очевидним (табл. 3).

Таблиця 3

Рейтинг країн за індексами кібербезпеки та розвитку цифрової економіки

Національний індекс кібербезпеки, 2019			Глобальний індекс кібербезпеки, 2018			Рівень цифрового розвитку (DDL)*, 2019	
Рейтинг	Країна	Оцінка	Рейтинг	Країна	Оцінка	Країна	Оцінка
1	Греція	96,10	1	Велика Британія	93,1	Швейцарія	85,13
2	Чеська Республіка	92,21	2	США	92,6	Республіка Корея	84,25
3	Естонія	90,91	3	Франція	91,8	Ісландія	84,19
4	Литва	88,31	4	Литва	90,8	Великобританія	83,96
5	Іспанія	88,31	5	Естонія	90,5	Нідерланди	83,88
6	Бельгія	85,71	6	Сінгапур	89,8	Норвегія	83,78
7	Словаччина	83,12	7	Іспанія	89,6	Данія	83,55
8	Хорватія	83,12	8	Малайзія	89,3	Швеція	83,48
9	Франція	83,12	9	Норвегія	89,2	Сінгапур	83,11
10	Фінляндія	81,82	10	Австралія	89,2	Люксембург	83,06
11	Данія	81,82	11	Люксембург	89,0	США	82,33
12	Нідерланди	81,82	12	Нідерланди	88,5	Фінляндія	82,26
13	Сінгапур	80,52	13	Саудівська Аравія	88,1	Японія	82,15
14	Німеччина	80,52	14	Японія	88,0	Німеччина	81,95
15	США	79,22	15	Республіка Корея	87,3	Нова Зеландія	80,94
…			…	…			
29	**Україна**	**63,64**	**54**	**Україна**	**66,1**	**Україна**	**58,10**

*Примітка: DDL – середній відсоток, отриманий країною від максимального значення обох індексів.
Джерело: https://ncsi.ega.ee/compare/

Відповідно до рейтингу NCSI-2019 Україна посіла 29 позицію. Серед сильних сторін нашої країни було відзначено серйозні напрацювання у сфері запровадження політики кібербезпеки, захисту персональних даних і боротьби з кіберзлочинністю. Проте слабкими залишаються позиції управління інцидентами та кіберкризами, захисту електронних сервісів, аналізу та інформування громадськості про кіберзагрози. Наші сусіди, – окремі країни пострадянського простору, – мають кращі позиції у рейтингу ніж Україна. Зокрема у першу десятку лідерів увійшли Чеська республіка (2), Естонія (3) та Литва (4).

Лідером рейтингу Глобального індексу кібербезпеки у 2018 році стала Велика Британія, другу сходинку посіли США, третю – Франція. Україна опинилась у шостій десятці країн, посівши 54 місце. Водночас і такий результат для нашої держави є прогресом, оскільки у попередні роки ми мали значно нижчі позиції, а поліпшення рейтингу зумовлене наполегливою роботою держави щодо створення системи адекватного реагування на комп'ютерні надзвичайні події та подолання наслідків кібератак на критично важливу інформаційну інфраструктуру. Зокрема був створений відповідний спеціалізований підрозділ – CERT-UA – команда реагування на комп'ютерні надзвичайні події України у вигляді спеціалізованого структурного підрозділу Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. Він 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.

Головними гравцями світового ринку інформаційних технологій відповідно до Індексу розвитку ІКТ (IDI) та Індексу мережевої готовності (NRI) у 2019 році є країни Південно-Східної Азії (Сінгапур і Японія), європейські країни (Фінляндія, Швеція, Норвегія, Нідерланди, Швейцарія, Велика Британія та Люксембург), а також США. Їх економікам притаманний високий рівень цифрового розвитку. Україна за Індексом розвитку ІКТ (ICT Development Index) відповідно до Звіту Міжнародного союзу електрозв'язку «Вимірювання інформаційного суспільства 2019» посіла 79 місце зі 176 країн, а за Індексом мережевої готовності (NRI) – 64 місце. Однією із причин невисокого місця України в зазначених рейтингах є нерівномірність розвитку та впровадження ІКТ в різних сферах господарювання та регіонах.

З огляду на зазначене, можна припустити, що забезпечення безпеки в кіберпросторі сприятиме підвищенню рівня цифрового розвитку в країнах. Проведення відповідного кореляційно-регресійного моделювання зв'язку між національним індексом кібербезпеки та комплексним показником рівня цифрового розвитку за даними 70 країн у 2019 р. таке припущення підтверджує (рис. 1).

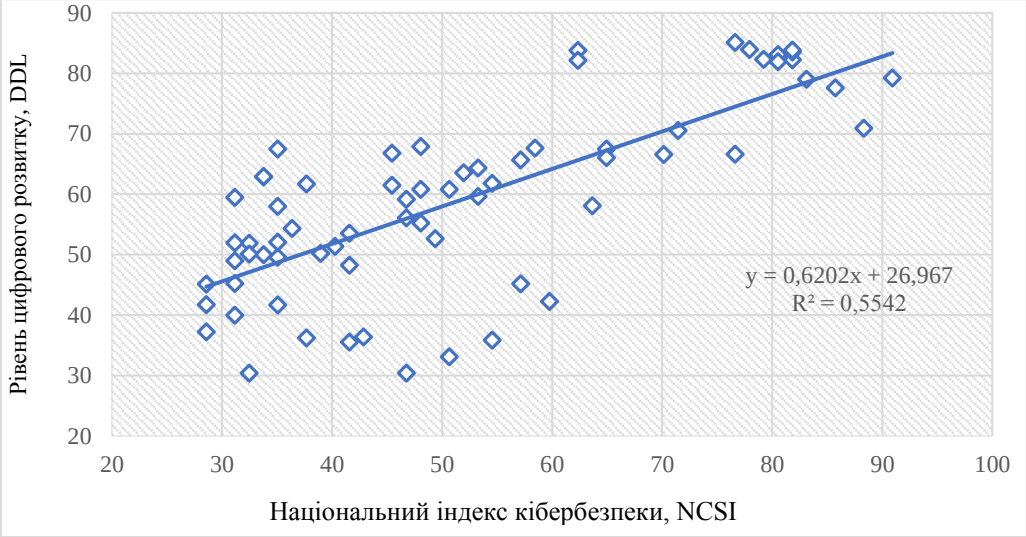

Рис. 1. Зв'язок між національним індексом кібербезпеки та рівнем цифрового розвитку країн у 2019 р.

Джерело: розрахунок автора за даними: https://ncsi.ega.ee/compare/.

Аналіз засвідчив високу тісноту зв'язку (за шкалою Чеддока) між досліджуваними показниками із значенням множинного коефіцієнта кореляції 0,7469. Разом з тим, R-квадрат, величина якого менше 0,6, вказує на те, що точність апроксимації недостатня і модель вимагає введення нових незалежних змінних. Тобто, можна говорити, що підвищення рівня кібербезпеки не завжди є достатнім для забезпечення розвитку цифрової економіки. Якщо згрупувати країни за рівнем розвитку, то виявляється, що в розвинених країнах рівень кібербезпеки і рівень цифрового розвитку вище, ніж в країнах, що розвиваються. Водночас, останні демонструють, що підвищення рівня кібербезпеки позитивно впливає на розвиток цифрової економіки, тоді як відносно перших такий взаємозв'язок дещо слабший.

Висновки. Розвиток цифрової економіки неможливий без посилення кібербезпеки як на рівні держави, так і на рівні окремих суб'єктів. Усвідомлення державою і бізнесом кібернетичних загроз та їх наслідків не набуло достатньої важливості, а тому часто сприймається як дещо другорядне. Однак, результати аналізу свідчать, що існує тісний зв'язок між рівнями кібербезпеки та цифрового розвитку: підвищення першої неминуче веде до прискорення другого і, як наслідок, зростання добробуту. Тому кібербезпека повинна посісти чільне місце у загальній стра-

тегії розвитку держави і кожної окремо взятої компанії. Необхідною є розробка окремої стратегії і програми безпеки для усієї бізнес-екосистеми країни і державного управління. Держава спільно з бізнесом має докласти зусиль для розробки і впровадження дієвих систем кібербезпеки державного і корпоративного управління, проводити наукові дослідження з розробки засобів кіберзахисту в правовому, організаційному і технічному аспектах, розпочати інформаційні та навчальні кампанії щодо підвищення обізнаності й навичок у сфері кібербезпеки для державних службовців, персоналу компаній, рядових громадян. Водночас, слід ураховувати, що само по собі підвищення рівня кібербезпеки не завжди є достатнім для забезпечення розвитку цифрової економіки, оскільки він залежить і від інших факторів, таких як загальний рівень економічного, технологічного і соціального розвитку країни, її положення у світовій економіці, ефективності державного управління, рівня захищеності прав власності. Останній має бути висхідним у формуванні державної стратегії кібербезпеки і подальшого розвитку цифрової економіки, оскільки усі без виключення кіберзлочини пов'язані із несанкціонованим перерозподілом цих прав. Для України їх захист становить проблему, оскільки держава у силу її інституційних особливостей, сама доволі часто (в особі своїх корумпованих представників в органах державного управління, правоохоронній і судовій системах) виступає основним порушником цих прав як щодо бізнесу, так і громадян, а кіберзлочинц часто стають лише інструментом в руках представників влади у незаконному перерозподілі власності шляхом використання сучасних інформаційно-комунікаційні технологій.

Література

1. The new digital economy. How it will transform business (White paper). Oxford: Oxford Economics, 2011.
2. UNCTAD. Information Economy Report: digitalization, trade and development, 2017. unctad.org/en/PublicationsLibrary/ier2017_en.pdf. (Дата звернення 21.07.2020).
3. Mat B., Pero S., Wahid R., Sule B. Cybersecurity and Digital Economy in Malaysia: Trusted Law for Customer and Enterprise Protection // International Journal of Innovative Technology and Exploring Engineering, 2019. www.ijitee.org/wp-content/uploads/papers/v8i8s3/H10610688S319.pdf (Дата звернення 21.07.2020).
4. Kearney A. T. Cybersecurity in ASEAN: An Urgent Call to Action, 2018. www.atkearney-.com/documents/20152/1792707/Cybersecurity+in+ASEAN%E2%80%94An+-Urgent+Call+to+Action.pdf/1e25fefa-8ecb-9f50-e262-2467ac4ea458?t=1544723905824 (Дата звернення 21.07.2020).
5. Баранов О. А. Інтернет речей: теоретико-методологічні основи правового регулювання / О. А. Баранов. – Київ, 2018. – Т. 1: Сфери застосування, ризики і бар'єри, проблеми правового регулювання. – 342 с
6. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія. / С. Ф. Гончар. – Київ, 2019. – 175 с.
7. Грановський М. В. Державна політика у сфері запобігання та протидії кібернетичним загрозам – досвід Республіки Польща / М. В. Грановський // Теорія та практика державного управління. – 2019. – Вип. 4. – С. 212–220.
8. Грабар І. Г. Безпекова синергетика: кібернетичний та інформаційний аспекти : монографія. / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька. – Житомир, 2019. – 279 с.
9. Дудикевич В. Б. Квінтесенція інформаційної безпеки кіберфізичної системи. / В. Б. Дудикевич, Г. В. Микитин, А. І. Ребець // Вісник Національного університету «Львівська політехніка». – Інформаційні системи та мережі. – 2018. – № 887. – С. 58–68.
10. Ткаченко О. Кіберпростір і кібербезпека: проблеми, перспективи, технології. / О. Ткаченко, К. Ткаченко. // Цифрова платформа: інформаційні технології в соціо-культурній сфері. – 2018. – Вип. 1. – С. 75–86.
11. Яковів І. Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека / І. Яковів // Information Technology and Security. – 2017. – Vol. 5. – № 2. – С. 134–144.
12. ITU. Global Cybersecurity Index (GCI), 2018. www.itu.int/en/ITU-D/Cybersecurity/-Documents/draft-18-00706_GlobalCybersecurity-Index-EV5_print_2.pdf (Дата звернення: 11.08.2020).
13. Мачуга Р. І. Сучасний стан ринку інформаційно-комунікаційних технологій України. / Р. І. Мачуга, О. С. Борух // Східна Європа: економіка, бізнес та управління. – 2016. – № 3. – С. 260–264.
14. Сегида Г. Почему бизнес должен серьезно воспринимать киберугрозы во время пандемии и удаленки. *Интернет-портал «Delo.ua»*. – 2020. 3 сентября. https://delo.ua/opinions/pochemu-biznes-dolzhen-serezno-vosprinimat-kiber-372407/ (Дата звернення: 03.09.2020).
15. Кибербезопасность: больше чем защита? Международное исследование EY в области информационной безопасности, 2018–2019 годы. Ernst & Young, 2018. 32 с. https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-rus/$FILE/ey-global-

information-security-survey-rus.pdf (Дата звернення: 08.09.2020).

16. Монін Д. Ризики й виклики нового часу. / Д. Монін // Дзеркало тижня. – 2020. – №5 вересня. https://zn.ua/ukr/macrolevel/riziki-j-vikliki-novoho-chasu.html (Дата звернення: 7 вересня 2020 р.).

References

1. The new digital economy (2011). How it will transform business (White paper). Oxford: Oxford Economics.

2. UNCTAD (2017). Information Economy Report: digitalization, trade and development. Retrieved from http: Unctad.org/en/PublicationsLibrary/ier2017_en.pdf.

3. Mat, B., Pero, S., Wahid, R., & Sule, B. (2019). Cybersecurity and Digital Economy in Malaysia: Trusted Law for Customer and Enterprise Protection. International Journal of Innovative Technology and Exploring Engineering. Retrieved from http: www.ijitee.org/wp-content/uploads/papers/v8i8s3/H10610688S319.pdf

4. Kearney, A.T. (2018). Cybersecurity in ASEAN: An Urgent Call to Action. Retrieved from http: www.atkearney.com/documents/20152/1792707/Cybersecurity+in+ASEAN%E2%-80%94An+Urgent+Call+to+Action.pdf/1e25fefa-8ecb-9f50-e262-2467ac4ea458?t=1544723905824

5. Baranov, O.A. (2018). Internet rechei: teoretyko-metodolohichni osnovy pravovoho rehuliuvannia. Kyiv. Proceedings from T.1: Sfery zastosuvannia, ryzyky i bariery, problemy pravovoho rehuliuvannia.

6. Honchar, S.F. (2019). Otsiniuvannia ryzykiv kiberbezpeky informatsiinykh system obiektiv krytychnoi infrastruktury. Kyiv.

7. Hranovskyi, M.V. (2019). Derzhavna polityka u sferi zapobihannia ta protydii kibernetychnym zahrozam – dosvid Respubliky Polshcha. Teoriia ta praktyka derzhavnoho upravlinnia, Issue 4, 212-220.

8. Hrabar, I.H., Hryshchuk, R.V., & Molodetska, K.V. (2019). Bezpekova synerhetyka: kibernetychnyi ta informatsiinyi aspekty. Zhytomyr.

9. Dudykevych, V.B., Mykytyn, H.V., & Rebets, A.I. (2018). Kvintesentsiia informatsiinoi bezpeky kiberfizychnoi systemy. Visnyk Natsionalnoho universytetu «Lvivska politekhnika». Informatsiini systemy ta merezhi, (887), 58-68.

10. Tkachenko, O., & Tkachenko, K. (2018). Kiberprostir i kiberbezpeka: problemy, perspektyvy, tekhnolohii. Tsyfrova platforma: informatsiini tekhnolohii v sotsiokulturnii sferi, Issue 1. 75-86.

11. Iakoviv, I. (2017). Informatsiino-telekomunikatsiina systema, kontseptualna model kiberprostoru i kiberbezpeka. Information Technology and Security, Issue 5, (2), 134-144.

12. ITU. Global Cybersecurity Index (GCI), 2018. Retrieved from www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_GlobalCybersecurity-Index-EV5_print_2.pdf

13. Machuha, R.I., & Borukh, O.S. (2016). Suchasnyi stan rynku informatsiino-komunikatsiinykh tekhnolohii Ukrainy. Skhidna Yevropa: ekonomika, biznes ta upravlinnia, (3), 260-264.

14. Sehyda, H. (2020). Pochemu biznes dolzhen seriyozno vosprynimat kiberuhrozy vo vremya pandemii i udalenki. Ynternet-portal «Delo.ua». Retrieved from https://delo.ua/opinions/pochemu-biznes-dolzhen-serezno-vosprinimat-kiber-372407/

15. Kiberbezopasnost: bolshe chem zashchita? Mezhdunarodnoe issledovanie EY v oblasti informatsionnoy bezopasnosti, 2018-2019 god?. Ernst & Young, 2018. Retrieved from https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-rus/$FILE/ey-global-information-security-survey-rus.pdf

16. Monin, D. (2020). Ryzyky y vyklyky novoho chasu. Dzerkalo tyzhnia. Retrieved from https://zn.ua/ukr/macrolevel/riziki-j-vikliki-novoho-chasu.html.

КИБЕРБЕЗОПАСНОСТЬ И СТАНОВЛЕНИЕ ЦИФРОВОЙ ЭКОНОМИКИ: ПРОБЛЕМЫ ВЗАИМОСВЯЗИ

Ю. В. Киндзерский, д. э. н., ведущий научный сотрудник ГУ «Институт экономики и прогнозирования НАН Украины»

Методология исследования. Методологической основой исследования стали общенаучные и специальные методы познания процессов и явлений цифровой трансформации экономики: статистические методы – для обработки данных при оценке уровня цифровой трансформации экономики; экспертных оценок – для определения факторов влияния на развитие цифровой экономики; корреляционного анализа – при установлении взаимосвязи между детерминантами и масштабом цифровизации экономики.

Результаты. Раскрыто значение кибербезопасности в формировании цифровой экономики. Проанализирован уровень готовности стран к защите данных в киберпространстве по «Глобальному индексу кибербезопасности» (Global Cybersecurity Index, GCI) и «Национальному индексу кибербезопасности» (National Cyber Security Index, NCSI), раскрыты особенности их составляющих. Акцентировано внимание на оценке влияния кибербезопасности на уровень развития цифровой экономики. Обнаружена проблема волатильности взаимосвязи между

кибербезопасностью и уровнем цифрового развития сквозь призму показателей развития ИКТ и сетевой готовности. Выявлено, что повышение уровня кибербезопасности неизбежно ведет к ускорению развития цифровой экономики и соответствующего роста общего благосостояния. Предложено направлять усилия государства на разработку и внедрение действенных систем кибербезопасности государственного и корпоративного управления, на проведения научных исследований по разработке средств киберзащиты в правовом, организационном и техническом аспектах, на организацию информационных и учебных кампаний по повышению осведомленности и формированию навыков деятельности в области кибербезопасности.

Новизна. Установлена взаимосвязь между уровнями безопасности киберпространства и цифрового развития. Показано, что повышение уровня кибербезопасности является необходимым, но недостаточным условием для более активного использования информационно-коммуникационных технологий и ускорения темпов развития цифровой экономики.

Практическая значимость. Результаты позволяют более гибко подойти к формированию параметров политики государства по безопасности киберпространства.

Ключевые слова: цифровая экономика, кибербезопасность, киберпространство, большие данные, облачные вычисления, интернет вещей, фишинг.

CYBERSECURITY AND BECOMING OF THE DIGITAL ECONOMY: PROBLEMS OF INTERCONNECTION

Yu. V. Kindzerskyi, D.E., Leading Researcher, Institute for Economics and Forecasting of the NAS of Ukraine

Methods. The methodological basis of the study includes general scientific and specific methods of understanding the processes and phenomena of digital economic transformation: statistical methods – for data processing in assessing the level of digital economic transformation; expert assessments – for determining factors influencing the digital economy; correlation analysis – in establishing the relationship between the determinants and the scale of digitalization of the economy, etc.

Results. The importance of cybersecurity in the formation of the digital economy is revealed. The level of readiness of countries to protect data in cyberspace according to the Global Cybersecurity Index (GCI) and the National Cyber Security Index (NCSI) is analyzed, and the specifics of their content are revealed. The emphasis is on assessing the impact of cybersecurity on the level of development of the digital economy. The problem of volatility of the relationship between cybersecurity and the level of digital development is identified through the prism of indicators of ICT development and network readiness. It is concluded that increasing the level of cybersecurity inevitably leads to accelerated development of the digital economy and a corresponding increase in overall welfare. It is proposed to focus the state's efforts on the development and implementation of effective cybersecurity systems of public and corporate governance, research on the development of cybersecurity in legal, organizational, and technical aspects, conducting information and training campaigns to raise public awareness and skills in the field of cybersecurity.

Novelty. The relationship between cyberspace security and digital development has been established. It is shown that increasing the level of cybersecurity is a necessary but insufficient condition for more active use of information and communication technologies and acceleration of the pace of development of the digital economy.

Practical value. The results allow a more flexible approach to the formation of the parameters of state policy on cybersecurity.

Keywords: Digital economy, cybersecurity, cyberspace, Big data, cloud computing, Internet of Things, phishing.

Надійшла до редакції 20.08.20 р.