DOI: https://doi.org/10.32782/2524-0072/2023-56-167

УДК 338.24

РОЗВИТОК СПІВПРАЦІ ПРИВАТНИХ ОРГАНІЗАЦІЙ СФЕРИ ІТ З ДЕРЖАВНИМИ АГЕНЦІЯМ ЯК ПЕРЕДУМОВА РОЗВИТКУ ПУБЛІЧНО-ПРИВАТНОГО ПАРТНЕРСТВА В УМОВАХ ВІЙНИ

DEVELOPMENT OF COOPERATION BETWEEN PRIVATE IT ORGANIZATIONS AND GOVERNMENT AGENCIES AS A PREREQUISITE FOR THE DEVELOPMENT OF PUBLIC-PRIVATE PARTNERSHIPS IN TIMES OF WAR

Дячек Віталій Васильович
кандидат економічних наук, доцент,
Харківський національний університет імені В.Н. Каразіна
ORCID: https://orcid.org/0000-0003-3542-5669

Мірошніченко Ілля Петрович
аспірант другого року навчання,
Каразинська школа бізнесу,
Харківський національний університет імені В.Н. Каразіна
ORCID: https://orcid.org/0009-0008-0345-8339

Diachek Vitalii, Miroshnichenko Illia
V.N. Karazin Kharkiv National University

Стаття присвячена особливостям організації співпраці приватного бізнесу ІТ сфери з державними установами, особливостям розвитку публічно-приватного партнерства в умовах війни в Україні. Проведено аналіз розвитку сфери інформаційних технологій в Україні. Зроблено висновок про те, що сфера інформаційних технологій в Україні досить розвинена і навіть під час повномасштабної війни та інших негараздів дана сфера діяльності розвивається та зростає. Проведено аналіз капітальних інвестицій за видами економічної діяльності в Україні за 2010–2022 рр. Також проаналізовано загальні обсяги надання послуг. Зроблено висновок про те, що сфера інформаційних технологій в Україні досить розвинений і навіть під час повномасштабної війни та інших негараздів дана сфера діяльності розвивається та зростає. Тому в ця сфера має відповідні можливості бути приватним партнером держави та громадськості у певних проєктах захисту, про що свідчить наявний досвід нашої країни.

Ключові слова: війна, інформаційні технології, конфлікт, державна агенція, приватний бізнес, партнерство.

The article is devoted to the peculiarities of organizing cooperation between private IT businesses and state institutions, as well as to the peculiarities of developing public-private partnerships in the context of war in Ukraine. The author analyzes the development of information technology in Ukraine. It is concluded that the information technology sector in Ukraine is quite developed and even during a full-scale war and other problems, this field of activity is developing and growing. The author analyzes capital investments by types of economic activity in Ukraine for 2010–2022. The total volume of services provided is also analyzed. It is concluded that the sphere of information technology in Ukraine is quite developed and even during a full-scale war and other problems, this sphere of activity is developing and growing. Therefore, this area has the appropriate opportunities to be a private partner of the state and the public in certain protection projects, as evidenced by the existing experience of our country. As international practice shows, cooperation between the state and the private sector in the form of public-private partnerships is effective in countering modern threats to public security. The development of effective tools for strengthening security measures requires the participation of all relevant parties – public authorities, the private sector and civil society. The public and private sectors should conduct risk assessments, and the government will strengthen the private sector by disseminating best practices for business security. The private sector will assist the public sector in combating

terrorism and emergency situations by creating expertise and technology to efficiently allocate available security resources. The main task of public-private partnership in emergency situations is to improve crisis management. Therefore, public-private cooperation in the security sector can ensure the effective performance of state functions aimed at protecting critical infrastructure, combating terrorism and cyberterrorism, and addressing a number of humanitarian issues, which will significantly improve public welfare, safety and security.

Keywords: war, information technology, conflict, government agency, private business, partnership.

Постановка проблеми. Повномасштабне вторгнення показало консолідацію українського суспільства: крім безпосереднього відгуку населення щодо вступу у військо, ряди територіальної оборони, велика кількість людей і організацій, в тому числі приватні підприємства, доєднались до волонтерського руху. Таке єднання показує можливість об'єднання зусиль суспільства та держави у формуванні відповіді на виклики, які постають не тільки за нормальних умов функціонування, але і під час криз, в тому числі геополітичних і навіть війни. Виконання певних функцій та завдань приватним сектором економіки, які є прогресивними та за рівнем розвитку цифрових навичок персоналу значно перевищують людський та матеріально-технічний потенціали державного сектору та державних агенцій оборони. Слід відзначити, що попередні великі конфлікти та геополітичні кризи такого масштабу у Європі відбувалися в середині минулого сторіччя під час попередніх науково-технічних укладів, тому про мобілізацію інтелектуального потенціалу приватного сектору не йшлося через нерозвиненість нематеріальної сфери виробництва. На сьогодні остання відіграє значну роль в економічній системі світу і може бути предметом сумісно-роздільного виробництва держави та приватного сектору.

Об'єкт: сумісно-роздільні виробничі відносини у суспільстві.

Предмет: публічно-приватні партнерства в сфері інформаційно-комунікаційних послуг.

Аналіз останніх досліджень і публікацій. Розвиток публічно-приватного партнерства досліджували у своїх працях наступні науковці: Б. Вагнер, М. Карр, К. Петерсен, Т. Тропіна та ін. Дослідженню питань створення публічно-приватного партнерства в сфері інформаційних технологій присвятили свої роботи А. Клімбург, Т. Коляда, В. Круглов, К. Мін, М. Хан та ін. Незважаючи на чисельні досліджень цієї сфери залишаються деякі питання дослідження проблематики застосування механізму публічно-приватного партнерства в сфері інформаційних технологій під час війни.

Мета статті – визначити можливості застосування механізмів публічно-приватного партнерства у сфері інформаційно-комунікаційних технологій для підвищення рівня обороноздатності.

Виклад основного матеріалу дослідження. Необхідність створення проєктів публічно-приватного партнерства обумовлена невідповідністю зростаючих потреб в суспільних послугах з ресурсними можливостями держави щодо їх задоволення. Виділяють основні економічні причини започаткування публічно-приватного партнерства:

– інфраструктурний дефіцит;
– бюджетний дефіцит;
– проблеми ефективності державних інвестицій [1, с. 275].

Як свідчить світова практика, співпраця держави та приватного сектору у формі публічно-приватного партнерства є ефективною в тому числі і у протидії сучасним загрозам громадській безпеці. Розробка ефективних інструментів посилення заходів безпеки вимагає участі всіх відповідних сторін – органів державної влади, приватного сектору та громадянського суспільства. Державний і приватний сектори повинні проводити оцінку ризиків, а уряд зміцнюватиме приватний сектор, поширюючи передовий досвід для забезпечення безпеки бізнесу. Приватні власники допомагатимуть державному сектору в боротьбі з проявами тероризму та надзвичайними ситуаціями, створюючи досвід і технології для ефективного розподілу наявних ресурсів для забезпечення безпеки [2; 3].

Окрім традиційних напрямків публічного-приватного партнерства у сферах освіти, охорони здоров'я та надання державних послуг, спостерігається тенденція делегування окремих функцій держави у сфері громадської безпеки. Доведено, що передача окремих функцій у сфері громадської безпеки недержавним структурам має сприяти суттєвій економії бюджетних коштів, зберігаючи при цьому соціально прийнятний «індекс безпеки» та зосереджуючи можливості спеціалізованих державних органів на ключових напрямках

діяльності запобігання, виявлення і усунення існуючих загроз [4].

Існує думка, що приватний сектор у партнерстві з органами національної безпеки має можливість заздалегідь координувати власні плани щодо евакуації, транспортування, кібербезпеки та інших питань, отримуватиме інформацію від національних органів влади про загрози та тенденції в цій сфері. У надзвичайних ситуаціях приватний сектор буде працювати з інформацією, зберігати, встановлювати протоколи конфіденційності, покращувати загальну безпеку країни. Одним із елементів безпечного простору є питання гуманітарної допомоги в надзвичайних ситуаціях. Гуманітарна логістика визначається як процес надання ефективної підтримки постраждалому населенню під час катастрофічних подій. Складність гуманітарних ланцюгів постачання полягає в тому, що ці процеси необхідно планувати та виконувати в умовах надзвичайної невизначеності та часових обмежень [5].

У надзвичайних ситуаціях публічно-приватні партнерства задіють свої комерційні ланцюжки поставок критично важливих товарів і послуг, які доповнюють ланцюжки поставок державних послуг або товарів, щоб мінімізувати кризові ситуації. Метою публічно-приватного партнерства у сфері безпеки є зменшення вартості негативних наслідків, спричинених обмеженнями витрат державного бюджету та обмеженнями корпоративної участі. Основним завданням публічно-приватного партнерства у надзвичайних ситуаціях вважається вдосконалення антикризового менеджменту. Отже, публічно-приватне співробітництво у сфері безпеки може забезпечити ефективне виконання функцій держави, спрямованих на захист критичної інфраструктури, боротьбу з тероризмом та кібертероризмом, вирішення низки гуманітарних проблем, що значно покращить суспільний добробут, безпеку та охорону діяльність [5].

Слід зазначити, що в Україні сфера інформаційних технологій протягом останніх років зазнала значних успіхів.

З рис. 1 можна бачити, що обсяг капітальних інвестицій на обраному періоді зростає.

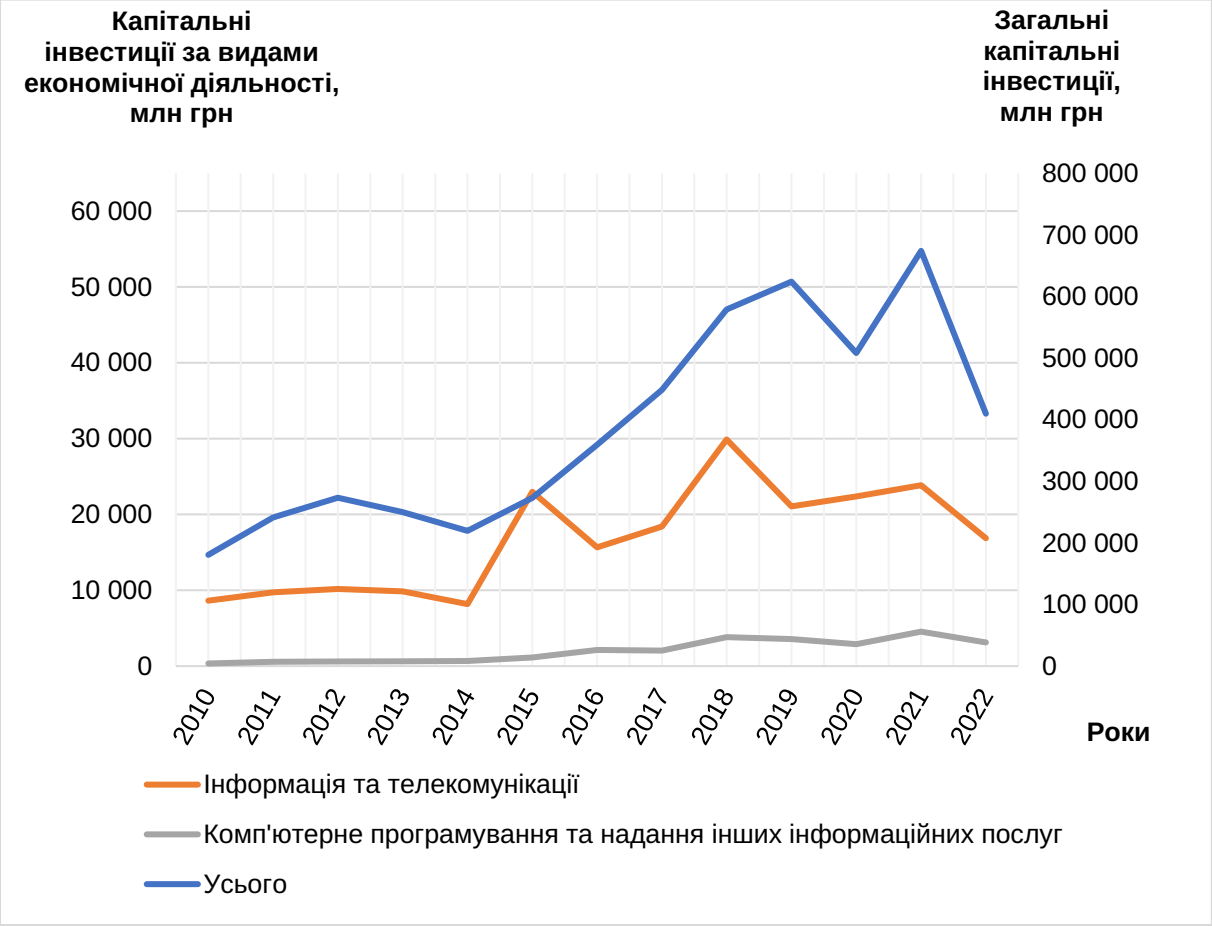

Рис. 1. Капітальні інвестиції за видами економічної діяльності за 2010–2022 рр., млн грн

Джерело: розраховано за [6]

Таблиця 1

Базисні темпи зростання капітальних інвестицій за видами економічної діяльності за 2010–2022 рр.

№	Вид діяльності	Базисні темпи зростання у 2022 р., 2010 р. – базисний
1	Загальні інвестиції	226,86
2	Інформація та телекомунікації	195,58
3	Комп'ютерне програмування та надання інших інформаційних послуг	898,48

Джерело: розраховано за [6]

Розглядаючи період 2021–2022 рр., повномасштабного вторгнення, ми бачимо значне зниження інвестицій, що є природнім. Але стосовно виду діяльності, комп'ютерне програмування та надання інших інформаційних послуг, то падіння значно менше. Також аналіз базисних темпів зростання у 2022 р., табл. 1, показує найбільше зростання капітальних інвестицій саме у підприємства цього виду діяльності.

Аналіз зайнятих у працівників у суб'єктів господарювання за видами економічної діяльності свідчить, що в цілому їх кількість знижувалася на обраному періоду, натомість у підприємствах за видом діяльності інформація і телекомунікація, а особливо комп'ютерне програмування, консультування та надання інших інформаційних послуг зростала. Аналіз базисних темпів зростання, табл. 2, також показав аналогічні результати. Але порівняльний аналіз показників зайнятості у 2022 році порівняно з 2021 показав зростання занятості у підприємствах, що займаються комп'ютерним програмуванням та наданням інших інформаційних послуг.

Аналіз обсягів реалізованої продукції суб'єктів господарювання за видами економічної діяльності у 2010–2021 рр. показує зростання, але найбільше зростання ми спостерігаємо у підприємств задіяних до комп'ютерного програмування (табл. 3).

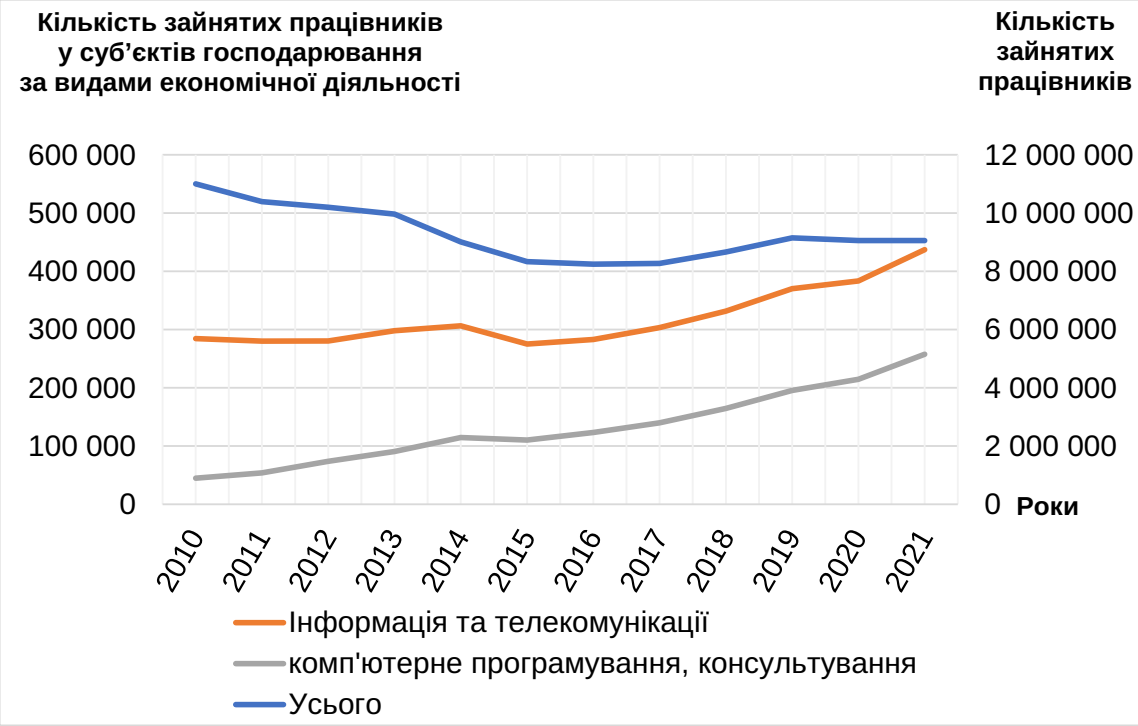

Рис. 2. Кількість зайнятих працівників у суб'єктів господарювання за видами економічної діяльності у 2010–2021 рр., людей

Джерело: розраховано за [6]

Таблиця 2

Базисні темпи зростання кількості зайнятих працівників у суб'єктів господарювання за видами економічної діяльності у 2010–2021 рр.

№	Вид діяльності	Темпи зростання у 2022 р. по відношенню до 2010 р.	Темпи зростання у 2022 р. по відношенню до 2021 р.
1	Всього	82,32	99,03
2	Інформація та телекомунікації	153,56	103,56
3	Комп'ютерне програмування та надання інших інформаційних послуг	575,06	120,04

Джерело: розраховано за [6]

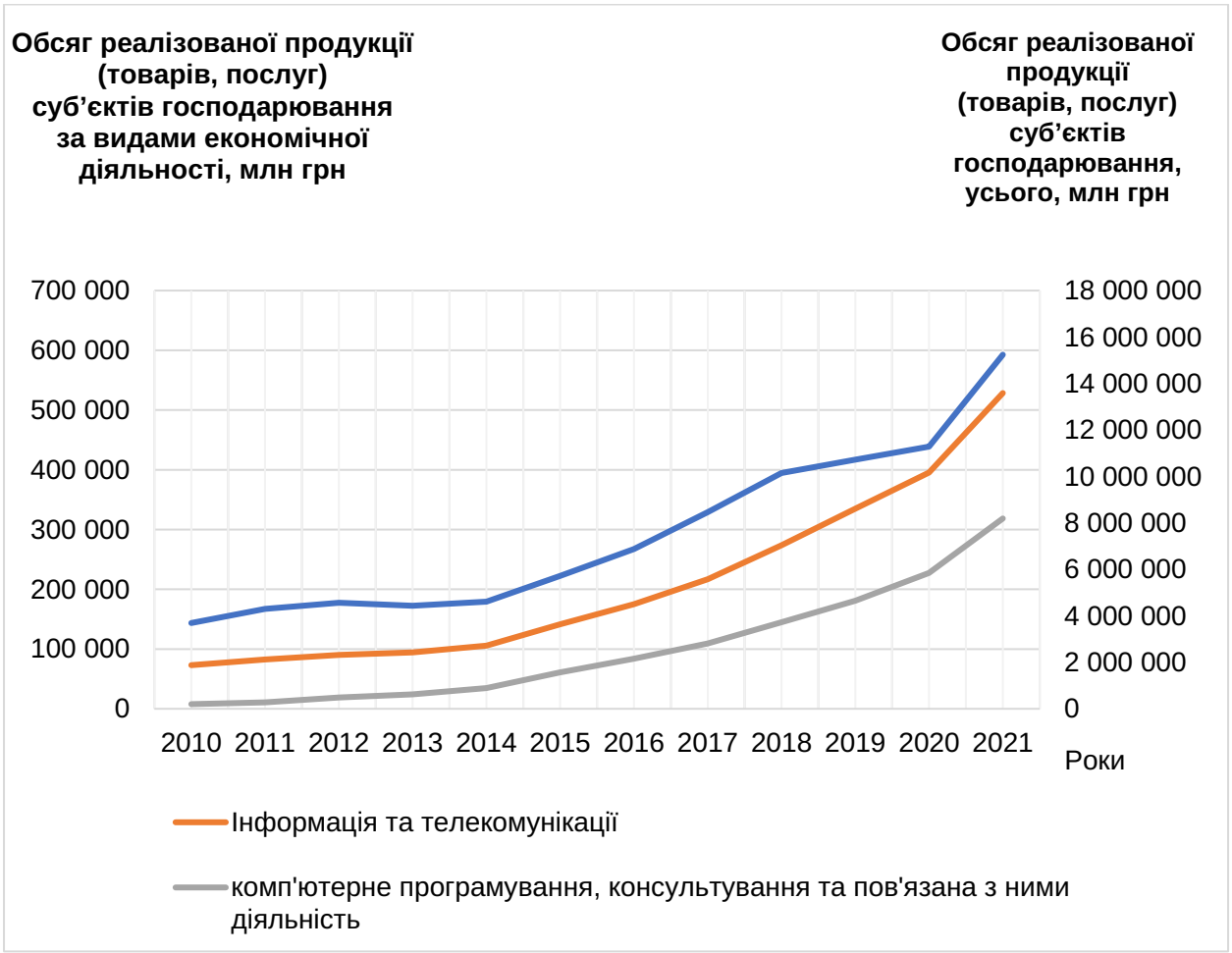

Рис. 3. Обсяг реалізованої продукції (товарів, послуг) суб'єктів господарювання за видами економічної діяльності у 2010–2021 рр., млн грн

Джерело: розраховано за [6]

Аналіз показників зовнішньої торгівлі послугами за видами у 2022 році показує, що в цілому обсяг експорту та імпорту у 2022 році знизився порівняно до 2021 р. Виключення складають лише експорт телекомунікаційних послуг, 121,7%, та інформаційних послуг, 109%.

В результаті проведеного статистичного аналізу ми бачимо що сфера інформаційних технологій в Україні досить розвинений і навіть під час повномасштабної війни та інших негараздів дана сфера діяльності розвивається та зростає. Тому в ця сфера має відповідні можливості бути приватним парт-

Таблиця 3

Базисні темпи зростання обсягу реалізованої продукції (товарів, послуг) суб'єктів господарювання за видами економічної діяльності у 2010–2021 рр.

№	Вид діяльності	Темпи зростання у 2021 р. по відношенню до 2010 р.
1	Загальні інвестиції	412,72
2	Інформація та телекомунікації	723,76
3	Комп'ютерне програмування та надання інших інформаційних послуг	4 103,86

Джерело: розраховано за [6]

Таблиця 4

Показники зовнішньої торгівлі послугами за видами у 2022 році [6]

Найменування послуги	Експорт		Імпорт		Сальдо
	тис.дол. США	У % до 2021	тис.дол. США	У % до 2021	
Усього	9166030,3	71,7	3015092,9	37,8	6150937,4
Телекомунікаційні послуги	124207,7	121,7	91177,2	85,0	33030,6
Комп'ютерні послуги	2751703,0	87,0	239966,2	59,8	2511736,7
Інформаційні послуги	837036,6	109,0	83078,8	40,6	753957,8

нером держави та громадськості у певних проєктах захисту, про що свідчить наявний досвід нашої країни.

26.02.2022 р. Михайло Федоров, міністр цифрових технологій, проголосив створення ІТ-армії. І одразу російські ЗМІ повідомили, що «портал Держпослуг, Кремль, Держдума, 1 канал, Роскосмос і сайт РЖД зазнали безпрецедентних кібератак». Командуванням ІТ-армії є команда технічних експертів, які займаються аналізом ситуації, ефективності здійсненних атак, способів обходу інструментів та засобів російської оборони та розробляють і встановлюють нові завдання. З початку повномасштабного вторгнення українські ІТ-військо активно діють, але сама структура залишається невідомою. За даними Цюріхського центру досліджень безпеки (CSS), українська ІТ-армія виникла стихійно, без чітких планів та завдань. В результаті вони є вийнятковою гібридною структурою, що не належить жодній державній агенції. Приклад Естонії в цій сфері надихнув на створення такої спеціальності структуру для забезпечення української цифрової безпеки. Але все ж таки в Україні ІТ-армія виникла через потребу в ній та випадково. Її можна розділити на дві частини:

1. Некваліфіковані учасники-аматори, які можуть організувати DDoS-атаки на різні цілі в росії, переважно інфраструктурні.
2. Фахівці-професіонали, які здатні виконувати більш складні місії та здатні співпрацювати з військовими та урядом.

Публічно-приватні партнерства можуть розглядатися як рішення з управління кібербезпеки. Такі партнерства є інструментом для досягнення певної гнучкості та надійності системи безпеки. Карр стверджує, що публічно-приватне партнерство спричиняє «ринковий підхід» у забезпеченні кібербезпеки, яка є частиною національної безпеки [7]. В такий же спосіб публічно-приватне партнерство може бути способом «передати» обов'язки забезпечення безпеки приватному партнерові на ринкових засадах [8, с. 299].

Для забезпечення кібербезпеки державі, громадськості та приватному сектору потрібно взаємодіяти одне з одним [9]. Це знаходить своє відображення у зростаючій кількості ініціатив, в яких підкреслюється важливість партнерських відносин між публічним та приватним секторами для забезпечення кібербезпеки [10].

На сьогодні вчені стверджують, що використання механізму публічно-приватного

партнерства можливе для забезпечення кібербезпеки [3].

Висновки. В результаті проведеного дослідження визначено, що публічно-приватні партнерства використовуються для вирішення проблем суспільства, за умови відсутності можливостей у держави та наявності певних стимулів для приватного сектору. Зазначено, що механізм публічно-приватного партнерства може бути задіяний для протидії сучасним загрозам суспільної безпеці. Передача приватному сектору питань безпеки має сприяти суттєвій економії бюджетних коштів, до того ж у надзвичайних ситуаціях приватний сектор може застосовувати свої більш гнучкі зв'язки та механізми управління, в тому числі антикризового менеджменту. Аналіз розвитку сфери інформаційних технологій показав, що дана сфера достатньо стрімко розвивається і хоча відчуває вплив війни, продовжує зростати. Тому приватний сектор цієї сфери може бути суб'єктом у публічно-приватному партнерстві. Досвід України під час військової агресії росії це довів у практичній площині із створення ІТ-армії та залученням фізичних та юридичних осіб до неї. Але слід зазначити, що ці відносини були формальними та стихійними і саме публічно-приватні партнерства можуть бути формою взаємозв'язку та формалізації цих відносин. Що і може бути предметом подальших досліджень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Соціально-економічний розвиток України: просторовий, організаційно-адміністративний та ціннісний виміри : монографія / за заг. ред. В. В. Александрова, В. Б. Родченка, В. П. Третяк. Харків : ХНУ імені В. Н. Каразіна, 2018. 310 с.

2. Круглов В. В. Роль державно-приватного партнерства у сфері безпеки. *Інвестиції: практика та досвід*. 2018. № 12. С. 107–110.

3. Круглов В. В. Державно-приватне партнерство у сфері кібербезпеки. *Вчені записки ТНУ імені В. І. Вернадського*. *Серія : Державне управління*. 2018. Т. 29 (68), № 3. С. 57–61.

4. Коляда Т. А. Перспективні сфери застосування державно-приватного партнерства в Україні. *Молодий вчений*. 2016. № 12.1(40). С. 588–590.

5. Круглов В. В. Співробітництво державного та приватного секторів у сфері безпеки. *Публічне управління та адміністрування в умовах війни і в поствоєнний період в Україні*. С. 77–79.

6. Державна служба статистики України. URL: https://www.ukrstat.gov.ua/

7. Carr M. Public private partnerships in national cyber-security strategies. *International Affairs.* 2016. № 92(1). P. 43–62.

8. Bures O. Contributions of private business to the provision of security in the EU: beyond public-private partnerships. *Crime, Law and Social Change*. 2017. No. 67(3). P. 289–312.

9. Tropina T. Public-private collaboration: Cybercrime, cybersecurity and national security. Self-and co-regulation in Cybercrime, cybersecurity and national security. Springer, Cham, 2015. P. 1–41.

10. Min K. S., Chai S. W., Han M. An International Comparative Study on Cyber Security Strategy. *International Journal of Security and Its Applications*. 2015. No. 9(2). P. 13–20.

REFERENCES:

1. Aleksandrov V. V. (2018) Sotsialno-ekonomichnyi rozvytok Ukrainy: prostorovyi, orhanizatsiino-administratyvnyi ta tsinnisnyi vymiry monohrafiia [Social and Economic Development of Ukraine: Spatial, Organizational, Administrative, and Values Dimensions] monohrafiia [a monograph]. Kharkiv : KhNU. 310 p. (in Ukrainian)

2. Kruglov V. V. (2018) Rol derzhavno-pryvatnoho partnerstva u sferi bezpeky [The role of public-private partnership in the security sector] *Investytsii: praktyka ta dosvid,* no. 12, pp. 107–110. (in Ukrainian)

3. Kruglov V. V. (2018) Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky [Public-private partnership in the field of cybersecurity] *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia : Derzhavne upravlinnia.* T. 29 (68), no. 3, pp. 57–61. (in Ukrainian)

4. Kolyada T. A. (2016) Perspektyvni sfery zastosuvannia derzhavno-pryvatnoho partnerstva v Ukraini [Promising areas of application of public-private partnership in Ukraine] *Molodyy vchenyy,* no. 12.1(40), pp. 588–590. (in Ukrainian)

5. Kruglov V. V. (2018) Spivrobitnytstvo derzhavnoho ta pryvatnoho sektoriv u sferi bezpeky [Public-private cooperation in the security sector]. *Publichne upravlinnia ta administruvannia v umovakh viiny i v postvoiennyi period v Ukraini*. P. 77–79. (in Ukrainian)

6. Derzhavna sluzhba statystyky Ukrainy. [State Statistics Service of Ukraine]. URL: https://www.ukrstat.gov.ua/ (accessed December 14, 2023).

7. Carr M. (2016) Public private partnerships in national cyber-security strategies. *International Affairs,* no. 92(1), pp. 43–62.

8. Bures O. (2017) Contributions of private business to the provision of security in the EU: beyond public-private partnerships. *Crime, Law and Social Change*, no. 67(3), pp. 289–312.

9. Tropina T. (2015) Public-private collaboration: Cybercrime, cybersecurity and national security. Self-and co-regulation in Cybercrime, cybersecurity and national security. Springer, Cham, pp. 1–41.

10. Min K. S., Chai S. W., Han M. (2015) An International Comparative Study on Cyber Security Strategy. *International Journal of Security and Its Applications*, no. 9(2), pp. 13–20.