

К. А. Ніжейко,
голова правління, Міжнародна асоціація майбутнього України,
аспірант, Державний торговельно-економічний університет
ORCID ID: <https://orcid.org/0000-0002-2925-1140>

DOI: 10.32702/2306-6814.2023.22.147

ПРАКТИЧНІ ЗАСАДИ ФУНКЦІОНУВАННЯ МІЖНАРОДНИХ СТРАТЕГІЧНИХ АЛЬЯНСІВ В ІТ-СФЕРІ

К. Nizheiko,
Chairman of the board, International association for the future of Ukraine,
PhD student, State University of Trade and Economics

PRACTICAL FOUNDATIONS OF FUNCTIONING OF INTERNATIONAL STRATEGIC ALLIANCES IN THE IT

В статті наведено результати дослідження практичних основ функціонування міжнародних стратегічних альянсів (МСА) в ІТ-сфері з метою використання отриманих результатів в стратегії повоєнної відбудови України. Обґрунтовано, що МСА більше не є випадковою діяльністю у сфері маркетингу, корпоративного планування та продажів; скоріше, вони перетворилися на критичну вимогу для забезпечення високих темпів зростання міжнародного бізнесу та представлення високоякісних товарів і послуг на все більш вимогливому ринку. Ідентифіковано, що стрімкий розвиток цифрових технологій почався ще в 70-х роках ХХ століття в цивільних галузях економіки і в 50-х роках у військово-промислових комплексах розвинутих країн. Здійснено аналіз цифрового середовища функціонування глобальної економіки, проблем та переваг які вони створюють для поширення МСА в ІТ сфері та виокремлено основні елементи, які формують основи цих альянсів. Отримано висновок, що сучасний ІТ-ринок виконуючі нові завдання розвивається та здобуває новий досвід формуючі нове середовище для функціонування МСА в ІТ-сфері.

The article presents the results of a study of the practical foundations of the functioning of international strategic alliances (ISAs) in the IT sector, with a view to using the results obtained in the strategy of post-war reconstruction of Ukraine. It is substantiated that ISAs are no longer incidental activities in the field of marketing, corporate planning and sales; rather, they have become a critical requirement for ensuring high growth rates of international business and presenting high-quality goods and services in an increasingly demanding market. IT ISAs are beneficial for participants as they serve as a significant source of investment and also increase the level of support from regulators. The author identifies that the rapid development of digital technologies began in the 70s of the twentieth century in the civilian sectors of the economy and in the 50s in the military-industrial complexes of developed countries. The new business models emerging in the twenty-first century bring significant benefits and fundamental changes, and this requires adjusting old rules and forming new ones for interactions on a global scale. The author analyzes the digital environment of the global economy, the problems and advantages they create for the spread of ISAs in the IT sphere and identifies the main elements that form the foundations of these alliances: online platforms as a mechanism for creating strategic alliances with each other to exchange databases or promote each other's goods and services; cross-border data flows that allow companies to create and manage global production and global supply chains, exchange and analyze data, and facilitate communication; cybersecurity systems; and last but not least, adoption and adaptation of military developments for civilian use.

It is concluded that the modern IT market is developing and gaining new experience that shapes a new environment for the functioning of ISAs in the IT sphere — a war of technology, in weapons and military equipment for direct physical engagement, in cyber warfare through interference with systems for intelligence gathering, spreading misinformation, sabotage and suppression of information systems, as well as the means to defend from such attacks; and, in the tools of information warfare for spreading propaganda, disinformation, and creating psychological pressure on specific groups and societies as a whole.

Ключові слова: міжнародні стратегічні альянси, інформаційний технології, онлайн платформи, транс-кордонні потоки даних, кібербезпека, COVID-19, російсько-українська війна.

Key words: international strategic alliances, information technology, online platforms, cross-border data flows, cybersecurity, COVID-19, Russian-Ukrainian war.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Здатність більшості економічних суб'єктів успішно реалізовувати стратегії, що призводить до досягнення поставлених цілей, визначає їхню ймовірність успіху. Глобалізація та динамізм, які є характерними рисами економічного середовища XXI століття, створюють висококонкурентне середовище в світовій економіці (див. наприклад [4]). В цих умовах міжнародні стратегічні альянси (далі МСА) стають все більш поширеними в сучасному діловому світі, оскільки фірми об'єднують свої ресурси, прагнучи отримати конкурентну перевагу на ринку. Можна зазначити, що МСА більше не є випадковою діяльністю у сфері маркетингу, корпоративного планування та продажів; скоріше, вони перетворилися на критичну вимогу для забезпечення високих темпів зростання міжнародного бізнесу та представлення високоякісних товарів і послуг на все більш вимогливому ринку. Саме брак можливостей, знань та ресурсів на національному рівні змушує компанії обирати міжнародні стратегічні альянси (МСА) як відповідне рішення для виходу на глобальні ринки. У зв'язку з цим, вибір відповідних партнерів є фундаментальним кроком у зменшенні ризиків та витрат, пов'язаних з такими альянсами. Стрімке поширення використання в міжнародному бізнесі надбань Четвертої промислової революції ще більше перевертає увагу керівництва компаній до прийняття рішення щодо пошуку співпраці в межах МСА з використанням інформаційних технологій. Зростаюча технологічна складність, швидкий життєвий цикл продуктів і висока вартість їхньої новизни зобов'язує значну кількість компаній об'єднати зусилля у просуванні власних продуктів, розробки нових послуг, а отже, продажів і маркетингу. МСА в ІТ-сфері є вигідними для учасників, оскільки вони слугують значним джерелом інве-

стицій, а також підвищують рівень підтримки з боку регуляторних органів. Для успішної інноваційної діяльності важливий не лише обсяг ресурсів, якими володіє фірма, але й їхня різноманітність. І саме МСА в ІТ-сфері дозволяють досягти ефективної рекомбінації за рахунок різноманітних внутрішніх, в тому числі інноваційних, ресурсів партнерів альянсу, що визначає актуальність обраної теми дослідження.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Слід зазначити, що визначенню особливостей використання інформаційних технологій в міжнародному бізнесі присвячено роботи іноземних та вітчизняних вчених, таких як: Г. Андрощук, Д. Александер, Л. Антонюк, Г. Бірман, Д. Бейлі, Ю. Брігхем, Г. Дугінець, Т. Мельник, Ш. Пратг, Р. Брейлі, Р. Фостер, Б. Твісс, Л. Федулова, та багатьох інших. Дослідженню міжнародних стратегічних альянсів в світовій економіці приділяють увагу в переважній більшості іноземні вчені, такі як S. Breschi, O. Granstrand, N. Rosenberg, J. Mohr, R. Spekman, P. Patel, K. Pavitt, F. Lissoni, F. Malerba, H. Lamrani, K. Khan, K. Li, J. Qiu, J. Wang та інші. Що стосується представників українського наукового середовища, то слід відмітити результати досліджень отримані А. Габреляном, Л. Михайлішиною, І. Морозовою, О. Ісаєнко, А. Касичем, В. Ковалем, І. Кривов'язюком, С. Якубовським, О. Черновою тощо. Аналіз існуючих напрацювань вітчизняних вчених доводить, що переважно вони орієнтовані на аналіз та оцінку можливості адаптації західного досвіду. Віддаючи належне наявним науковим розробкам вітчизняних і закордонних дослідників з цієї проблематики, варто зазначити, що опубліковані на сьогодні праці не мають системного характеру та не можуть претендувати на повноту аналізу щодо розуміння особливостей функціонування МСА в ІТ-сфері в другій декаді XXI століття.



Рис. 1. Середовище цифрової економіки в другій чверті XXI ст.

Джерело: складено автором.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Метою статті є дослідження практичних основ функціонування МСА в ІТ-сфері з метою використання отриманих результатів в стратегії повоєнної відбудови України. Для досягнення мети дослідження авторами застосовано комплекс взаємодоповнюючих методів наукового пізнання: історико-логічний, системно-структурний, компаративного та статистичного аналізу, інформаційний, процесний та інституційний.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

За останні кілька десятиліть все більше і більше економічних суб'єктів розуміють, що вони не можуть вижити поодиночки через посилення глобальної конкуренції та пришвидшення темпів технологічних змін. Зростання складності продуктів і виробничих процесів з часом також змусило їх визнати нагальну потребу в альянсах (див. детально. [2; 10; 13—15; 23]). Це, в свою чергу, підтверджується еволюцією кількості стратегічних альянсів, в тому числі міжнародних, особливо в наукомістких галузях наприкінці XX століття (див. наприклад [9]). Значна кількість існуючих досліджень підтверджує висновок, що економічні суб'єкти можуть розширювати свою технологічну базу шляхом отримання додаткових джерел знань та підтримувати свої конкурентні переваги та інновації в різних галузях і країнах саме за рахунок співпраці в межах МСА (див. детально [1; 4; 11; 12; 24]).

Саме поняття цифровізація економіки та перші концепції, що описували ці процеси, з'явилися ще наприкінці XX століття, коли значної популярності стала набувати мережа Інтернет по всьому світу. Також можемо зазначити, що Четверта промислова революція, поява цифрової економіки та стрімкий розвиток Інтернет мережі це взаємопов'язані події. Звернувшись до відомого автора Nicholas Negroponte, який у 1995 році в своєму дослідженні "Цифрова революція: Причини для опти-

мізму" [16] описував основні теорії переходу від матеріального (атомів) до не матеріальних цифрових одиниць виміру (бітів) і став автором відомого висловлювання від "атомів до бітів", та враховуючі власні спостереження можна зазначити, що стрімкий розвиток цифрових технологій почався ще в 70-х роках XX століття в цивільних галузях економіки і в 50-х роках у військово-промислових комплексах розвинутих країн. Перші цифрові мережі передавання даних у військовій сфері вже функціонували з початку 50-х років, при тому що сильний поштовх для розвитку цифрових технологій в ВПК, які потім перейшли до цивільних галузей економіки, спричинила Друга Світова Війна. Отож, початок Третньої промислової революції можна визначити як перехід цифрових технологій військового призначення в цивільні сфери економіки. Зокрема можна вважати початком процесу цифровізації виставковий захід у Нью-Йорку в 1964 році, на якому завдяки доступу до технологій, був представлений широкому загалу перший настільний програмований калькулятор-комп'ютер з можливістю запису на носії інформації "Programma 101". Цей винахід набув значної популярності в тих сферах господарювання, де були потрібні складні розрахунки та аналітика. І одразу на виставковому заході було укладено договір про співробітництво між Італійським виробником цього винаходу компанією "Olivetti" та компанією "General Electric". Це був один з перших міжнародних стратегічних альянсів, яких допоміг стрімко поширити винахід на світовому ринку та отримати значні прибутки від партнерства і подальший сталий розвиток співпраці (див. детально [6]). Найближчий конкурент компанія Hewlett Packard's змогла тільки через три роки виготовити подібний зразок обладнання і це був програмований калькулятор-комп'ютер 9100A. Але за три роки основні ринки збуту та цільова аудиторія споживачів вже була майже втрачена.

В XXI столітті, з поширенням результатів Четвертої промислової революції, все більша частка глобальної економічної діяльності забезпечується цифровими тех-

нологіями. Виникаючи в цьому середовищі нові бізнес-моделі приносять суттєві переваги та фундаментальні зміни, і це вимагає зміни старих і формування нових правил взаємодії у глобальному масштабі. Основні цифрові інструменти функціонування глобальної економіки наведено на рис. 1 Розглянемо яким чином ці інструменти формують основу для функціонування МСА в ІТ-сфері враховуючи те, що з початку 2020 року в період глобальної пандемії світова економіка зазнає значних потрясінь та екстремального переформатування і новий поштовх в розвитку ІТ-технологій. Трансформаційні зрушення поглибилися після початку повномасштабної збройної агресії РФ на території України.

Онлайн-платформи дозволяють проводити транзакції та взаємодію між кількома різними групами користувачів по всьому світу. Вони відкривають ринки та можливості для споживачів і бізнесу, в тому числі між невідомими сторонами. Однак вони викликають занепокоєння щодо конкуренції та захисту споживачів. Фрагментована політика та регуляторні заходи призводять до витрат і невизначеності для фірм і споживачів і вимагають транснаціональної координації. Об'єднання користувачів по всьому світу сприяє глобальній економічній діяльності шляхом надання компаніям доступу до більшої кількості ринків, а споживачам — до більшої кількості контенту та продуктів. Хоча рання цифрова екосистема була перепоповнена підприємницькою енергією, зростає занепокоєння, що цей динамізм зменшився, а існуючі платформи вкоренилися. Вчені-юристи та економісти відзначають, що ринкова влада цифрових компаній зростає, водночас зростає занепокоєння щодо захисту прав споживачів в Інтернеті (див. детально [17; 18; 20]). За результатами проведеного аналізу можна навести фактори, що сприяють цьому зростанню:

- Сильні мережеві ефекти. Зі збільшенням кількості користувачів цінність продукту для них зростає, залучаючи інших користувачів. Це може призвести до "перекидання" ринку до монополії (також відомого, як ефект "переможець отримує все") [18].

- Економія на масштабах. Оскільки ціна додавання додаткового користувача часто є низькою, платформи можуть легко масштабуватися і розширювати своє географічне покриття без значних додаткових інвестицій.

- Збір даних. Онлайн-платформи можуть збирати детальну інформацію від користувачів з усіх сторін ринку, включаючи споживачів, рекламодавців та інші компанії. Ці дані можуть підвищити якість продукції, посилити мережеві ефекти, націлити продукти на різні аудиторії та керувати процесом прийняття рішень споживачами [19]. У поєднанні з масштабом, перевага наявних онлайн-платформ у даних може створити бар'єр для входу на ринок інших [17].

- Вертикальна інтеграція, конгломерати та міжринкові зв'язки. Онлайн-платформи часто об'єднують кілька цифрових продуктів, таких як операційні системи та пристрої, в єдину пропозицію, що базується на даних, і це може ускладнити для споживачів зміну постачальника [17]. Вони також можуть скористатися своїм домінуючим становищем на одному ринку, наприклад, використовуючи свої дані або пакетні пропо-

зиції, щоб вийти на інший на інший. Деякі онлайн-платформи мають вертикально інтегровані бізнес-моделі, що може змусити конкурентів, які знаходяться нижче за течією, покладатися на них у доступі до клієнтів, що може призвести до скарг на антиконкурентну поведінку (наприклад, коли платформа конкурує з конкурентами, що знаходяться нижче за течією на ринку, на якому вона працює) [20].

У відповідь на це багато країн адаптували традиційні інструменти правозастосування, підвищили технічну спроможність органів влади та надали пріоритет застосуванню законів про конкуренцію та захист прав споживачів на цифрових ринках. Крім того, часто звертаючи увагу на структурні характеристики цифрових ринків, які можуть призвести до концентрації, багато правових компетенцій вийшли за межі традиційних інструментів, пропонуючи або впроваджуючи додаткові регуляторні ініціативи, які застосовуються до обмеженого кола компаній, зазвичай до найбільших онлайн-платформ. Хоча ці нормативні акти відрізняються, вони, як правило, спрямовані на вирішення певних проблем [20]:

- Проблеми, пов'язані з даними, включаючи зобов'язання надавати конкурентам доступ до важливих наборів даних та впроваджувати заходи з перенесення та інтероперабельності даних.

- Сприйняття онлайн-платформ як "вартових", включаючи заходи, пов'язані з обмеженням самостійного надання переваг власним товарам і послугам, а також пакетуванню.

- Зобов'язання щодо прозорості та чесної ділової практики, включаючи обов'язкові кодекси поведінки та вимоги до прозорості алгоритмів, ділових і рекламних практик та збору даних. Деякі запропоновані правила обмежують способи зберігання спостережуваних або передбачуваних даних користувачів, оброблятися або передаватися.

- Додаткові вимоги до злиття, включаючи зобов'язання інформувати регуляторів про всі відповідні злиття та поглинання.

Хоча регуляторні акти в цій сфері мають певні спільні риси і всі вони спрямовані на сприяння конкуренції в Інтернеті, вони суттєво відрізняються в різних юрисдикціях. В іншому випадку, фрагментарне політичне та регуляторне середовище для платформ призводить до витрат як для фірм, так і для споживачів, збільшує невизначеність і може перешкоджати інноваціям, спрямованим на підвищення добробуту [20]. Крім того, оскільки найбільші онлайн-платформи є глобальними, наслідки регулювання в одній юрисдикції може поширюватися на інші. Тому узгоджений глобальний підхід має підвищити ефективність регулювання та гарантуватиме, що цифрові ринки залишатимуться конкурентними, змагальними та сприятимуть економічному добробуту.

Платформи часто надають нові високоякісні продукти та послуги за низькими цінами або навіть безкоштовно (хоча іноді в обмін на збір даних). За рахунок цього онлайн-платформи підірвали існуючі аналогові бізнеси та уможливили поширення інформації, яка допомагає споживачам робити поінформований вибір, у тому числі переключатися між товарами, послугами та постачальниками [18]. У підсумку, аналізуючи принцип дії онлайн

платформи можна зробити висновок, що вони є механізмом створення між собою стратегічних альянсів для обміну базами даних або просування товарів та послуг одна одної.

На початку поширення мережі Інтернет експериментальні бізнес-моделі швидко з'являлися і швидко занепадали [7]. Однак з середини 1990-х років кілька онлайн-платформ стали загальновідомими, привертаючи увагу, навички, дані та доходи. Хоча онлайн-платформи відрізняються за розміром, кількістю користувачів та функціональністю [22], політика та суспільні інтереси зосереджені на цій групі цифрових гігантів у питаннях від приватності до модерації контенту та посередництва на ринку праці. Оскільки ця група займає ліву частку основних онлайн ринків, включаючи електронну комерцію, пошук, онлайн-рекламу та соціальні мережі [18], їхній вплив на конкуренцію став предметом особливої уваги.

Транскордонні потоки даних, які в тому числі переміщуються в межах цих онлайн-платформ та дозволяють компаніям створювати та керувати глобальним виробництвом та глобальними ланцюгами поставок, обмінюватися та аналізувати дані, а також сприяти комунікації. Однак вони посилюють проблеми в галузі інформаційної політики, змушуючи уряди вживати відповідні політичні та регуляторні заходи, що регулюють потоки даних. Приймаючи ті чи інші норми потрібно оцінити ці зміни і переконатися, що фрагментація, відсутність прозорості, регуляторної чіткості та ясності в регулюванні не обмежують економічні можливості і не підривають цілі цих правил та не перешкоджають досягненню цілей, яким покликані служити ці регуляторні норми. Архітектура Інтернету дозволяє безперешкодно передавати дані між мережевими пристроями в будь-якій точці світу, уможливаючи координацію глобальних ланцюгів створення вартості та транскордонне надання послуг. Однак уряди все частіше приймають регуляторні та політичні заходи, які регулюють передачу даних між юрисдикціями. Користувачі Інтернету все частіше відчувають, що за ними стежать в Інтернеті. Це робить захист приватного життя ключовим питанням, поряд із захистом прав інтелектуальної власності та іншими питаннями публічних політик, в тому числі питанням цифрової безпеки.

ІТ-безпека високого рівня — це основа успішної цифрової трансформації та її подальшого сталого розвитку. Однак вибуховий темп цифрової трансформації не супроводжується таким же прогресом у сфері безпеки онлайн-сервісів та пов'язаних з ними продуктів. Кінцеві користувачі майже не можуть оцінити достатні підходи до безпеки, що призводить до ринкових збоїв, які підривають довіру споживачів і ставлять під загрозу систему. Багато викликів, що стоять перед цифровою безпекою, є міжнародними, оскільки вразливості та погані практики повинні вирішуватися в глобальному масштабі, щоб досягти максимального впливу. Без цифрової безпеки окремі особи та організації не могли б впевнено взаємодіяти з цифровими продуктами та послугами, які дедалі більше впливають на міжнародне виробництво та торгівлю. Оскільки все більша частина економіки покладається на цифрові технології, ставки на цифрову безпеку зростають: погана безпека може

призвести до емоційної, фінансової та фізичної шкоди в безпрецедентних масштабах.

Так, наприклад відносно невелика кількість зловмисників змогла скористатися перевагами цифрової трансформації використовуючи бізнес-моделі кіберзлочинності, які намагаються обійти традиційні правоохоронні органи. Програми-вимагачі стали поширеною загрозою, що впливає на всі типи підприємств та організацій, незалежно від їхнього розміру та місцезнаходження. У США в 2021 році оператори критичної інфраструктури подали 649 скарг до ФБР, а 14 з 16 секторів критичної інфраструктури з яких щонайменше один учасник став жертвою атаки з використанням програмного забезпечення з вимогою викупу [5]. Аналогічно, інформаційні системи мають вразливості, пов'язані з тим, як розробляється, впроваджується та оновлюється програмне забезпечення. Зловмисники розробляють, продають і використовують такі інструменти, як шкідливе програмне забезпечення, щоб використовувати ці вразливості через інциденти, які завдають шкоди бізнесу, урядам і приватним особам, загрожують критично важливим видам діяльності та підривають довіру до цифрової трансформації.

Збитки від незахищеної цифрової екосистеми можуть бути величезними. За оцінками експертів, потенційні глобальні збитки від кібератак зросли до 6 трильйонів доларів США на рік (що дорівнює сукупному ВВП Франції та Німеччини) і зростають щороку [21]. Зловмисники шукають жертв, залежних від цифрових технологій. За даними CyberPeace Institute, 253 інциденти в 32 країнах у 2021 році вплинули на сектор охорони здоров'я, в середньому понад 21 день операційного впливу та понад 13 мільйонів порушених записів [3].

Оскільки все більше галузей світової економіки покладаються на цифрові технології, увага до цифрової безпеки зростає, оскільки ефективна безпекова система забезпечує довіру до цифрової трансформації та її поширення. Хоча було досягнуто певного прогресу в нормалізації передового досвіду (наприклад скоординоване управління вразливостями або вимоги до безпеки для Інтернету речей), ці базові вимоги не були впроваджені установами на всіх рівнях. Зараз у регуляторів по всьому світу з'явилася можливість вирішити ці міжнародні проблеми, зосередившись на бажаних результатах для кінцевого користувача і спираючись на глобальні технічні стандарти і кращі галузеві практики для посилення інтероперабельності.

Ескалація кіберзлочинності та онлайн-шахрайства під час пандемії COVID-19 зробило прийняття надійних законів у поєднанні з ефективними механізмами правозастосування ще більш нагальним. І ці тенденції тільки посилилися з початком повномасштабної війни росії з Україною та стала звичним явищем новітнього світу. Війна зумовила переформатування існуючих платформ і сервісів під військову тематику, а також появу нових платформ та сервісів, як від нових власників, так і розширення сфери діяльності вже існуючих. А з відміною коронавірусу взагалі переформатувались тільки на військову тематику і з перших днів нападу рф на Україну поруч з основними цифровими інструментами функціонування глобальної економіки світу стає військове ІТ. Основні цифрові інструменти

економік більшості країн світу набувають нових значень та змінюють свої регуляторні політики. Зокрема це пов'язано з санкціями проти країни-агресорки. Серед ключових змін цифрових інструментів в останні два роки слід відзначити:

— Онлайн-платформи закривають свої сервіси, товари та інш. для санкційних країн-користувачів.

— Транскордонні потоки даних формують кордони з певними країнами і не передаються на санкційні країни.

— IT-безпека стає більш жорсткою і направлена проти прямих та непрямих кібератак країни-агресорки та країн, що її підтримують.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Отже сучасний IT-ринок виконуючі нові завдання розвивається та здобуває новий досвід формуючи нове середовище для функціонування МСА в IT-сфері: війна технологій в озброєнні та військовій техніці через пряме фізичне знищення та знешкодження ворога і його техніки; кібервійна через втручання в роботу систем для збору розвідданих, поширення хибної інформації, хибної роботи або виведення їх з ладу, також це включає захист своїх систем від втручання в них ворога, інформаційна війна через поширення пропаганди, недостовірних новин та створення психологічного тиску на ворога.

Як при COVID-19, так і при широкомасштабному вторгненню росії на територію України можна підтвердити поширення такого явища як Екстремальні (надзвичайні) МСА. Про їх умови створення, подальшого функціонування та виконання свого призначення буде присвячено наступні дослідження. Зазначимо лише, що така форма МСА це результат стрімкого розвитку цифрових інструментів світової економіки більш ніж на 5 років вперед при пандемії. А саме початку поширення IT-технологій, що розвинулись при COVID-19 і вже задіяні у військовій галузі, наслідком чого є розвиток R&D IT-сектору в Україні, а також за її межами, з акцентом на військову сферу. І за попередньою авторською оцінкою таки альянси перевищать світові показники розвитку МСА до 2020 року, що є головним напрямом подальших досліджень автора.

Література:

1. Belderbos, R.; Cassiman, B.; Faems, D.; Leten, B. & Van Looy, B. (2014), 'Co-ownership of intellectual property: Exploring the value-appropriation and value-creation implications of co— patenting with different partners', *Research policy* 43(5), 841—852.
2. Breschi, S.; Lissoni, F. & Malerba, F. (2003), Knowledge-relatedness in firm technological diversification, *Research policy* 32(1), 69-87. [https://doi.org/10.1016/S0048-7333\(02\)00004-5](https://doi.org/10.1016/S0048-7333(02)00004-5)
3. Cyber Peace Institute (2021) Playing with Lives: Cyberattacks on Healthcare are Attacks on People <https://cyberpeaceinstitute.org/publications/sar001-healthcare/>
4. Dahlander, L. & Gann, D. M. (2010), 'How open is innovation?', *Research policy* 39(6), 699—709.

5. FBI (2021), Internet Crime Report, U.S. Federal Bureau of Investigation, Washington, DC, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

6. From Bits to Atoms: Co-Creating the Third Industrial Revolution <https://bigthink.com/articles/from-bits-to-atoms-co-creating-the-third-industrial-revolution/>

7. Furman, J. et al. (2019), Unlocking digital competition: Report from the Digital Competition Expert Panel, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.

8. Hameed, K., & Arshed, N. (2021). On globalization and Business Competitiveness: A panel data country classification. *Studies of Applied Economics*, 39 (2), 1—27. <https://doi.org/10.25115/eea.v39i2.3586>

9. Hagedoorn, J. (1993), 'Understanding the rationale of strategic technology partnering: Nterorganizational modes of cooperation and sectoral differences', *Strategic management journal* 14(5), 371-385.

10. Granstrand, O.; Patel, P. & Pavitt, K. (1997), 'Multitechnology corporations: why they have "distributed" rather than "distinctive core" competencies', *California management review* 39 (4), 8—25. <https://doi.org/10.2307/4116590>

11. Granstrand, O. (2000). Corporate innovation systems. A Comparative Study of Multi-Technology Corporations in Japan, Sweden and the USA, Chalmers University of Technology.

12. Granstrand, O. (2003), Innovations and Intellectual Property Studies' *Economics, law and intellectual property*, Springer, pp. 9—40.

13. Li, K., Qiu, J., & Wang, J. (2019). Technology conglomeration, strategic alliances, and corporate innovation. *Management Science*, 65 (11), 5065—5090. <https://doi.org/10.1287/mnsc.2018.3085>

14. Lamrani, H. C., & Khan, K. (2020) Drivers of Strategic Alliances: The Influence of Technological Diversification and Operational Efficiency. *Journal of Innovative Research in Management Sciences*, 1—11. <https://www.agasr.org/index.php/jirms/article/view/14>

15. Mohr, J. & Spekman, R. (1994), 'Characteristics of partnership success: partnership attributes, communication behavior, and conflict resolution techniques', *Strategic management journal* 15 (2), 135—152. <https://doi.org/10.1002/smj.4250150205>

16. Negroponte, N. (1995). The digital revolution: Reasons for optimism. *The Futurist*, 29 (6), 68.

17. OECD (2022a), "The Evolving Concept of Market Power in the Digital Economy", OECD Competition Policy Roundtable Background Note, <https://www.oecd.org/daf/competition/the-evolvingconcept-of-market-power-in-the-digital-economy-2022.pdf>.

18. OECD (2022b), OECD Handbook on Competition Policy in the Digital Age, <https://www.oecd.org/daf/competition/oecd-handbook-on-competition-policy-in-the-digitalage.pdf>.

19. OECD (2022c), "Dark Commercial Patterns Online", OECD Digital Economy Papers, No. 336, <https://doi.org/10.1787/44f5e846-en>.

20. OECD (2021a), "Ex Ante Regulation and Competition in Digital Markets", OECD Competition Committee Discussion Paper, <https://www.oecd.org/daf/competition/ex-ante-regulation-andcompetition-in-digital-markets-2021.pdf>.

21. OECD (2021b), "Smart Policies for Smart Products: A Policy Maker's Guide to Enhancing the Digital Security of Products", STI Policy Note, OECD Publishing, Paris, <https://www.oecd.org/digital/smart-policies-for-smart-products.pdf>

22. OECD (2019), An Introduction to Online Platforms and Their Role in the Digital Transformation, OECD Publishing, Paris, <https://doi.org/10.1787/53e5f593-en>

23. Rosenberg, N. (1976). Perspectives on technology. (No Title). <https://doi.org/10.1017/CBO9780511-561313>

24. Zhang, G., & Tang, C. (2018). How R&D partner diversity influences innovation performance: an empirical study in the nano-biopharmaceutical field. *Scientometrics*, 116 (3), 1487—1512.

References:

1. Belderbos, R. Cassiman, B. Faems, D. Leten, B. & Van Looy, B. (2014), "Co-ownership of intellectual property: Exploring the value-appropriation and value-creation implications of co— patenting with different partners", *Research policy*, vol. 43 (5), pp. 841—852.

2. Breschi, S. Lissoni, F. & Malerba, F. (2003), "Knowledge-relatedness in firm technological diversification", *Research policy*, vol. 32 (1), pp. 69—87. [https://doi.org/10.1016/S0048-7333\(02\)00004-5](https://doi.org/10.1016/S0048-7333(02)00004-5)

3. Cyber Peace Institute (2021), "Playing with Lives: Cyberattacks on Healthcare are Attacks on People", available at: <https://cyberpeaceinstitute.org/publications/sar001-healthcare/> (Accessed 25 Oct 2023).

4. Dahlander, L. & Gann, D. M. (2010), "How open is innovation?", *Research policy*, vol. 39 (6), pp. 699—709.

5. FBI (2021), Internet Crime Report, U.S. Federal Bureau of Investigation, Washington, DC, USA, available at: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (Accessed 25 Oct 2023).

6. BIG THINK (2012), "From Bits to Atoms: Co-Creating the Third Industrial Revolution", available at: <https://bigthink.com/articles/from-bits-to-atoms-co-creating-the-third-industrial-revolution/> (Accessed 25 Oct 2023).

7. Furman, J. et al. (2019), "Unlocking digital competition: Report from the Digital Competition Expert Panel", available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf (Accessed 25 Oct 2023).

8. Hameed, K., & Arshed, N. (2021), "On globalization and Business Competitiveness: A panel data country classification", *Studies of Applied Economics*, vol. 39 (2), pp. 1—27. <https://doi.org/10.25115/eea.v39i2.3586>

9. Hagedoorn, J. (1993), "Understanding the rationale of strategic technology partnering: Nterorganizational modes of cooperation and sectoral differences", *Strategic management journal*, vol. 14 (5), pp. 371—385.

10. Granstrand, O. Patel, P. & Pavitt, K. (1997), "Multi-technology corporations: why they have "distributed"

rather than "distinctive core" competencies", *California management review*, vol. 39 (4), pp. 8—25. <https://doi.org/10.2307/4116590>

11. Granstrand, O. (2000), *Corporate innovation systems. A Comparative Study of Multi-Technology Corporations in Japan, Sweden and the USA*, Chalmers University of Technology, Gothenburg, Sweden.

12. Granstrand, O. (2003), "Innovations and Intellectual Property Studies", *Economics, law and intellectual property*, Springer, pp. 9—40.

13. Li, K., Qiu, J., & Wang, J. (2019). "Technology conglomeration, strategic alliances, and corporate innovation", *Management Science*, vol. 65 (11), pp. 5065—5090. <https://doi.org/10.1287/mnsc.2018.3085>

14. Lamrani, H. C., & Khan, K. (2020) "Drivers of Strategic Alliances: The Influence of Technological Diversification and Operational Efficiency", *Journal of Innovative Research in Management Sciences*, vol. 1—11, available at: <https://www.agasr.org/index.php/jirms/article/view/14> (Accessed 25 Oct 2023).

15. Mohr, J. & Spekman, R. (1994), "Characteristics of partnership success: partnership attributes, communication behavior, and conflict resolution techniques", *Strategic management journal*, vol. 15 (2), pp. 135—152. <https://doi.org/10.1002/smj.4250150205>

16. Negroponte, N. (1995), "The digital revolution: Reasons for optimism", *The Futurist*, vol. 29(6), no. 68.

17. OECD (2022), "The Evolving Concept of Market Power in the Digital Economy", OECD Competition Policy Roundtable Background Note, available at: <https://www.oecd.org/daf/competition/the-evolvingconcept-of-market-power-in-the-digital-economy-2022.pdf> (Accessed 25 Oct 2023).

18. OECD (2022), "OECD Handbook on Competition Policy in the Digital Age", available at: <https://www.oecd.org/daf/competition/oecd-handbook-on-competition-policy-in-the-digitalage.pdf> (Accessed 25 Oct 2023).

19. OECD (2022), "Dark Commercial Patterns Online", OECD Digital Economy Papers, vol. 336, <https://doi.org/10.1787/44f5e846-en>.

20. OECD (2021), "Ex Ante Regulation and Competition in Digital Markets", OECD Competition Committee Discussion Paper, available at: <https://www.oecd.org/daf/competition/ex-ante-regulation-andcompetition-in-digital-markets-2021.pdf> (Accessed 25 Oct 2023).

21. OECD (2021), "Smart Policies for Smart Products: A Policy Maker's Guide to Enhancing the Digital Security of Products", STI Policy Note, OECD Publishing, Paris, available at:). <https://www.oecd.org/digital/smart-policies-for-smart-products.pdf> (Accessed 25 Oct 2023).

22. OECD (2019), An Introduction to Online Platforms and Their Role in the Digital Transformation, OECD Publishing, Paris, <https://doi.org/10.1787/53e5f593-en>

23. Rosenberg, N. (1976), *Perspectives on technology*, Cambridge University Press, Cambridge, UK. <https://doi.org/10.1017/CBO9780511561313>

24. Zhang, G., & Tang, C. (2018), "How R&D partner diversity influences innovation performance: an empirical study in the nano-biopharmaceutical field", *Scientometrics*, vol. 116 (3), pp. 1487—1512.

Стаття надійшла до редакції 05.11.2023 р.