DOI: https://doi.org/10.32782/2524-0072/2024-68-6

УДК 332.146

РОЛЬ ТРАНСФЕРУ ТЕХНОЛОГІЙ У ЗМІЦНЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ВИКЛИКИ ТА МОЖЛИВОСТІ

THE ROLE OF TECHNOLOGY TRANSFER IN STRENGTHENING NATIONAL SECURITY CHALLENGES AND OPPORTUNITIES

Васильєва Надія Борисівна
кандидат економічних наук, доцент,
Український Католицький університет
ORCID: https://orcid.org/0009-0003-0289-8045

Теребух Марта Іванівна
кандидат економічних наук, доцент,
Львівський національний університет імені Івана Франка
ORCID: https://orcid.org/0000-0002-2918-0581

Моторнюк Уляна Іванівна
кандидат економічних наук, доцент,
Національний університет «Львівська політехніка»
ORCID: https://orcid.org/0000-0002-8628-3560

Vasylieva Nadiia
Ukrainian Catholic University

Terebukh Marta
Ivan Franko National University of Lviv

Motorniuk Uliana
Lviv Polytechnic National University

Стаття присвячена значенню міжнародного трансферу технологій у зміцненні національної безпеки в умовах зростання глобальних загроз, таких як кіберзлочинність, енергетичні кризи та військові конфлікти. Проаналізовано потребу країн у новітніх технологіях для підвищення обороноздатності та стабільності критичної інфраструктури. Розглянуто ключові міжнародні програми з метою оцінки їхнього впливу на безпеку, кіберстійкість та енергетичну незалежність країн-учасників. Визначено актуальні виклики та можливості трансферу технологій для забезпечення національної безпеки, зокрема у контексті міждержавної співпраці. Окреслено перспективи подальших досліджень для адаптації інноваційних моделей взаємодії, що враховують специфічні потреби окремих країн і регіонів.

Ключові слова: трансфер технологій, національна безпека, кібербезпека, оборонні технології, енергетична безпека, міжнародне співробітництво, новітні технології.

The article is devoted to the importance of international technology transfer in strengthening national security in the face of growing global threats, such as cybercrime, energy crises, and military conflicts. The countries' need for the latest technologies to increase the defense capability and stability of critical infrastructure was analyzed. Key international programs are considered in order to assess their impact on security, cyber resilience and energy independence of the participating countries. Current challenges and opportunities for technology transfer to ensure national security, in particular in the context of interstate cooperation, are identified. Prospects for further research to adapt innovative models of interaction that take into account the specific needs of individual countries and regions are outlined. The main results demonstrated that the integration of artificial intelligence technologies, advanced defense systems and smart energy solutions allows countries to reduce dependence on traditional resources, strengthen cyber defense and ensure a rapid response to potential threats. Prospects for further research are aimed

at improving the mechanisms of international technology transfer, as well as at developing innovative cooperation models that take into account the specific needs of individual countries and regions in order to ensure effective adaptation of advanced technologies. Modern approaches to the integration of defense, cybernetic and energy technologies, which contribute to increasing the level of national security through the joint efforts of partner countries, are considered. The role of international organizations, such as NATO, the EU, and the International Energy Agency, in supporting technological exchange and developing common standards for the protection of critical infrastructure is analyzed. The importance of international regulation and standardization for the effective use of advanced technologies in the field of security is emphasized.

Keywords: technology transfer, national security, cyber security, defense technologies, energy security, international cooperation, emerging technologies.

Постановка проблеми. Міжнародний трансфер технологій став критично важливим для забезпечення національної безпеки держав, оскільки новітні загрози, такі як кіберзлочинність, енергетичні кризи та збройні конфлікти, вимагають постійного впровадження інноваційних рішень. Традиційні підходи до забезпечення національної безпеки стають менш ефективними в умовах стрімкого розвитку технологій, що створює потребу в розробці сучасних методів захисту. Сучасні виклики потребують інтеграції технологій штучного інтелекту, кіберзахисту та «розумних» енергетичних систем, які не тільки сприяють посиленню обороноздатності, а й забезпечують стійкість критичної інфраструктури. Основна проблема полягає в необхідності розробки гнучких моделей міжнародного співробітництва, які дозволять країнам адаптувати новітні технології відповідно до національних умов і потреб. Дослідження спрямоване на вивчення основних механізмів технологічного обміну між державами й визначення шляхів для підвищення надійності систем національної безпеки в умовах постійного розвитку глобальних загроз.

Аналіз останніх досліджень і публікацій. У науковій літературі значну увагу було приділено різним аспектам забезпечення національної безпеки через впровадження технологічних інновацій. Наприклад, дослідження таких авторів, як Аль Гаффар [1], Граттон П. [4], Хаммонд-Еррі М. [5], Клочко О. і Семенець-Орлова І. [6], Кобко Є. [7], Пратіві А. Ч. і Таріган Г. [13] та Яровий Т. та ін. [16], розглянули питання інтеграції технологій штучного інтелекту, хмарних обчислень, блокчейн-рішень та квантових обчислень у процеси національної безпеки. Наукові праці показують, що новітні технології, зокрема у сфері кібербезпеки та управління даними, можуть суттєво підвищити ефективність національної безпеки та забезпечити стійкість держав до зовнішніх та внутрішніх загроз. Попри різнобічні дослідження, актуальними залишаються питання інтеграції технологічних рішень у різних країнах. Важливим є створення ефективних моделей міжнародного обміну інноваціями для адаптації до специфічних умов безпеки.

Виділення невирішених раніше частин загальної проблеми. Попри наявність численних досліджень, залишаються нерозв'язаними кілька важливих аспектів у сфері міжнародного трансферу технологій для безпеки. Зокрема, мало уваги приділяється розробці універсальних методів інтеграції різних видів технологій у національні системи безпеки, враховуючи індивідуальні потреби держав і регіонів. Відсутність єдиних стандартів і нормативів, що регулюють технологічний обмін у галузі національної безпеки, знижує ефективність інтеграції передових рішень у державні структури. Недостатньо вивчено вплив міжнародних організацій НАТО та ЄС на процеси адаптації технологій безпеки у країнах-партнерах. Стаття зосереджується на виявленні можливостей для підвищення стійкості систем національної безпеки через технологічний обмін.

Формулювання цілей статті (постановка завдання). Метою статті є аналіз сучасних підходів до трансферу технологій у галузі національної безпеки та визначення шляхів покращення міжнародного співробітництва. Основним завданням дослідження стало вивчення можливостей для розробки універсальних стандартів і протоколів обміну інноваційними рішеннями для національної безпеки, надання оцінки впливу передових технологій: штучного інтелекту, квантових обчислень, наноматеріалів, сучасних систем цифрового зв'язку, розумної робототехніки, систем кіберзахисту та військових розробок на стійкість держав. Стаття також має на меті виокремити напрямки подальших досліджень для розробки інноваційних моделей співпраці, що дозволять адаптувати сучасні технології до специфічних умов та потреб різних країн.

Виклад основного матеріалу дослідження. Трансфер технологій для зміцнення національної безпеки означає передачу знань, інноваційних рішень та обладнання з однієї країни до іншої з метою підвищення обороноздатності, кібербезпеки та стабільності критичної інфраструктури. Поняття охоплює як передавання окремих компонентів технологій, так і повну інтеграцію систем оборонного або інфраструктурного характеру. Залежно від конкретних потреб країни, трансфер може включати як готові продукти, так і технічні знання (ноу-хау), що забезпечує доступ до сучасних технологій та можливість створення аналогічних рішень у майбутньому. Національна безпека потребує інноваційного підходу через поширення глобальних проблем: тероризм, гібридні загрози, кіберзлочинність. Перераховані тенденції роблять трансфер технологій важливою частиною сучасних міжнародних відносин [5, с. 28].

Розвиток систем трансферу технологій протягом останніх десятиліть значно прискорився завдяки глобалізації, а також демократизації та консьюмерізації технологічних рішень і привели до їх здешевлення та доступності. Технології для національної безпеки, які були раніше зосереджені лише в межах однієї країни, тепер можуть швидко поширюватися серед союзників і партнерів. Дане прискорення стало можливим через спільні оборонні проєкти, науково-технічні альянси та міжнародні організації, які спеціалізуються на стандартизації та безпеці. Однак важливим залишається питання контролю над передачею стратегічних технологій, оскільки їх поширення може нести як вигоду, так і ризики, включаючи можливе використання цих технологій проти країни-донора в разі зміни міжнародної політичної ситуації.

Функціонування трансферу технологій потребує чіткої регламентації та міжнародної підтримки, яка забезпечує узгодження технічних стандартів і безпеки. Країни НАТО застосовують стандартизацію та спільні програми навчання для підвищення взаємосумісності оборонних систем, що підвищує їхню ефективність у разі військових конфліктів. З економічної точки зору трансфер технологій підтримується інвестиціями у створення місцевих виробничих центрів, що дозволяє адаптувати оборонні технології до місцевих потреб і зменшує залежність від імпорту в довгостроковій перспективі [13].

Історично міжрегіональна взаємодія у сфері трансферу технологій мала різні форми та адаптувалася до політичних умов свого часу. У XX столітті розвиток оборонних технологій у США, СРСР, Європі та Китаї привів до створення стратегічних альянсів, які базувалися на обміні військовими технологіями [4, с. 54]. Наприклад, під час Холодної війни країни Варшавського договору активно обмінювалися технологіями з СРСР, тоді як країни НАТО розвивали тісне технологічне співробітництво зі США. У сучасному світі таке співробітництво стало ще більш складним та інтегрованим, охоплюючи традиційні оборонні технології та цифрові та енергетичні рішення. Війна в Україні протягом 2022–2024 років спричинила активізацію світових організацій та лідерів в технологічному протистоянні. Основними серед них є технології військових розробок та інноваційні засоби функціонування держави, які більш детально окреслено в табл. 1.

Україна може суттєво посилити обороноздатність, співпрацюючи з країнами, що мають передові технології у сфері національної безпеки: США, Ізраїль, Велика Британія, Швеція, Німеччина, Франція та Італія [6, с. 19]. Військова підтримка від цих держав, зокрема передача технологій та інноваційного обладнання, здатна покращити ефективність військових операцій. Застосування сучасних антидронових систем Rafael Drone Dome (Ізраїль) або автономних безпілотників Taranis UCAV (Велика Британія) допоможе захистити критичні об'єкти і забезпечити контроль над переміщенням ворога. Удосконалення систем цілевказування та патрулювання за допомогою JETS та DARPA Sea Hunter (США) дозволить Україні суттєво покращити оборонні позиції. Одноразова передача технології може бути корисна лише в дуже короткостроковому проміжку часу, оскільки ворогуюча країна адаптується дуже швидко до нових технологій і з'являється термінова потреба у постійних оновленнях та нових генераціях продуктів і технологій в цілому.

Кібербезпека є важливим елементом оборонної системи, оскільки сучасні конфлікти включають як фізичні, так і цифрові загрози. Для ефективного захисту необхідно враховувати не лише технічні аспекти, але й забезпечити право власності на інтелектуальні розробки. Одним з таких рішень є приклад Фінляндії, яка розробила платформу Cyber Range Finland, що дозволяє проводити навчання з кіберзахисту та моделювати сценарії кіберзагроз, може стати незамінним рішенням також і для сучасної війни, яка відбувається в Україні [7, с. 56].

Таблиця 1

Інноваційні технології для зміцнення національної безпеки: міжнародний досвід

Назва технології	Рік заснування	Країна	Технічні параметри	Призначення
DARPA Sea Hunter	2016	США	Автономний корабель, довжина – 40 м, швидкість – 27 вузлів	Патрулювання прибережних зон, виявлення підводних човнів.
Cyber Range Finland	2017	Фінляндія	Віртуальна платформа, до 1 000 користувачів	Тренування кіберзахисту, моделювання кіберзагроз.
Rafael Drone Dome	2016	Ізраїль	Антидронова система, радіус – 3,5 км	Захист об'єктів від дронів.
Sentinel R1	2008	Велика Британія	Радіолокаційна платформа, дальність – 9 600 км	Повітряна розвідка та спостереження.
JETS (Joint Effects Targeting System)	2018	США	Портативний лазерний цілевказівник, точність – 1 м	Маркування цілей для авіаційних та артилерійських ударів.
SAAB Giraffe 4A	2014	Швеція	Мультифункціональний радар, радіус – 280 км	Моніторинг повітряних і наземних загроз.

Джерело: розроблено авторами

Співпраця з розвиненими країнами сприятиме не лише захисту під час війни, а й закладе основу для модернізації інфраструктури у процесі відбудови. Передача передових оборонних рішень, таких як безпілотна авіація та розумні децентралізовані енергомережі, дозволить створити стійку інфраструктуру, здатну швидко відновлюватися після пошкоджень.

Для відновлення критичної інфраструктури будуть використані сучасні гнучкі технології, які забезпечать безпековий контур, сталий розвиток та безперебійне функціонування. Окреслені в таблиці 1 технології будуть ключовими у відбудові та оснащенні критичної інфраструктури у післявоєнний період. Система SAAB Giraffe 4A (Швеція) для моніторингу повітряних і наземних загроз підвищить захист об'єктів від можливих атак, а протиракетні комплекси забезпечать безпеку енергетичної інфраструктури. «Розумні» мережі та системи зберігання енергії сприятимуть стабільності енергопостачання навіть за умов повторних загроз. Вкладення в моніторингові системи та технології відновлення інтегрують Україну в європейську і глобальну системи безпеки [10, с. 27].

Трансфер таких технологій можливий через міжнародні організації, зокрема НАТО, Європейський Союз, ОБСЄ, а також шляхом двосторонніх угод. Програми військово-технічного співробітництва НАТО дозволяють передавати оборонні технології, включно з кіберсистемами та антидроновими рішеннями. ЄС підтримує відновлення інфраструктури через фінансування проєктів з інтеграцією передових технологій в енергетичну та оборонну системи України.

Взаємодія у трансфері технологій для зміцнення національної безпеки є універсальною та підходить для більшості країн і регіонів, що прагнуть зміцнити обороноздатність. Вона охоплює три ключові напрями: оборонні технології, кібербезпека, а також енергетична безпека. Кожен із напрямів включає критичні піднапрями, необхідні для ефективної передачі технологій. На рівні оборонних технологій першорядне значення мають спільні оборонні програми, розвиток безпілотних систем і створення новітніх засобів патрулювання. Саме вони забезпечують контроль над територією та охоплення зон можливих загроз. Військові союзи НАТО та ОБСЄ, сприяють обміну досвідом і технологіями в оборонній сфері, а також інтеграції сучасного озброєння, адаптованого до потреб конкретних держав.

Кібербезпека – вимагає глобальної взаємодії, оскільки кіберзагрози не обмежені територіально. Тут критичні піднапрями включають міжнародні програми з кіберзахисту, спільні освітні програми для підготовки фахівців та створення систем моніторингу і раннього попередження кіберзагроз. Організація Глобального форуму з кібербезпеки (GFCE)

забезпечує країни-учасники інструментами для обміну досвідом, підвищення кваліфікації та доступу до інноваційних технологій кіберзахисту. Спільні навчальні платформи допомагають адаптувати новітні технології захисту до специфіки локальних загроз і швидко реагувати на нові виклики [11, с. 82].

Енергетична безпека як третій напрям включає піднапрями розвитку відновлюваних джерел енергії, впровадження технологій зберігання енергії та розвиток «розумних» енергомереж. Розвинені країни, об'єднані в Міжнародне енергетичне агентство (МЕА), активно обмінюються досвідом у впровадженні інноваційних енергетичних систем, що підвищують стійкість до атак і мінімізують залежність від імпорту. Програми МЕА сприяють розвитку екологічно чистої енергетики, що забезпечує автономність регіонів навіть у випадку кризи. Впровадження «розумних» мереж підвищує стабільність енергопостачання, що критично важливо для національної безпеки.

Дані напрями передбачають багатосторонню співпрацю між урядами та організаціями, включно з Європейським Союзом, який забезпечує обмін критичними технологіями у сфері кібербезпеки та енергетичної стабільності. Завдяки міжнародним програмам обміну технологіями країни отримують не тільки доступ до новітніх розробок, але й підтримку у впровадженні та адаптації цих рішень [3, с. 75]. Інтеграція оборонних технологій і систем моніторингу сприяє створенню глобальної платформи для спільної безпеки, де країни об'єднують зусилля у відповідь на глобальні загрози.

Україна є прикладом, де трансфер технологій набув особливого значення через масштабний конфлікт, що веде до технологічного суперництва серед держав. У цьому контексті трансфер технологій для України включає як сучасні оборонні системи, такі як антидронові та протиракетні комплекси, так і цифрові платформи для захисту від кіберзагроз. США, ЄС та НАТО підтримують Україну шляхом передачі високотехнологічних систем і забезпечення спеціалізованого навчання. Держави-партнери допомагають модернізувати військову інфраструктуру та створюють умови для адаптації нових технологій до умов бойових дій. Взаємодія міжнародного товариства у трансфері технологій зображена на рисунку 1.

Можливості міжнародного співробітництва в галузі трансферу технологій до 2025–2030 років набуватимуть ще більшої ваги, особливо в контексті безпеки, кіберзахисту та енергетичної незалежності. Прогрес у розвитку штучного інтелекту (AI), квантових обчислень, наноматеріалів та нових компо-

Рис. 1. Взаємодія міжнародного товариства у трансфері технологій для зміцнення національної безпеки

Джерело: розроблено авторами

зитів, розумної робототехніки, інноваційних видів зв'язку, включаючи лазер, новітні оборонні інтегровані системи стимулює країни об'єднувати зусилля для розробки та обміну критичними технологіями. НАТО планує поглибити співпрацю в напрямку розвитку технологій штучного інтелекту, як це закріплено в програмі DIANA (Defence Innovation Accelerator for the North Atlantic), запущеній у 2021 році [1, с. 18]. DIANA передбачає розробку та впровадження рішень з використанням ШІ для ситуаційної обізнаності та розвідки, що дозволяє інтегрувати цифрові інструменти для управління військовими операціями. Зазначена програма є важливою, оскільки надає країнам-учасникам доступ до технологічних інновацій, які сприятимуть посиленню обороноздатності завдяки спільному використанню аналітичних інструментів і даних.

Значущим напрямом співробітництва є розвиток кібербезпеки, де критично важливою стала Програма кіберзахисту Європейського Союзу, прийнята у 2020 році. Програма зосереджується на захисті критичної інфраструктури держав-членів і передбачає створення єдиної системи моніторингу кіберзагроз. Мета – зменшення кіберзагроз, включно з потенційним зниженням ризиків атак на енергетичні та фінансові системи. За даними Європейської комісії, до 2025 року очікується повна інтеграція цієї системи в державні служби та критичні галузі [12, с. 34]. Зусилля щодо посилення кіберзахисту сприяли створенню Європейського центру з кібербезпеки у Бухаресті, який забезпечує навчання та підтримку для державних і приватних структур. Співробітництво між країнами, зокрема з європейськими партнерами, дозволить використовувати передові системи кіберзахисту для зниження ризиків кіберзагроз і підвищення стабільності інфраструктури.

На порядку денному також стоїть питання енергетичної безпеки, де країни ЄС спільно з НАТО впроваджують новітні технології для забезпечення стійкості енергомереж і переходу на відновлювані джерела енергії. Угода про «Зелений пакт для Європи», укладена у 2019 році, передбачає співпрацю країн у розробці технологій для зниження залежності від традиційних джерел енергії [10, с. 55]. За планом до 2030 року очікується досягнення 55% скорочення викидів вуглецю, що стало можливим завдяки розвитку технологій вітрової та сонячної енергетики [14]. В рамках пакту розробляються інноваційні системи зберігання енергії, зокрема батарейні та водневі установки, що сприяють створенню незалежних і автономних енергомереж. Залучення технологій «розумних» мереж, які автоматично регулюють потоки енергії, дозволить країнам не лише скоротити витрати на енергетику, а й підвищити енергетичну незалежність. Створення децентралізованих систем генерації та розподілу енергії з оптимальною собівартістю та сталістю існування є одним з ключових викликів безпекового питання в енергетичній системі як окремої країни, регіону, так і міжнародного енергетичного співробітництва.

Особливої уваги заслуговує розвиток оборонних технологій, де інтеграція нових систем протиповітряної оборони стала пріоритетом у безпековій політиці країн-членів НАТО та партнерів. Наприклад, до 2025 року Альянс планує запровадити систему «Балістичний щит», яка здатна забезпечити протиракетну оборону на надзвичайно високому рівні. Згадана система включає сучасні радари та системи протиповітряної оборони, розроблені за спільної участі США, Ізраїлю та країн ЄС [17, с. 76]. Важливим кроком у цьому напрямі стало укладення угоди між США та Європою про модернізацію ППО на основі передових технологій стелс та антидронових систем. Технології дозволять забезпечити захист від загроз як на національному, так і на міжнародному рівні, зміцнивши оборонну інфраструктуру завдяки обміну інноваційними рішеннями.

Отже, до 2025–2030 років ключові напрями міжнародного трансферу технологій охоплюватимуть ШІ, кібербезпеку, енергетичну та оборонну безпеку. Нові угоди DIANA та «Зелений пакт для Європи» ілюструють зростаючу важливість обміну передовими рішеннями для спільного забезпечення національної та міжнародної безпеки. Синергія між країнами сприятиме зниженню ризиків у сферах безпеки та створенню стабільних інноваційних мереж, де держави взаємодіють для розробки та впровадження технологій. Завдяки цьому з'являться нові можливості для підвищення обороноздатності країн, а спільні зусилля гарантуватимуть швидке реагування на сучасні та майбутні виклики.

Висновки. Міжнародний трансфер технологій у галузі національної безпеки до 2025–2030 років набуде ще більшого значення, оскільки країни об'єднують зусилля для протидії сучасним загрозам, зокрема у сфері кібербезпеки, енергетичної незалежності та оборони. Використання штучного інтелекту для моніторингу та управління військовими

операціями, як це передбачено програмою DIANA, є кроком до інтеграції інновацій у захист критичної інфраструктури. Важливі програми та угоди демонструють прагнення країн спільно знижувати залежність від традиційних ресурсів і посилювати кіберстійкість. Впровадження нових технологій зберігання енергії, автономних систем управління енергомережами та передових засобів для захисту від кіберзагроз створює стійку інфраструктуру, здатну ефективно реагувати на внутрішні й зовнішні виклики.

Отже, на період до 2030 року технологічний обмін стає не тільки засобом підвищення обороноздатності, а й стратегічною основою для формування міжнародної безпекової мережі. Програми співробітництва дозволяють швидко впроваджувати новітні технології та інтегрувати їх між собою, що забезпечує ефективний захист від сучасних загроз. Спільна розробка технологій у партнерстві з НАТО, ЄС та іншими організаціями гарантує доступ до передових інноваційних рішень, знижуючи ризик непередбачених ситуацій і формуючи надійну систему взаємної підтримки. Так, міжнародний трансфер технологій закладає основу для довгострокової стабільності та посилює здатність країн своєчасно реагувати на будь-які нові загрози в галузі безпеки та оборони.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Абд Аль Гаффар, Х. т. А. Н. (2024). Використання державних хмарних технологій та національна безпека. *Review of Economics and Political Science, 9*(2), 116–133. https://doi.org/10.1108/REPS-09-2019-0125

2. Ампонсах, А. А., Адекоя, А. Ф., & Вейори, Б. А. (2022). Підвищення фінансової безпеки національного медичного страхування за допомогою хмарних блокчейн-технологій. *International Journal of Information Management Data Insights, 2*(1). https://doi.org/10.1016/j.jjimei.2022.100081

3. Баліцький, В. (2024). Гносеологія формування понять «Безпека», «Державна безпека» та «Національна безпека». *Litopys Volyni, (29)*, 183–188. https://doi.org/10.32782/2305-9389/2023.29.29

4. Граттон, П. (2022). Лідерство, технології та національна безпека. *The Journal of Intelligence, Conflict, and Warfare, 4*(3), 147–151. https://doi.org/10.21810/jicw.v4i3.4164

5. Хаммонд-Еррей, М. (2024). Великі дані, новітні технології та розвідка: порушення національної безпеки. *Taylor and Francis.* https://doi.org/10.4324/9781003389651

6. Клочко, О., & Семенець-Орлова, І. (2022). Національна безпека: український вимір. *Наукові Праці Міжрегіональної Академії Управління Персоналом. Політичні Науки та Публічне Управління, (2(62))*, 66–75. https://doi.org/10.32689/2523-4625-2022-2(62)-10

7. Кобко, Є. (2022). До проблеми визначення поняття «національна безпека». *Вісник Пенітенціарної Асоціації України, (1)*, 62–70. https://doi.org/10.34015/2523-4552.2022.1.07

8. Коп, М., & Бронгерсма, М. (2022). Інтеграція індивідуальних режимів ІВ для квантових технологій у політику національної безпеки. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.4095763

9. Лімба, Т., Станкевічус, А., & Андрулевічус, А. (2019). Промисловість 4.0 та національна безпека: феномен підривних технологій. *Entrepreneurship and Sustainability Issues, 6*(3), 1528–1535. https://doi.org/10.9770/jesi.2019.6.3(33)

10. Минцевич, В. (2020). Технологія блокчейн і національна безпека – можливість впровадження блокчейну у сфері національної безпеки. *De Securitate et Defensione. O Bezpieczeństwie i Obronności, 7*(2). https://doi.org/10.34739/dsd.2020.02.08

11. Окоріе, Ч. (2022, 1 серпня). Технології та національна безпека: яке відношення має інтелектуальна власність? *Journal of Intellectual Property Law and Practice.* Oxford University Press. https://doi.org/10.1093/jiplp/jpac065

12. Патрашку, П. (2021). Новітні технології та національна безпека: Вплив IoT на захист критичної інфраструктури. *Land Forces Academy Review, 26*(4), 423–429. https://doi.org/10.2478/raft-2021-0055

13. Пратіві, А. Ч., & Таріган, Г. (2023). Вплив передових технологій на стабільність національної безпеки Індонезії. *Jurnal Pertahanan: Media Informasi Ttg Kajian & Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism & Integrity, 9*(3), 571–579. https://doi.org/10.33172/jp.v9i3.16858

14. Шеху, І. (2022). Правовий аспект технології GPS як засіб захисту національної безпеки. *Scholars International Journal of Law, Crime and Justice, 5*(4), 178–181. https://doi.org/10.36348/sijlcj.2022.v05i04.004

15. Сміт, Ф. Л. (2020). Гіперболізація квантових технологій та національна безпека. *Security Dialogue, 51*(5), 499–516. https://doi.org/10.1177/0967010620904922

16. Яровий, Т., Коваль, Ю., Кириченко, А., Гаврилечко, Ю., Москалец, І., & Сокіл, М. (2024). Використання цифрових технологій у розвитку державної політики з питань національної безпеки. *Multidisciplinary Science Journal.* Malque Publishing. https://doi.org/10.31893/multiscience.2024ss0227

17. Єганегі, К., Арбабі, З., & Гуссейн, А. І. (2020). Роль інформаційних технологій у національній безпеці. *Journal of Physics: Conference Series, 1530*, 012112. https://doi.org/10.1088/1742-6596/1530/1/012112

18. Халіл, М. К. М. (2021, 1 грудня). Технології платформ вакцин та національна безпека. *Journal of the Egyptian Public Health Association.* Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1186/s42506-021-00070-5

REFERENCES:

1. Abd Al Ghaffar, H. t. A. N. (2024). Government Cloud Computing and National Security. *Review of Economics and Political Science, 9*(2), 116–133. https://doi.org/10.1108/REPS-09-2019-0125

2. Amponsah, A. A., Adekoya, A. F., & Weyori, B. A. (2022). Improving the Financial Security of National Health Insurance using Cloud-Based Blockchain Technology Application. *International Journal of Information Management Data Insights, 2*(1). https://doi.org/10.1016/j.jjimei.2022.100081

3. Balitsky, V. (2024). The Epistemology of the Formation of the Concepts "Security," "State Security," and "National Security." *Litopys Volyni, (29)*, 183–188. https://doi.org/10.32782/2305-9389/2023.29.29

4. Gratton, P. (2022). Leadership, Technology, and National Security. *The Journal of Intelligence, Conflict, and Warfare, 4*(3), 147–151. https://doi.org/10.21810/jicw.v4i3.4164

5. Hammond-Errey, M. (2024). Big Data, Emerging Technologies and Intelligence: National Security Disrupted. *Taylor and Francis.* https://doi.org/10.4324/9781003389651

6. Klochko, O., & Sements-Orlova, I. (2022). National Security: The Ukrainian Dimension. *Scientific Papers of the Interregional Academy of Personnel Management. Political Sciences and Public Administration, (2(62))*, 66–75. https://doi.org/10.32689/2523-4625-2022-2(62)-10

7. Kobko, Ye. (2022). On the Problem of Defining the Concept of “National Security.” *Bulletin of the Penitentiary Association of Ukraine, (1)*, 62–70. https://doi.org/10.34015/2523-4552.2022.1.07

8. Kop, M., & Brongersma, M. (2022). Integrating Bespoke IP Regimes for Quantum Technology into National Security Policy. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.4095763

9. Limba, T., Stankevičius, A., & Andrulevičius, A. (2019). Industry 4.0 and National Security: The Phenomenon of Disruptive Technology. *Entrepreneurship and Sustainability Issues, 6*(3), 1528–1535. https://doi.org/10.9770/jesi.2019.6.3(33)

10. Mincewicz, W. (2020). Blockchain Technology and National Security – The Ability to Implement Blockchain in the Area of National Security. *De Securitate et Defensione. O Bezpieczeństwie i Obronności, 7*(2). https://doi.org/10.34739/dsd.2020.02.08

11.Okorie, C. (2022, August 1). Technology and National Security: What's IP Got to Do with It? *Journal of Intellectual Property Law and Practice.* Oxford University Press. https://doi.org/10.1093/jiplp/jpac065

12. Patrascu, P. (2021). Emerging Technologies and National Security: The Impact of IoT in Critical Infrastructure Protection and Defence Sector. *Land Forces Academy Review, 26*(4), 423–429. https://doi.org/10.2478/raft-2021-0055

13. Pratiwi, A. C., & Tarigan, H. (2023). The Impact of Advanced Technology on Indonesia’s National Security Stability. *Jurnal Pertahanan: Media Informasi Ttg Kajian & Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism & Integrity, 9*(3), 571–579. https://doi.org/10.33172/jp.v9i3.16858

14. Shehu, I. (2022). The Legal Aspect of GPS Technology as Means of Safeguarding National Security. *Scholars International Journal of Law, Crime and Justice, 5*(4), 178–181. https://doi.org/10.36348/sijlcj.2022.v05i04.004

15. Smith, F. L. (2020). Quantum Technology Hype and National Security. *Security Dialogue, 51*(5), 499–516. https://doi.org/10.1177/0967010620904922

16. Yarovoy, T., Koval, Y., Kyrychenko, A., Havrilechko, Y., Moskaliets, I., & Sokol, M. (2024). Utilization of Digital Technologies in the Development of State Policy on National Security Issues. *Multidisciplinary Science Journal.* Malque Publishing. https://doi.org/10.31893/multiscience.2024ss0227

17. Yeganegi, K., Arbabi, Z., & Hussein, A. I. (2020). The Role of Information Technology in National Security. *Journal of Physics: Conference Series, 1530*, 012112. https://doi.org/10.1088/1742-6596/1530/1/012112

18. Khalil, M. K. M. (2021, December 1). Vaccine Platform Technologies and National Security. *Journal of the Egyptian Public Health Association.* Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1186/s42506-021-00070-5