http://doi.org/10.35668/2520-6524-2022-1-10
УДК 330.47:004

Г. О. АНДРОЩУК, канд. екон. наук, доц.

ТЕХНОЛОГІЧНА БЕЗПЕКА: ПРОГНОЗНІ ОЦІНКИ ТРЕНДІВ У РОЗВИТКУ НАУКИ І ТЕХНОЛОГІЙ

Резюме. *У статті досліджено зміст "технологічної безпеки" на різних ієрархічних рівнях (держави, регіону, підприємства), її місце в системі економічної безпеки та фактори впливу на її рівень. Подано прогнозні оцінки світових трендів у розвитку науки та техніки. Показано глобальні технологічні та наукові тренди у сфері озброєння та військової техніки на основі аналізу публікацій НАТО, урядів зарубіжних країн, SIPRI, Мюнхенської конференції з безпеки, ЄС, міжнародних аналітичних і консалтингових організацій. Проаналізовано стан економічної безпеки в Україні, основні виклики та загрози у сфері інвестиційно-інноваційної безпеки. Підсумовано, що конкуренція найбільших технологічних лідерів світу лише посилилася. Політично мотивована війна технологій лише починається. Інтереси національної безпеки будуть дедалі більшою мірою впливати на конкуренцію технологічних платформ у різних сферах. Інтелектуальна безпека є системоутворювальним елементом, первинною в порівнянні з інноваційною та/або технологічною безпекою, оскільки безпосередньо впливає на стан не лише науково-технологічної, а й інших складових економічної безпеки. Реалізація Стратегії економічної безпеки України дасть змогу запровадити систему моніторингу економічної стійкості й оцінку стану економічної безпеки, сприятиме підвищенню ефективності реалізації державної політики у сфері забезпечення економічної безпеки та політичної відповідальності за її результати.*

Ключові слова: *технологічна безпека, економічна безпека, глобальні технологічні тренди, міжнародне науково-технологічне співробітництво, стратегія економічної безпеки.*

ВСТУП

Сучасний стан економіки характеризується надзвичайно швидкими змінами як на мікро-, так і на мезо- і макрорівнях, тому виникає необхідність оперативного виявлення негативних явищ і потенційних можливостей для забезпечення стабільного функціонування та розвитку економічної системи загалом. Протистояти загрозам різного характеру може лише чітко налагоджена система економічної безпеки.Технологічна безпека на рівні держави є важливим чинником забезпечення як економічної, так і національної безпеки.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Дослідженню проблемних питань національної безпеки, забезпечення економічної безпеки на рівні держави, регіону та підприємства присвячені наукові праці вітчизняних вчених: Г. Андрощука, Ю. Бажала, О. Бутнік-Сіверського, В. Васенка, З. Варналія, О. Власюка, В. Гейця, Б. Губського,Є. Діденка, М. Єрмошенка, Г. Жаворонкової, Я. Жаліла, Т. Качали, Т. Кваші, Ю. Когута, А. Козаченка, В. Лойко, Б. Маліцького, І. Мігус, В. Мунтіяна, О.Ревак, І. Руденка, В. Рокочі, Й. Петровича, Т.Писаренко, О. Степанова, А. Сухорукова, С. Пірожкова, Л. Федулової, Л. Шемаєвої та ін. Проте щодо складу та визначення функціональних складових економічної безпеки на різних ієрархічних рівнях автори не дотримуються єдиного підходу. Саме тому це питання залишається дискусійним. Чинники, які мають як позитивний, так і негативний вплив і суттєво впливають на рівень економічної, зокрема технологічної та інтелектуальної безпеки, також потребують дослідження.

Мета статті. Визначення змісту "технологічної безпеки" на різних ієрархічних рівнях (держави, регіону, підприємства), її місця в системі економічної безпеки та чинників впливу на її рівень, прогнозних оцінок світових трендів у розвитку науки і техніки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

У Методиці розрахунку рівня економічної безпеки України [1] для "науково-технологічної" складової економічної безпеки держави значення вагового коефіцієнту становить 0,1183. Це друге значення після "енергетичної" складової економічної безпеки. Такий високий ваговий коефіцієнт "науково-технологічної" складової підкреслює важливість цього елементу для розрахунку інтегрального показника економічної безпеки на рівні держави.Технологічна безпека на всіх ієрархічних рівнях (держави, регіону, підприємства) забезпечується за рахунок впровадження новітніх технологій та інновацій на основі досягнень науково-технічного прогресу,

збереження рівня науково-технічного потенціалу та раціонального використання інтелектуальних і технологічних ресурсів, що сприяє забезпеченню технологічної незалежності.

У Вікіпедії подано таке визначення терміна "технологічна безпека": "технологічна безпека — це такий стан науково-технологічного та виробничого потенціалу держави, який дає змогу забезпечити належне функціонування національної економіки, достатнє для досягнення та підтримки конкурентоздатності вітчизняної продукції, а також гарантування державної незалежності *за рахунок власних інтелектуальних і технологічних ресурсів*". Це формулювання збігається з визначенням "науково-технологічної складової економічної безпеки держави", яке наведено в Методиці розрахунку рівня економічної безпеки України [1].Технологічна безпека — це забезпечення стійкості потенційно небезпечних технологій за ускладнень, які виникають у зв'язку з несприятливими тенденціями або конкретними подіями в державі [2].

Технологічна безпека — стан розвитку науково-дослідних і дослідно-конструкторських робіт (НДДКР) і провідних галузей, які виробляють сучасну техніку, що забезпечує для країни можливість самостійного вирішення найбільш важливих для національної (зокрема економічної) безпеки завдань навіть в екстремальних умовах (наприклад, в умовах війни). Нині, коли фронт наукових досліджень значно розширився і величезних величин досягла номенклатура продукції, що випускається, у межах окремо взятої країни неможливо вести наукові дослідження в усіх напрямках науки та виробляти всі види продукції. Однак країна повинна на базі власного науково-виробничого потенціалу виробляти або мати можливість швидко освоїти випуск найсучаснішої військової техніки, що забезпечує обороноздатність країни, а також, з огляду на ключові напрями, виробляти продукцію на світовому науково-технічному рівні або вище його і постійно оновлювати цю продукцію, зберігаючи її конкурентоспроможність. Досвід повоєнної Японії показує, що не маючи власної наукової бази, а лише запозичуючи зарубіжну технологію, можна вийти на провідні позиції на світовому ринку в найсучасніших галузях. Свої досягнення у сфері науки і техніки, що мають оборонне значення, країна повинна захищати режимом секретності, а ті, що мають комерційну цінність — шляхом патентування як у своїй країні, так і за кордоном. Технологічна безпека, на нашу думку, охоплює систему заходів, що спрямовані на збереження такого рівня розвитку вітчизняного науково-технічного та виробничого потенціалу, який гарантує виживання національної економіки за рахунок власних інтелектуальних і технологічних ресурсів, оборонну достатність і економічну незалежність країни в разі негативної зміни політичних і економічних умов. Прямими ознаками порушення технологічної безпеки країни є зниження національного науково-технічного потенціалу та формування односторонньої технологічної залежності від більш розвинених західних держав. Наразі в Україні, мають місце обидва ці чинники і, як наслідок, вона втрачає колишню технологічну самостійність. Головними причинами зниження науково-технічного потенціалу є різке скорочення фінансування науки, закупівель приладів і обладнання для наукових лабораторій, експериментальних досліджень, а також низька заробітна плата науковців, у результаті чого більша частина вчених та інженерів перейшла зі сфери науки в різні комерційні структури або виїхала за кордон.

У своєму дослідженні доктор економічних наук Б. А. Маліцький зазначає: "Наука, технології та інновації ще більш відсуваються на узбіччя національних пріоритетів. Тим самим ще більше посилюється ця давно сформована ключова загроза національній безпеці. На жаль, новий інститут влади схильний керуватися тими ж хибними моделями і теоріями, застосування яких ввергло Україну в економічну трясовину і спричинило величезні ризики. У держави немає ресурсів для протистояння їм, окрім нових знань, технологій та інновацій" [3, С. 22]. Аналізуючи загрози, зумовлені станом науки і технологій, Б. А. Маліцький, зокрема, підкреслює посилення загроз національній безпеці технологоекономічного характеру. Найбільш істотними з них нині є: відірваність фінансового капіталу від високотехнологічного виробництва; збереження слабкої затребуваності новітніх результатів науки і технологій вітчизняною економікою; відсутність реформ, спрямованих на впровадження інноваційної моделі розвитку економіки; загострення проблем у сировинних і видобувних галузях унаслідок вичерпності природних ресурсів, зростання цін на ресурси; неефективна з точки зору інтересів суспільства структура експорту та імпорту; однобока орієнтація влади та бізнесу на залучення в країну фінансових кредитів і інвестицій з-за кордону, ігнорування можливостей масштабного використання в інтересах розвитку економіки накопичень громадян країни; переважна ірраціональна з погляду суспільних інтересів орієнтація вітчизняного бізнесу на зарубіжні технології та техніку; слабкий рівень наукового забезпечення в легкій, харчовій промисловості і в побутовому машинобудуванні; надмірна з точки зору соціальних

інтересів комерціалізація охорони здоров'я та освітньої сфери; загострення проблем з формуванням високопродуктивної робочої сили і погіршення умов для її ефективного використання в інтересах України [3, С. 39–40].

У сучасних умовах високі технології набувають дедалі більшого значення для розвитку національної економіки України. Вважається, що захист інтересів особистості, суспільства і держави в інноваційному середовищі стане одним із головних напрямів забезпечення національної безпеки в найближчому майбутньому. Через відставання свого інноваційного сектору Україна стикається з низкою проблем у сфері забезпечення технологічної безпеки.Технологічна безпека (ТБ) — стан захищеності життєво важливих інтересів особистості, суспільства і держави від зовнішніх і внутрішніх загроз у технологічній сфері, яке сприяє забезпеченню стабільного економічного зростання держави та підвищення добробуту населення. Технологічна безпека передбачає широку низку сфер регулювання, з-поміж яких варто назвати такі: промислове виробництво, науково-технічна діяльність, транспорт, енергетика, інформація та інформатизація, ВПК, автоматизація державного управління та державних послуг тощо.

Технологізація сучасного світу досягла такого рівня, за якого зупинити наростання технологічних досягнень уже практично неможливо. Однозначно оцінити вплив процесів, пов'язаних із технологізацією суспільства, складно. Стрімке збільшення швидкості науково-технічного прогресу, нові досягнення у сфері високих технологій — мікроелектроніка, кібернетика, нанотехнології, робототехніка — дають підставу вважати, що технологічний розвиток наближається до певної точки, за якою прогнозування основних показників прогресу стає неможливим. Ця точка позначається як "точка сингулярності", зумовлена створенням штучного інтелекту (ШІ, AI (*англ.* Artificial intelligence), самовідтворюючих машин, інтеграцією людини і обчислювальної машини (кіборг), збільшенням можливостей людського мозку за рахунок біотехнологій. На думку Р. Курцвейла, людство у своєму розвитку досягає такого рівня, на якому людина ітехніка вже не мисляться окремо [4]. Прихильники теорії технологічної сингулярності вважають, що при виникненні "постлюдського" інтелекту неможливо передбачити долю цивілізації, спираючись на людське знання і поведінку. Неспроможність людини зрозуміти результати роботи ШІ в ситуації, коли на чолі цивілізації стануть не люди, а "суперінтеллект", — ця проблема, яка переміщається зі "світу фантастики" у світ реальності недалекого майбутнього.

Технологічну безпеку варто розуміти також як стійкість людства до постійно зростаючого впливу високих технологій. Ставлення до безпеки людини мають проблеми глобального і регіонального характеру, однією з яких є небезпека розв'язання світової війни із застосуванням нових видів зброї (включаючи психотропну, інформаційну). Використання електронних засобів для впливу на мозок людини, дослідження у сфері людської свідомості, електроніки, медицини дають змогу маніпулювати свідомістю людини в певних цілях. "Завдяки" новим біотехнологіям з'являються небезпечні для людини мікроорганізми, проникнення яких у навколишнє середовище загрожує поширенням невиліковних хвороб. Експерименти у сфері генної інженерії, євгеніки, технологічні маніпуляції на рівні людського ембріона можуть призвести до катастрофічних наслідків. Одним із видів технологічної безпеки є безпека технологічних процесів і виробництв (усі види застосовуваних машин, апаратів, устаткування та технологічних процесів, засоби колективного та індивідуального захисту від небезпечних і шкідливих виробничих факторів)[5].

Тренди в науці та технологіях 2020–2040 рр.: прогнозні оцінки НАТО. У сучасному світі застосування новітніх наукових розробок і проривних технологій створює конкурентні переваги у багатьох сферах. У найближчому майбутньому це буде мати визначальний вплив на забезпечення національної і колективної безпеки й оборони. Найчастіше *розробка новітніх технологій відбувається на стику декількох галузей науки, а їх застосування здійснює синергетичний ефект.* З огляду на це, дедалі більш актуальним стає пошук нових форматів міжнародного науково-технічного співробітництва. Міжнародне безпекове середовище та природа конфліктів швидко змінюються, значною мірою через розвиток науки і технологій. Новітні та проривні технології створюють як нові можливості, так і загрози не лише у сфері безпеки і оборони, а й в інших галузях. У воєнній сфері такі технології спрямовані на розширення здатності сил і засобів діяти в оперативній обстановці, що швидко змінюється: у космосі, кіберпросторі, районах міської забудови.

Водночас *постає питання щодо забезпечення належного контролю за їх поширенням і використанням, а також урахування правових, політичних, економічних та організаційних обмежень на самому початку їх розробки*. НАТО приділяє значну увагу розробці та застосуванню передових технологій у сфері безпеки й оборони, прагне зберегти переваги в цій сфері за допомогою генерування, обміну та застосування

передових наукових знань, технологічних розробок та інновацій із залученням можливостей країн-партнерів.

Україні, яка має розвинений науковий потенціал і тісно співпрацює з НАТО, варто долучитися до цієї роботи використовуючи наявні механізми співпраці для отримання доступу до новітніх і проривних військових технологій. Зокрема, це можна робити, поглиблюючи співпрацю у рамках проєктів програми НАТО "Наука заради миру і безпеки", у якій з 1991 р. Україна бере участь, та під егідою Наради національних керівників у галузі озброєнь й Організації НАТО з питань науки і технологій. Водночас доцільно шукати нові формати співробітництва у сфері фундаментальної та прикладної науки, які нині активно формуються як у рамках НАТО, так і в інших форматах багатосторонніх відносин [6].

Які зміни можуть статися у військових технологіях у найближчі 20 років? Це питання є досить важливим. Відповідь на нього має вирішальне значення для внесення відповідних змін до озброєння держав і їх союзників, військових операцій, підготовку до військового часу і пріоритетів оборонного бюджету. Рішення з оборонних ресурсів мають базуватися на ретельному аналізі, який розглядає категорії великих військових технологічних винаходів та інновацій одну за одною і досліджує кожну з них. Імовірно, ті сфери, у яких ситуація змінюється швидше за все, можуть зажадати найбільших інвестицій, а також найбільш творчого мислення про те, як змінити тактику й оперативні плани, щоб використовувати нові можливості (і зменшити нові уразливості, які противники можуть розвинути в результаті тих самих імовірних досягнень).

З урахуванням зазначеного вище, органам сектору безпеки й оборони рекомендується враховувати глобальні технологічні тренди, можливості міжнародного науково-технологічного співробітництва в цій сфері, зокрема в рамках особливого партнерства з НАТО, під час розроблення стратегічних і програмних документів, за результатами комплексного огляду сектору безпеки і оборони.

У грудні 2019 р. на зустрічі в Лондоні главами держав і урядів країн НАТО були схвалені головні напрями новітніх і проривних технологій (emerging and disruptive technologies — EDTs1), які матимуть вплив на розвиток колективної безпеки й оборони Альянсу. Серед них: технології даних (Big data); технології штучного інтелекту (AI); технології автономності (робототехніка) (Autonomy); космічні технології (Space); гіперзвукові технології (Hypersonics); квантові технології (Quantum); біотехнології (Biotechnology).

Аналіз дослідження "Тренди в науці та технологіях 2020–2040 рр." (Science & Technology Trends 2020–2040) подає оцінку виникаючих або руйнівних наук і технологій (S&T) та їх потенційний вплив на військові операції НАТО, оборонні спроможності та простір для політичних рішень [7]. Ця оцінка спирається на колективні уявлення Організації НАТО з науки і технологій (STO), її мережі спільної роботи з понад 6000 вчених, аналітиків, дослідників, інженерів і пов'язаних із ними наукових установ. Ці погляди поєднуються з вичерпним оглядом літератури майбутнього S&T із відкритих джерел та обраними національними науково-дослідними програмами.

Понятійний апарат, прийнятий у дослідженні. Новітні технології: технології або наукові відкриття, які, як очікується, досягнуть повного розвитку в період 2020–2040 рр. і на сьогодні широко не використовуються або чий вплив на функції оборони, безпеки та підприємства Альянсу не зовсім зрозумілий. Проривні технології: технології чи наукові відкриття, які, як очікується, матимуть значний або навіть революційний вплив на функції оборони, безпеки або організації НАТО в період 2020–2040 рр.). Конвергентні технології: комбінація технологій, які поєднуються новим способом для створення проривного ефекту. Дослідження має на меті допомогти нинішнім і майбутнім військовим і цивільним, які приймають рішення, у розумінні нових та/або руйнівних технологій (EDT). Зокрема, воно зосереджується на таких питаннях: Чому EDT важливі для майбутньої діяльності Альянсу? Яким чином вони розвиватимуться з часом, а також що це означає для Альянсу з операційної, організаційної чи промислової перспективи? Зрештою, ця оцінка має на меті зосередити увагу на зусиллях Альянсу в галузі S&T досліджень та: (1) на високому рівні, забезпечує огляд загроз і можливостей, які представляють EDT; (2) на рівні персоналу, допомогти в управлінні проєктуванням майбутніх військових концепцій і можливостей; а також (3) загалом допомогти розробникам політики в підготовці сил Альянсу та промисловості в країнах НАТО до успішних місій у майбутньому середовищі безпеки.

Упродовж наступних 20 років можна очікувати, що чотири загальні характеристики визначатимуть багато ключових передових військових технологій:

- **інтелектуальні:** використовувати інтегрований штучний інтелект (AI), орієнтовані на знання аналітичні можливості та симбіотичний AI-людини, щоб забезпечити руйнівні програми в усьому технологічному спектрі;

- **пов'язані між собою:** використовувати мережу віртуальних і фізичних просторів, включаючи мережі сенсорів, організацій, осіб та автономних агентів, пов'язаних за допомогою нових методів шифрування та технології розподілених книг;
- **розподілені:** використовувати децентралізовані та всюдисущі масштабні зондування, зберігання й обчислення для досягнення нових руйнівних військових ефектів;
- **цифрові:** цифрове змішування людських, фізичних та інформаційних просторів для підтримки нових руйнівних ефектів. Технології з цими характеристиками повинні збільшити оперативну й організаційну ефективність Альянсу через: розвиток переваг знань і рішень; використання нових надійних джерел даних; підвищену ефективність мережевих можливостей у всіх операційних просторах та інструментів влади; адаптування до майбутнього середовища безпеки, наповненого дешевими, поширеними та доступними в усьому світі технологіями.

Вісім сильно взаємозалежних S&T сфер вважатимуться основними стратегічними руйнівниками впродовж наступних 20 років. Технологічний розвиток у сферах даних, AI, автономії, космосу та гіперсоніки вважається переважно руйнівним за своєю природою, оскільки розвиток у цих сферах ґрунтується на довгих історіях підтримки технологічного розвитку.

Отож, значний або революційний підрив військових спроможностей чи вже триває, або матиме значний вплив протягом наступних 5–10 років. Новий розвиток у сферах кванту, біотехнології та матеріалів оцінюються як такий, що виникає, і потребує значно більше часу (10–20 років), перш ніж їх підривний характер повністю відчується на військових спроможностях. Руйнівний вплив, швидше за все, відбуватиметься за допомогою комбінації EDT і складних взаємодій між ними. Наступні синергії та взаємозалежності, як передбачається, чинитимуть значний вплив на розвиток майбутніх військових спросожностей:

- **Дані-AI-Автономія:** синергетичне поєднання Автономії, Великих Даних та AI з використанням інтелектуальних, поширених і дешевих сенсорів поряд із автономними сутностями (фізичними чи віртуальними) дасть змогу використовувати нові технології та методи, щоб отримати потенційну перевагу над військовими стратегічними й оперативними рішеннями.
- **Дані-AI-Біотехнологія:** AI, спільно з Великими Даними, буде сприяти розробці нових препаратів, цілеспрямованих генетичних модифікацій, прямому маніпулюванню біохімічними реакціями та живими сенсорами.
- **Дані-AI-Матеріали:** AI, спільно з Великими Даними, сприятиме розробці нових матеріалів з унікальними фізичними властивостями. Це підтримає подальший розвиток використання 2D-матеріалів та найновіших конструкцій.
- **Дані-Квант:** упродовж 15–20-річного періоду квантові технології збільшать можливості збирання, обробки й експлуатації даних C4ISR завдяки значно підвищеним можливостям сенсорів, безпечного зв'язку та обчислення.
- **Космос-Квант:** космічні квантові сенсори, із застосуванням квантової комунікації для безпечної передачі секретного ключа (квантовий розподіл ключа), сприятимуть формуванню цілком іншого класу сенсорів, придатних для розміщення на супутниках. Дедалі більш комерційні, менші за розміром, низькоенергоспоживчі, більш чутливі та більш розподілені космічні сенсорні мережі, що підтримуються квантовими сенсорами, будуть важливим аспектом майбутньої військової архітектури ISR через 20 років.
- **Космос-Гіперсоніка-Матеріали:** розробка екзотичних матеріалів, найновіших конструкцій, мініатюризації, накопичення енергії, способів виготовлення та приведення в дію будуть необхідними для повного використання космічного та гіперзвукового середовища за рахунок зниження витрат, підвищення надійності, підвищення продуктивності та полегшення виробництва недорогих орієнтованих на задачі за замовленням систем.

Сили Альянсу та промисловість у країнах НАТО, що підтримується EDT, розширять здатність Альянсу діяти у таких швидко еволюціонуючих оперативних середовищах, як космос, кібер (включаючи інформаційну сферу) та міські райони.

Водночас перед НАТО постає завдання швидко розглянути та належним чином врахувати необхідність вжиття правових, політичних, економічних та організаційних обмежень у процесі розвитку цих технологій. З початку 1960-х рр. наш світ стає дедалі більш цифровим і віртуальним. Упродовж наступних 20 років очікується, що ця тенденція прискориться та буде мати принципово руйнівний вплив на операції та спроможності Альянсу. Набори даних такого масштабу, які складно обробляти логістично (визначення, яке щорічно змінюється) через збільшення обсягу, швидкості, різноманітності, правдивості та візуалізації, представлятимуть

суттєві технічні, організаційні та інтероперабільні виклики. Датчики розподілу, автономність, нові технології зв'язку (наприклад, 5G) посилене використання космосу, віртуальні соціально-пізнавальні простори, цифрові двійники та розробка нових й розширених аналітичних методів збільшать нашу здатність розуміти людський, фізичний та інформаційний простори навколо нас.

BDAA — це технологія, що розрахована для всіх EDTs і стане головною для їх експлуатації з метою розширених військових спроможностей. Зокрема AI вимагає якісних даних про навчання для розробки нових алгоритмів і програм. Для НАТО BDAA дасть змогу підвищити ефективність роботи, зменшити витрати, покращити логістику, моніторинг активів у реальному часі та прогнозовані оцінки планів кампанії. Водночас це буде генерувати значно більшу ситуаційну обізнаність на стратегічному, оперативному, тактичному та промисловому рівнях. Ці програми приведуть до більш глибокого та широкого застосування прогнозної аналітики для розширеної підтримки прийняття рішень на всіх рівнях. Він має потенціал створити знання та переваги рішень, що стане важливим стратегічним руйнівником у спектрі можливостей НАТО.

Існує потенціал суттєво вплинути на ефективність кінетичного та некінетичного націлювання НАТО за рахунок використання дешевих поширених датчиків (як частина Інтернет-речей (IoT)), що пов'язані з новими протоколами зв'язку (такими, як 5G), спираючись на аналіз і розповсюдження критичної інформації в режимі реального часу.

Потенційно наближені чи близько наближені супротивники шукатимуть аналогічних технічних переваг, тоді як реалізатори асиметричних загроз будуть експлуатувати дедалі більш відкриті та доступні джерела даних для цілеспрямованого впливу чи руйнування.

Промисловість інвестує значні кошти в BDAA і надалі буде лідирувати в процесі загального розвитку та застосування. Ефективність цього інвестування є основою сучасної економіки знань. Проте унікальні потреби військових сил НАТО потребуватимуть розробки методів і стандартів взаємодії, обміну, накопичення, моделювання, аналізу, класифікації, курування, комунікацій та управління даними. Нарешті, не факт, що в кінцевому підсумку більше даних і вдосконалених алгоритмів будуть виробляти кращі рішення.

Розуміння складного соціально-пізнавально-технічного контексту навколо прийняття рішень та належна роль й інтеграція BDAA в цьому контексті будуть важливими для розвитку переваг рішення НАТО. Розвиток штучного загального інтелекту (AGI, тобто узагальненої інтелектуальної поведінки на рівні людини), представляє значну (і потенційно неможливу) технічну проблему, попри понад 60 років досліджень AI. Вважається малоймовірним, що системи AI будуть відповідати цьому рівню пізнавальної здатності впродовж наступних 20 років.

Виклики щодо політики, законодавства та взаємосумісності будуть серйозними для НАТО. Забезпечення довіри до AI поради, етичність та послідовність з національними правилами взаємодії (ROE) вимагатимуть AI підходи з особливим акцентом на роз'ясненні, довірі та співпраці між людьми та AI. Це буде потрібно (особливо в контексті операцій Альянсу), щоб визначити процеси та стандарти для перевірки, підтвердження та акредитації (VV&A) таких систем AI.

Підходи до автономії можуть варіюватися від повністю автономних до напівавтономних або навіть безпілотних систем. Конкретні рівні автономності – це функція датчиків, тип місії, зв'язки зв'язку, бортова обробка та правові / політичні обмеження. Застосування дедалі більш і більш напівавтономних і цілком автономних систем в операціях різко розширять майбутні спроможності НАТО в середовищі, де кожен солдат діє як група, кожен корабель — як група для виконання завдань, а кожен літак — як ескадра. Розвиток автономних систем насамперед визначається такими операційними потребами, як висотна довговічність (HALE), підвищення рівня інтегрованого AI та факторів людини-машини (тобто, як зробити загальну "людина-машина" команду/систему ефективнішою, зберігаючи необхідний людський контроль та прийняття рішень). Зокрема правові, політичні та взаємосумісні міркування поставлять під сумнів використання автономних систем по всій кілчейн.

Однак, враховуючи операційні переваги обох НАТО та потенційних супротивників, існує мало сумнівів, що використання автономних систем значно посилиться, загрожуватиме та забезпечуватиме операційні можливості протягом наступних 20 років.

Використання космосу для C4ISR, навігації та оборони є центральним для багатьох наявних спроможностей НАТО, а зрештою, — це фундамент, на якому НАТО побудувала технологічну перевагу. Це використання космосу і даних, отриманих із космосу, лише збільшуватимуться протягом наступних 20 років, забезпечуючи дедалі більш дієздатні та повсюдні можливості C4ISR. У поєднанні з BDAA та AI, це може значно покращити ситуаційну обізнаність на всіх рівнях, підтримку, рівень операційної ефективності,

а також спрямовуватися на збільшення націленості на успіх. Однак, оскільки дедалі більше спроможностей Альянсу покладаються на ці активи, ризики з боку ASAT (антисупутникової) або роботизованих паразитарних систем стануть більш гострими. Дедалі частіше переповнені орбіти, посилене використання великих сузір'їв малих супутників і підвищення рівня космічного сміття вплине на ефективність та надійність космічних систем. Чимало країн значно збільшили свою присутність у космосі та доступ до космічного простору. Проте очікується, що комерційні розробки та збільшення використання даних, отриманих у космосі, будуть домінувати впродовж наступних 20 років.

Дедалі більш потужні маленькі супутники та великомасштабні сузір'я/скупчення будуть сприяти більшому використанню простору, продукуючи значні політичні та правові питання. Ці правові та політичні виклики охоплюють: конфлікти між комерційним, академічним і військовим застосуванням; управління глобальним (космосом) простором; потенціал для посиленої мілітаризації космосу.

Нові матеріали та методи приведення в рух останнім часом сприяли розробкам у гіперзвукових дослідженнях і значно збільшили ймовірність їх широкого операційного застосування. Китай, Росія, США, Велика Британія, Франція, Індія, Японія та Австралія — усі відкрито визнали дослідження та тестування гіперзвукових систем. Ці системи є особливо стратегічно руйнівними з огляду на скорочені часи реакцій, доступні для ITWAA (Інтегроване Тактичне Попередження/Оцінка Атаки), труднощі в розробленні контрзаходів і загроз, які вони становлять.

Для НАТО гіперзвукові спроможності забезпечать підвищення ефективності (летальність та реагування) проти пріоритетних наземних і військово-морських цілей. Завдяки високим швидкостям вони також можуть обходитися без боєголовок, цілком покладаючись на масову та кінетичну енергію, тим самим спрощуючи конструкцію зброї. Такі швидкості будуть збільшувати шанси на вдалий постріл і зменшувати ризики перехоплення.

Очікуються, що американські системи будуть розміщені до 2025 р., а з підтримкою гіперзвуковими дронами — до 2035 року. І Китай, і Росія продемонстрували вдосконалені надзвукові програми й обмежене полірування гіперзвукової зброї. Окрім того, ці переваги доступні для рівних за силою чи майже рівних за силою супротивників із гіперзвуковою зброєю. З огляду на високі витрати, що пов'язані з розвитком гіперзвукових систем, навряд чи вони будуть доступні в цей період асиметричним антагоністам. Гіперзвукова зброя висуває значні виклики стратегіям і технологіям оборонних контрзаходів. Цей виклик є особливо гострим завдяки швидкості та можливостям великої маси.

Контрзаходи із застосуванням м'яких підходів щодо враження (наприклад, заклинювання, обман тощо) можуть певною мірою бути корисними. Однак спрямована енергетична зброя (високо енергетичні лазери або пучок частинок) або космічні перехоплювачі дають найкращу загальну надію на знищення. Ці системи повинні бути вдосконаленими й операційно спроможними у відповідних політичних та юридичних обмеженнях, якщо ефективні оборонні контрзаходи мають бути розгорнуті протягом наступних 10 років.

Використання нових технологій стане серйозним викликом і порушить фундаментальні питання етики та законності. Розширене використання штучного інтелекту, великих баз даних, передових методів аналізу й автономності забезпечать більш широкий доступ до критично важливих оперативних даних і знань, але загрожує їх спотворенням. Сама інформація дедалі більшою мірою буде перетворюватися на товар та сферу війни. Прогнозується поширення використання автоматизованих і потенційно автономних систем в операціях, у яких люди не братимуть безпосередньої участі в циклі прийняття рішень, а також зростання рівня стратегічної конкуренції. Поєднання використання застарілих і новітніх систем озброєнь може завадити здатності Альянсу до взаємодії. Технологічні прогалини створюватимуть комунікаційні, доктринальні, юридичні проблеми й ускладнюватимуть взаємосумісність.

Упровадження новітніх технологій може призвести до того, що НАТО зіткнеться з нестачею спроможностей і потужностей у деяких державах-членах. Натомість технологічний прогрес у поєднанні з демографічними змінами призведе до розвитку людських ресурсів, покращення здатності керувати та діяти в усіх сферах (враховуючи стратегічний, оперативний і тактичний рівні) та на різних територіях. Темпи та результати розвитку науки і технологій майже неможливо спрогнозувати з високим ступенем точності. Прогнозування глобальних тенденцій у цій сфері покликане підвищити рівень готовності окремих держав та їх союзів до нових загроз і можливостей, а отже, спрямоване на підвищення їхньої стійкості.

Майкл О'Хенлон — старший науковий співробітник і директор з досліджень відділу зовнішньої політики Інституту Брукінгса, який спеціалізується на стратегії оборони США, застосуванні

військової сили і політики національної безпеки США. У своєму дослідженні [8] він зазначає, що загальна оцінка полягає в тому, що технологічні зміни, що стосуються військових інновацій, можуть бути більш швидкими і значними в наступні 20 років, ніж це було за останні 20. Цілком можливо, що швидкі темпи комп'ютерних інновацій можуть зробити наступні два десятиліття більш революційними, ніж два останніх. Обговорювана тут динаміка робототехніки та кібербезпеки може лише посилитися. Вони можуть більш повно використовуватися сучасними військовими організаціями. Швидше за все, вони будуть важливим чином поширюватися і на сферу штучного інтелекту (AI). Дослідження останніх 20 років передбачають можливість такого прискорення. Це особливо вірно в світлі того факту, що декілька країн (насамперед Китай і Росія) мають ресурси, щоб конкурувати із західними країнами у сфері військових інновацій. Деякі інші сфери технологій, можливо насамперед енергетичні системи, гіперзвукові ракети і певні типи сучасних матеріалів, можуть зіграти важливу додаткову роль у перетворенні наступних двох десятиліть у справжній період військової революції чи, принаймні, дуже швидкої та стрімкої революції.

Українські науковці Т. Писаренко і Т. Кваша у своїй праці [9] дослідили глобальні технологічні та наукові тренди у сфері озброєння та військової техніки на основі аналізу публікацій урядів зарубіжних країн, НАТО, SIPRI, Мюнхенської конференції з безпеки, ЄС, міжнародних аналітичних і консалтингових організацій. Автори зазначають, що технологія є фундаментальним чинником соціальних змін, що пропонує нові можливості виробляти, зберігати та поширювати знання. Особливо це стосується військової сфери, основні зрушення в якій часто супроводжуються новаторськими подіями в історії науки та техніки. Якщо спочатку технологія не є результатом військових досліджень і розробок, все одно вона часто знаходить військове застосування і впливає на методи ведення війни. Прогрес у військовій техніці може мати як позитивні, так і негативні наслідки: покращення можливостей запобіжних заходів щодо мобілізації та застосування сили, або більш потужні можливості заподіяння шкоди та знищення. Поточні інновації в галузі ШІ, робототехніки, автономних систем, космічних технологій, 3D-друку, біотехнології, матеріалознавства та квантових обчислень, як очікується, принесуть безпрецедентні перетворення. Згідно з висновками Всесвітнього економічного форуму, вони формують фундамент "четвертої промислової революції". Частково ці технології вже використовуються у військових сферах та у сферах безпеки, а частково потребують подальшого вивчення. ШІ стає "визначальною технологією майбутнього", як у повсякденному житті, так і у військовій сфері. Щоб розвивати військовий потенціал, який придатний для геостратегічних викликів сьогодення та майбутнього, країни мають триматися за провідні позиції в галузі інновацій, науки і техніки. Для цього також потрібна оцінка потенційного середовища безпеки в майбутньому, особливо щодо військових викликів і викликів безпеці, які виникають унаслідок нових науково-технічних питань, проривних інновацій. Моніторинг інновацій і нових технологій є важливим для розуміння майбутніх війн та глобальної безпеки [9, с. 4].

Стан економічної безпеки в Україні. Кабінет Міністрів України 10 березня 2021 р. схвалив проєкт Стратегії економічної безпеки України на період до 2025 року. Це фундаментальний документ, що є основою для формування державної політики у сфері гарантування економічної безпеки. Вперше на законодавчому рівні визначені взаємоузгоджені поняття "економічна безпека", "національні економічні інтереси", "економічна стійкість" та "економічний суверенітет", а також основні виклики та загрози для економічної безпеки України та способи їх подолання. Стратегія визначає загрози економічній безпеці України за фінансовою, виробничою, інвестиційно-інноваційною, зовнішньо-економічною, макроекономічною складовою. Прописано також виклики, що пов'язані зі збройною агресією Російської Федерації та тимчасовою окупацією частини території України. Упродовж останніх 10 років економіка України не забезпечувала досягнення національних економічних інтересів. Так, у період 2010–2019 рр. стан економічної безпеки оцінювався як незадовільний із погіршенням показників практично за всіма складовими до небезпечного рівня у 2012 та 2014–2015 роках. Середнє значення рівня економічної безпеки за цей період становило 40 % (зона рівня незадовільного стану). У 2019 р. рівень економічної безпеки України становив 43 %, а за підсумками першого півріччя 2020 р. — 41 % відповідно. Загалом рівні всіх головних складових економічної безпеки залишалися низькими, що зберігає високими ризики прояву масштабних дестабілізаційних явищ у розвитку економіки в довгостроковій перспективі. Основними викликами та загрозами у сфері інвестиційно-інноваційної безпеки залишаються: 1) відсутність привабливих умов для залучення інвестицій та реінвестування, а також недостатнє інституційне забезпечення цих процесів; 2) відсутність механізму оцінки (скринінгу) прямих

іноземних інвестицій, які залучаються в об'єкти, що мають стратегічне значення для національної безпеки України; 3) недосконалість регіональної інвестиційної політики та цілеспрямованої іміджевої інвестиційної політики, відсутність науково обґрунтованого моніторингу інвестиційного потенціалу України та її регіонів; 4) слабо розвинена інноваційна інфраструктура загалом і зокрема для ведення бізнесу та впровадження інновацій суб'єктами малого та середнього підприємництва; 5) відсутність сприятливих умов для створення та розвитку технологічних компаній та інноваційних підприємств (стартапів); 6) незадовільний стан об'єктів дослідницької інфраструктури; 7) недостатній обсяг фінансування наукової, науково-технічної та інноваційної діяльності; 8) недостатній обсяг фінансування основного капіталу для забезпечення інтенсивного розвитку економіки в довгостроковому періоді; 9) відсутність дієвих економічних стимулів, сприятливих умов для інноваційного оновлення виробництва, низький попит на внутрішньому ринку на інноваційну продукцію; 10) *низький рівень захисту інтелектуальної власності*; 11) низький захист прав власності; 12) корупція.

Дослідження проведені автором підтверджують, що втрата державою контролю над патентно-ліцензійною політикою призводить до відтоку результатів науково-технічної діяльності, є перешкодою формуванню інноваційної економіки України. У системі міжнародної передачі технології існують три традиційні канали: 1) торгівля товарами та послугами; 2) прямі іноземні інвестиції; 3) ліцензування інтелектуальної власності, включаючи ліцензування комерційної таємниці (ноу-хау). Однак останнім часом з'явилися додаткові канали міжнародної передачі технології, а саме: 4) відкриті інновації; 5) міграція; 6) глобальні інноваційні мережі, які потребують особливої уваги [10].

Неконтрольований витік з України інноваційних технічних рішень за кордон здійснює негативний вплив на технологічну й економічну безпеку держави. В обхід ст. 37 Закону України "Про охорону прав на винаходи та корисні моделі", що передбачає реєстрацію пріоритетної заявки на винахід (корисну модель) в Україні, багато винахідників подають заявки на винаходи безпосередньо в інші країни, без подачі заявки на винахід (корисну модель) в Україні. Несанкціонований виток винаходів, так звана "патентна міграція" з України, постійно зростає. Рівень патентів-втікачів становить 10–12 % від загального щорічного обсягу патентування. Найбільш активними секторами міграції є: медичні препарати, ІТтехнології (системи та обладнання), фармакологія. Водночас розширюється географія міграції: Російська Федерація (51 %), США (11 %), Південна Корея (9 %), Тайвань (3 %), Німеччина (2 %). До групи патентів-втікачів зазвичай належать найбільш конкурентоздатні винаходи, які потім повертаються в Україну як інноваційні продукти іноземних компаній [10]. Інновації є рушійною силою зростання рівня технологічної безпеки держави, регіону та підприємства. Високий рівень технологічної безпеки можна досягти лише за рахунок розробки та впровадження інновацій. Міністерству економіки України спільно з Міністерством освіти та науки України необхідно терміново запровадити організаційноекономічний механізм державної підтримки закордонного патентування винаходів, а також передбачити законодавчі санкції за порушення порядку закордонного патентування. Врешті-решт, це питання економічної та технологічної безпеки держави.

Державна політика щодо економічної безпеки повинна провадитися у двох взаємопов'язаних напрямах — у напрямі розвитку та безпековому напрямі. За кожним із них визначаються завдання і механізми їх виконання. У складі Стратегії затверджуються індикатори економічної безпеки з критичними межами та цільовими орієнтирами.

Завдання державної політики у сфері інвестиційно-інноваційної безпеки: 1) розвиток інституційної системи супроводження інвесторів, зокрема інформаційно-консультаційного забезпечення інвестування, здійснення її належного ресурсного забезпечення; 2) створення умов для малого та середнього бізнесу для інвестування в науково-дослідну діяльність шляхом реалізації заходів щодо розвитку співпраці науково-дослідного та реального секторів; 3) запровадження фінансових стимулів і механізму підтримки вітчизняних підприємств у разі впровадження ними новітніх технологій; 4) створення сприятливих умов для генерування та комерціалізації інновацій і виробництва інноваційної продукції (послуг); 5) впровадження моделі "відкритих інновацій"; 6) забезпечення інклюзивності та реалізації нової системи оцінювання суб'єктів науково-технічної та освітньої діяльності на основі визначення рівня якості нових наукових і технічних знань, науково-технічної інформації, освітніх послуг, а також кардинального підвищення суспільного статусу науки й освіти в Україні; 7) забезпечення міжнародної співпраці у сфері інноваційної та науково-технічної діяльності, сприяння участі вчених, науковців, МСП у Рамковій програмі досліджень та інновацій "Горизонт Європа" та інтеграція України до Європейського дослідницького та

інноваційного простору; 8) впровадження інструментів державної регіональної політики, що спрямовані на підвищення інвестиційної привабливості регіонів; 9) внесення змін до податкового законодавства України в частині перегляду видів податків і механізмів оподаткування, які сприятимуть реінвестуванню прибутку та мінімізації податкового навантаження в процесі запровадження у виробництві концепції циркулярної економіки та сталого розвитку.

ВИСНОВКИ

Епідемія COVID-19 дала потужний поштовх інформаційно-комунікаційним технологіям. Витрати режиму ізоляції вдалося знизити завдяки платформам віддаленої роботи. Уже наявні екосистеми фінансових трансакцій, електронного документообігу, зберігання даних тощо дали змогу пом'якшити шок від розриву звичних комунікацій. Здавалося б, пандемія повинна була консолідувати світову спільноту в питаннях розробки та впровадження нових технологій задля загального блага. Проте насправді у 2020–2021 рр. конкуренція найбільших технологічних лідерів (США і Китай) лише посилилася. Політично мотивована війна технологій лише починається. Інтереси національної безпеки будуть дедалі більшою мірою впливати на конкуренцію технологічних платформ у різних сферах. *Інтелектуальна безпека є системоутворювальним елементом. Вона є первинною у порівнянні з інноваційною та/або технологічною безпекою, оскільки безпосередньо впливає на стан не лише науково-технологічної, а й інших складових економічної безпеки.* У широкому стратегічному та геополітичному контексті характер конфлікту змінюється, важливим стає трансформуюче технологічне середовище. Ця зміна характеру конфлікту проявляється в гібридній війні — гіпервійні, меметичній війні, кібервійні, конфлікті наступного покоління. У кожному з них проривні технології поєднуються з наявними технологіями та військовими можливостями для створення нових способів і засобів вступу в конфлікт. Загальними чинниками, що пов'язують ці технології четвертої промислової революції, є те, що всі вони певним чином формують розумні, взаємопов'язані, розподілені та цифрові (I2D2) сили. Майбутній науково-технічний ландшафт буде характеризуватися (і водночас керуватися) такими особливостями:

1) ***інтелектуальність:*** інтегрований ШІ, аналітика та можливості прийняття рішень у всьому технологічному спектрі: — *автономія*: автономні системи із ШІ, здатні до певного рівня автономного прийняття рішень. Такі автономні системи можуть бути роботизованими, заснованими на платформі чи (цифровими) агентами; — *гуманістичний інтелект:* безшовна інтеграція психосоціальнотехнологічних систем, що підтримують об'єднання людей та машин та синергетична поведінка; — *аналітика знань:* передові аналітичні методи (включаючи ШІ), що вивчають великі масиви даних і сучасні математичні методи, щоб надавати уявлення, знання та поради;

2) ***взаємозв'язок:*** використання мережі (або сітки) накладання реального та віртуального доменів, враховуючи датчики, організації, установи, приватних осіб, автономні агенти та процеси: — *довірені комунікації:* використання таких технологій, як технології розподіленого реєстру (наприклад, блокчейн), розподіл квантових ключів (QKD), постквантова криптографія та кіберагенти ШІ для забезпечення надійних взаємодій та обміну інформацією; — *синергетичні системи:* розвиток змішаних (фізичних або віртуальних) складних систем, що дають змогу створювати нові екосистеми (наприклад, розумні міста);

3) ***розподіленість:*** децентралізоване та повсюдне широкомасштабне зондування, зберігання, обчислення, прийняття рішень, дослідження та розробки: — *Edge Computing:* вбудовування сховищ, обчислень та аналітики / ШІ в агенти та об'єкти, близькі до джерел інформації; — *повсюдне зондування:* вбудовування недорогих датчиків для створення великих сенсорних мереж у людських фізичних інформаційних доменах [9, с. 65–66].

Реалізація Стратегії економічної безпеки України дасть змогу запровадити прозору систему постійного моніторингу економічної стійкості та щорічну оцінку стану економічної безпеки, а також буде сприяти підвищенню ефективності реалізації державної політики у сфері забезпечення економічної безпеки та політичної відповідальності за її результати.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методика розрахунку рівня економічної безпеки України [Електронний ресурс] : наказ Міністерства економіки України від 02 берез. 2007 р. № 60. — Режим доступу: http://www.me.gov.ua/control/uk/publish/printable_article?art_id=97980.
2. Рекомендации по совершенствованию законодательства государств — участников СНГ в сфере противодействия технологическому терроризму, принятые постановлением Межпарламентской Ассамблеи государств — участников Содружества Независимых Государств от 16 апреля 2015 г. № 42-7 // Информационный бюллетень Межпарламентской Ассамблеи СНГ. — 2015. — № 63.
3. *Маліцький Б. А.* Наука, технології, інновації та національна безпека: теоретичні та прикладні аспекти / Б. А. Маліцький. — Київ : КЖТ "София", 2014. — 56 с.

4. *Kurzweil R.* The singularity is near: when humans transcend biology / R. Kurzweil. — Viking Press, 2005. — 672 p.
5. *Калмыкова О. М.* Технологическая безопасность и будущее человечества в условиях глобализации мировых процессов [Електронний ресурс] / О. М. Калмыкова, Е. Б. Ивушкина. — Режим доступу: https://elib.bsu.by/bitstream/123456789/90469/1/567-571.pdf.
6. *Войтовський К. Є.* Глобальні тренди розвитку науки і технологій: нові виклики і можливості [Електронний ресурс] / К. Є. Войтовський. — Режим доступу: https://niss.gov.ua/sites/default/files/2020-05/nauka-i-tehnologii.pdf.
7. Science & Technology Trends 2020–2040 Exploring the S&T Edge NATO Science & Technology Organization. Office of the Chief Scientist NATO Headquarters B-1110 Brussels Belgium [Electronic resource]. — Access mode: http:/www.sto.nato.int.
8. *O'Hanlon Michael E.* Forecasting Change in Military Technology 2020-2040 / Michael E. O'Hanlon. [Electronic resource]. — Access mode: https://www.japcc.org/forecasting-change-in-military-technology-2020-2040/.
9. *Писаренко Т.* Глобальні технологічні тренди у сфері озброєння та військової техніки [Електронний ресурс] / Т. Писаренко, Т. Кваша. — Київ : УкрІНТЕІ, 2020. — 88 с. http://doi.org/10.35668/978-966-479-117-2.
10. *Андрощук Г. О.* Патентна міграція в міжнародному трансфері технологій: аспекти технологічної безпеки / Г. О. Андрощук // Питання інтелектуальної власності у сфері трансферу технологій : збірн. наук. прац. IV Всеукр. наук.-практ. конф.-семін. з пробл. екон. інтел. власн. (Київ, 21 травн. 2021 р.). — Київ : Науково-дослідний інститут інтелектуальної власності НАПрН України, 2021. — С. 11–24.

REFERENCES

1. *Metodyka rozrakhunku rivnia ekonomichnoi bezpeky Ukrainy*: Nakaz Ministerstva ekonomiky Ukrainy № 60 vid 02.03.2007 [Methods of calculating the level of economic security of Ukraine. Order of the Ministry of Economy of Ukraine № 60 dated 02.03.2007] (2007). Retrieved from: http://www.me.gov.ua/control/uk/publish/printable_article?art_id=97980 [in Ukr.].
2. *Rekomendatsii po sovershenstvovaniyu zakonodatelstva gosudarstv — uchastnikov SNG v sfere protivodeystviya tekhnologicheskomu terrorizmu*, prinyatye postanovleniem Mezhparlamentskoy Assamblei gosudarstv — uchastnikov Sodruzhestva Nezavisimykh Gosudarstv ot 16 aprelya 2015 g. № 42-7 [Recommendations for improving the legislation of the CIS member states in the field of combating technological terrorism, adopted by the Resolution of the Interparliamentary Assembly of the Commonwealth of Independent States of April 16, 2015 № 42-7]. *Informatsionnyy byulleten Mezhparlamentskoy Assamblei SNG* [Information Bulletin of the Interparliamentary Assembly 63 of the CIS Assembly]. (2015). [in Russ.].
3. Malitsky, B. A. (2014). *Nauka, tekhnolohii, innovatsii ta natsionalna bezpeka: teoretychni ta prykladni aspekty [Science, technology, innovation and national security: theoretical and applied aspects]*. Kyiv, 56 p. [in Ukr.].
4. Kurzweil, R. (2005). *The singularity is near: when humans transcend biology.* Viking Press, 672 p.
5. Kalmykova, O. M., & Ivushkina, E. B. *Tekhnologicheskaya bezopasnost i budushchee chelovechestva v usloviyakh globalizatsii mirovykh protsessov [Technological security and the future of mankind in the context of globalization of world processes*]. Retrieved from: https://elib.bsu.by/bitstream/123456789/90469/1/567-571.pdf [in Russ.].
6. Voitovskii, K. E. (2020). *Hlobalni trendy rozvytku nauky i tekhnolohii: novi vyklyky i mozhlyvosti [Global trends in science and technology: new challenges and opportunities].* Retrieved from: https://niss.gov.ua/sites/default/files/2020-05/nauka-i-tehnologii.pdf [in Ukr.].
7. Science & Technology Trends 2020–2040 Exploring the S&T Edge NATO Science & Technology Organization. Office of the Chief Scientist NATO Headquarters B-1110 Brussels Belgium. Retrieved from: http//www.sto.nato.int.
8. Michael, E. O'Hanlon Forecasting Change in Military Technology, 2020-2040. Retrieved from: https://www.japcc.org/forecasting-change-in-military-technology-2020-2040.
9. Pysarenko, T. V., & Kvasha, T. K. (2020). *Hlobalni tekhnolohichni trendy u sferi ozbroiennia ta viiskovoi tekhniky [Global technological trends in the field of weapons and military equipment].* Kyiv. 88 p. https://doi.org/10.35668/978-966-479-117-2 [in Ukr.].
10. Androshchuk, H. O. (2021). Patentna mihratsiia v mizhnarodnomu transferi tekhnolohii: aspekty tekhnolohichnoi bezpeky [Patent migration in international technology transfer: aspects of technological security]. *Pytannia intelektualnoi vlasnosti u sferi transferu tekhnolohii* [Issues of intellectual property in the field of technology transfer: collection]. Science. works. IV All-Ukrainian scientific-practical conf.-semin. with probl. econ. intel. own. (May 21, 2021). Kyiv, P. 11–24. [in Ukr.].

H. O. ANDROSHCHUK, PhD in Economics, Associate Professor

TECHNOLOGICAL SAFETY: FORECAST ESTIMATES OF TRENDS IN THE DEVELOPMENT OF SCIENCE AND TECHNOLOGIES

Abstract. *The content of "technological security" at different hierarchical levels (state, region, enterprise), its place in the system of economic security and factors influencing its level are studied, forecast estimates of world trends in the development of science and technology are given. The global technological and scientific trends in the field of weapons and military equipment are shown based on the analysis of publications by NATO, foreign governments, SIPRI, the Munich Security Conference, the EU, international analytical and consulting organizations. The state of economic security in Ukraine, the main challenges and threats in the field of investment and innovation security has been analyzed. It is concluded that the competition of the world's largest technology leaders has only intensified. The politically motivated technology war is just beginning. National security interests will increasingly influence the competition of technology platforms in various fields. Intellectual security is a*

system-forming element, primary in comparison with innovative and/or technological security, since it directly affects the state of not only scientific and technological, but also other components of economic security. The implementation of the Economic Security Strategy of Ukraine will allow introducing a system for monitoring economic stability and assessing the state of economic security; will contribute to increasing the efficiency of the implementation of state policy in the field of ensuring economic security and political responsibility for its results.

Keywords: *cosmetic industry, innovations, technological advancement, cosmetic brands, beauty-industry.*

ІНФОРМАЦІЯ ПРО АВТОРА

Андрощук Геннадій Олександрович — канд. екон. наук, доцент, головний науковий співробітник, Науково-дослідний інститут інтелектуальної власності Національної академії правових наук України, вул. Казимира Малевича, 11, корп. 4, м. Київ, Україна, 03680; +38 (044) 200-08-76; genandro1@gmail.com; ORCID: 0000-0003-0781-9740

INFORMATION ABOUT THE AUTHOR

Androshchuk H. O. — PhD in Economics, Associate Professor, Chief Researcher, Scientific Research Institute of Intellectual Property of the National Academy of Legal Sciences of Ukraine; Kazymira Malevycha Str., 11, building 4, Kyiv, 03680; genandro1@gmail.com; +38 044 200-08-76, ORCID: 0000-0003-0781-9740