УДК 327:339.564:623.45

Аріна РУБАН, асп.
ORCID ID: 0009-0006-3165-4623
e-mail: 29ruban@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

АНАЛІЗ ТРЕНДІВ У ТРАНСФЕРІ ТЕХНОЛОГІЙ ПОДВІЙНОГО ПРИЗНАЧЕННЯ У ГЛОБАЛЬНІЙ ЕКОНОМІЦІ

В с т у п . ***За останні десятиліття сформувалась міжнародна система експортного контролю як військової продукції, так і технологій подвійного призначення (ТПП). Через об'єктивні причини ця система постійно змінюється, що вимагає відповідної адаптації національного законодавства й адміністративних механізмів. З огляду на це важливим науково-практичним завданням є дослідження тенденцій розвитку міжнародної системи експортного контролю, зокрема і щодо ТПП. Це необхідно для розроблення заходів щодо поглиблення міжнародного співробітництва та підвищення ефективності експортного контролю ТПП на національному рівні.***

М е т о д и . ***Було використано такі методи: аналітичний, компаративний, ретроспективний.***

Р е з у л ь т а т и . ***У статті уточнено суть й особливості здійснення експортного контролю технологій подвійного призначення.***

В и с н о в к и . ***Експортний контроль, як сукупність норм міжнародного права, договірних і політичних зобов'язань, орієнтованих на зниження ризику застосування військової сили, нерозповсюдження зброї масового знищення, засобів її доставки та протидію тероризму, є важливою складовою режиму міжнародної безпеки. Актуальність експортного контролю обумовлюється двома чинниками: можливістю експортного контролю сприяти інтересам міжнародної безпеки та можливістю досягнення власних національних інтересів державами, які його застосовують.***

К л ю ч о в і с л о в а : ***технології подвійного призначення, МАГАТЕ, ядерна зброя, кіберзброя, біологічна зброя, експортний контроль.***

Вступ

Глобалізація сприяє поширенню технологій подвійного призначення в нових регіонах і країнах. Крім того, технологічний прогрес полегшує розроблення та використання таких ризикових технологій, а їхній руйнівний потенціал постійно зростає. З огляду на це важливо, щоб правила передання подвійного використання сприймалися як сумісні з наявними нормами та правилами, залучали основних зацікавлених сторін і не суперечили основним інтересам у контролі або спільному доступі до таких технологій. Законність, інклюзивність й ефективність є трьома ключовими параметрами, за якими слід оцінювати інструменти для запобігання зловживанню технологіями подвійного призначення.

Мета статті – дослідити та проаналізувати вплив технологій подвійного призначення на глобальні економічні зміни.

Методи

Дослідження ґрунтується на принципі науковості. У статті використано такі методи, як: аналітичний – під час виявлення умов і причин, що обумовили виникнення розповсюдження технологій подвійного призначення; ретроспективний – у процесі аналізу досвіду міжнародних організацій у системах контролю; компаративний – у порівнянні позицій провідних міжнародних організацій й іноземних держав щодо систем експортного контролю технологій подвійного призначення.

Результати

Технологія є ключовим чинником політичної, військової та економічної влади. Оскільки технічна компетентність стає дедалі більш розпорошеною, розвинені держави все частіше володіють технологіями, щоб кинути виклик ліберальним нормам та інститутам. Експортний контроль ТПП забезпечується сукупністю відповідних норм міжнародного права і багатосторонніх політичних зобов'язань, який створений, щоб запобігти критичній концентрації таких технологій та їхньому використанню для створення загроз. Такі механізми спрямовані на зниження ризику військових конфліктів і тероризму, запобігання та протидію розповсюдженню зброї, засобів її доставки. Саме через це експортний контроль (озброєнь, військової техніки і ТПП) є однією з головних складових системи міжнародної безпеки.

Актуалізація проблем ефективного міжнародного експортного контролю ТПП зумовлена такими причинами, як підвищення рівня військово-політичної напруги у світі та вірогідності військових конфліктів, загострення глобального тероризму; розширення видів і способів ТПП, а також звуження можливостей експортного контролю на національному рівні.

У сучасному світі з розвитком глобалізації ефективні заходи експортного контролю можливо здійснювати лише за якісної активізації міжнародної співпраці. Головними організаціями, які розробляють засади експортного контролю у світі, є: ООН, ОБСЄ, НАТО, ЄС, МАГАТЕ та Організація із заборони хімічної зброї. На основі багатосторонньої взаємодії створено такі міжнародні режими експортного контролю (United Nations charter), як:

- Комітет Цангера – неформальна організація, створена з метою реалізації Договору про нерозповсюдження ядерної зброї. Комітет також складається з експертів, які займаються гармонізацією Договору, підтримує й оновлює список обладнання і матеріалів, які можуть бути експортовані тільки у разі надання певних гарантій ("Тригерний список"). На основі досліджень комітету розробляють норми і процедури експортного контролю такого обладнання та матеріалів, які застосовує МАГАТЕ;
- Група ядерних постачальників (ГЯП) – це об'єднання, що займається експортним контролем окремих видів матеріалів, устаткування, програмного забезпечення, які зазвичай можуть використовувати для виготовлення ядерної зброї;
- Режим контролю ракетних технологій – погоджує і координує виконання спільної експортної політики країн-учасниць, встановлює єдиний список товарів і ТПП, що контролюють, а також матеріалів, устаткування і програмного забезпечення, необхідних для розвитку, виробництва й експлуатації ракетної техніки, і саме контролює передання ракет;
- Австралійська група – неформальна організація, що також займається забезпеченням експортного конт-

ISSN 1728-3817

ролю ТПП, нею визначено окремі види матеріалів, устаткування та програмного забезпечення, що можуть бути використані у створенні хімічної та біологічної зброї (Australia Group, Introduction);

- Вассенаарські домовленості – найоб'ємніший режим експортного контролю. Він спрямований на запобігання накопиченню зброї, обладнання і ТПП, які можуть сприяти підвищенню військового потенціалу. Відповідає за розроблення механізмів обміну інформацією як способу гармонізації практики експортного контролю. Домовленості охоплюють товари військового призначення, а також ТПП, що можуть бути використані для створення звичайних видів озброєнь, військової чи спеціальної техніки (Wassenaar Arrangement, Introduction).

Варто зазначити, що, окрім цього, у контролі ТПП беруть участь МАГАТЕ, яка сприяє міжнародній співпраці у сфері контролю за ядерними технологіями (International Nuclear Information System (INIS) | IAEA) та Організація із заборони хімічної зброї, що відповідає за моніторинг хімічної індустрії, контроль за розповсюдження хімічних речовин і технологій, сприяє міжнародному співробітництву у цій сфері.

Потенціал управління цими технологіями можна розглядати як лінію, де технологія, яка найбільше піддається управлінню – ядерна – перебуває у крайньому лівому куті, а технологія з найбільш обмеженими можливостями – інформаційні технології – у крайньому правому. Біологічні ж технології розміщуються десь між ними.

Положення кожної із цих технологій у парадигмі управління тісно пов'язане з її характеристиками – її історією та потенційним використанням, характер і наявність відповідних матеріалів й обладнання, рівень зусиль, необхідних для його використання в руйнівних цілях. Ядерна технологія має особливу історію, починаючи своє існування як військова технологія, розроблена урядом для озброєння, яку згодом використовували для цивільних цілей, насамперед в енергетиці та дослідженнях. Національні уряди були і залишаються центральними в розробленні та використанні ядерних технологій, навіть у країнах, де комунальні підприємства або інші суб'єкти приватного сектора експлуатують ядерні установки (Смирнова, 2017).

Інша ситуація сформувась для біологічних й інформаційних технологій, що були насамперед цивільними технологіями, руйнівний потенціал яких був визнаний після їхнього винайдення. Біологічні матеріали й обладнання широко використовують у цивільних цілях, зокрема і в дослідженнях, медицині та сільському господарстві. Інформаційні технології також мають необмежену кількість законних застосувань. Уряди відіграли важливу роль у розробленні та використанні обох технологій. Перше застосування сучасних інформаційних технологій, комп'ютерів було для військових цілей, таких як злам кодів й обчислення для атомної бомби. Проте найважливішими зацікавленими сторонами як у сфері біологічних, так і в інформаційних технологіях є приватні організації: академічні установи, компанії та окремі особи (Ruttan, 2001).

Характер і доступність матеріалів й обладнання, а також рівень зусиль, необхідних для використання ядерної, біологічної та інформаційної технології для руйнівних цілей, також дуже різні. У випадку ядерного вибухового пристрою кількість ключових матеріалів і ключових технологій обмежена, хоча інші матеріали подвійного використання, такі, наприклад, як низькозбагачений уран і відпрацьоване паливо та технології, як-от ядерні реактори, теж можуть бути використані. Існує також відносно обмежена кількість країн, що володіють або можуть постачати необхідні технології. Крім того, незважаючи на те, що недержавні суб'єкти можуть отримати так звану брудну бомбу, розроблення ядерної зброї, яка не тільки працюватиме, але й зможе успішно доставлятися до цілі, є надзвичайно складною та дорогою справою й потребує спеціальної національної програми (Moon, 2003).

На відміну від ядерної зброї, для розроблення бойових біологічних агентів можна використовувати набагато ширший спектр матеріалів й обладнання. Більшість з них нині контролюються членами Австралійської групи, оскільки їх можна використовувати для виробництва бойових біологічних агентів. Синтетична біологія й інші досягнення в науці та техніці ще більше розширюють кількість потенційних агентів загрози, а також коло практиків, до якого входять не лише дослідники в академічних чи приватних лабораторіях, але й інженери та інші особи поза науковою спільнотою. Багато матеріалів і предметів обладнання, які використовуються цим більш широким всесвітом практиків, доступні у всьому світі, що робить створення модифікованих або нових патогенів простішим і дешевшим, ніж будь-коли раніше. Однак, незважаючи на те, що кількість і тип суб'єктів, які можуть розвинути небезпечний патоген, збільшилася, виробництво збройового бойового біологічного агента та його ефективне розповсюдження залишається як технічно, так й операційно набагато складнішим, ніж прийнято вважати.

Останнім часом замість спеціальних матеріалів чи обладнання, ключовою технологією, яку використовують у кіберзброї, є інформаційна технологія. Інформаційні технології доступні всюди, де є комп'ютери. Що робить її застосування дедалі менш прогнозованим й обмеженим (Davis, & Sanger, 2015). Спочатку невелика кількість комп'ютерів була визначальним фактором в обмеженні ворожих застосувань інформаційних технологій. Нині приблизно п'ятнадцять мільярдів пристроїв у всьому світі під'єднано до інтернету, значну частину з яких становлять комп'ютери, і їхня кількість зростає (Soderbery, 2013). За винятком висококласних цілей, кіберзброю також на порядки легше та дешевше виробляти, ніж ядерні вибухові пристрої чи біологічну зброю, оскільки кожен, хто має доступ до комп'ютера, може розробити таку зброю.

Останньою характеристикою, що вплинула на потенціал управління кожною із цих технологій, є її руйнівний вплив. Після нападів на Хіросіму та Нагасакі в 1945 р. стало зрозуміло, що ядерні технології можуть бути використані для загибелі людей, а також фізичної шкоди. Хоча жодного використання біологічної технології, з яким можна було б порівнювати, не було, потенційний вплив, особливо дуже смертоносного агента, що може поширюватися від людини до людини, також визнавали протягом багатьох років. Ці побоювання щодо наслідків масового знищення ядерної та біологічної зброї допомогли стимулювати зусилля із запобігання поширенню та використанню відповідних технологій, включно з переговорами щодо Договору про нерозповсюдження ядерної зброї, Конвенції про біологічну зброю, а також багато інших заходів управління (Корсунський, 2005).

На відміну від ядерної та біологічної зброї, кіберзброю використовували неодноразово, а в деяких випадках у великих масштабах у ворожих цілях як національними урядами, так й іншими суб'єктами. Деякі кібератаки, як-от атака на вебсайти уряду, ЗМІ Естонії та банківські послуги, призвели до тривалих відмов в обслуговуванні по всій країні, що зазнала атаки. Інші,

як-от атака на комп'ютери національної нафтової компанії Саудівської Аравії, порушили важливу комерційну діяльність. Ще інші, такі як атака Stuxnet на іранські центрифуги зі збагачення урану, знищили життєво важливе обладнання, кероване комп'ютером. Багато інших кібератак, наприклад витік даних у роздрібному продавці Target, поставила під загрозу десятки мільйонів записів клієнтів. Однак жодна із цих атак не призвела до узгоджених зусиль щодо контролю за використанням кіберзброї, можливо, частково тому, що не було втрачено жодного людського життя.

Ці характеристики ядерної, біологічної й інформаційної технології значною мірою пояснюють різний потенціал управління цими трьома технологіями. Ядерна технологія була сприятливішою для урядових зусиль, оскільки її величезний руйнівний потенціал був очевидний від самого початку, а головними учасниками були національні уряди. Навіть там, де комерційні й інші приватні організації зацікавлені в ядерній політиці, ці інтереси зазвичай розглядаються під час внутрішніх обговорень в уряді (Sandevski, 2003). Крім того, ядерні предмети подвійного призначення, які були в центрі уваги уряду, країни, які можуть постачати ці предмети, і види діяльності подвійного призначення, у яких їх використовують, є відносно обмеженими, і все це сприяло зусиллям уряду.

Для порівняння: усе, що стосується кіберзброї, суперечить урядуванню: базові технології та комп'ютери, на яких їх використовують, глибоко вкорінені в цивільному суспільстві в усьому світі, виробництво більшості кіберзброї не потребує спеціальних матеріалів чи обладнання, а коло зацікавлених сторін – це будь-хто, хто має доступ до інформаційних технологій і комп'ютера, тобто доступ практично необмежений. Крім того, на відміну від ядерної та біологічної зброї, кіберзброя може поставити під загрозу людські життя лише опосередковано, наприклад, націлюючись на критично важливу інфраструктуру, таку як ядерні та хімічні об'єкти, газопроводи, транзитні системи та водопостачання.

Біологічна технологія займає позицію між ядерною та інформаційною технологією в континуумі управління. Біологічна технологія має набагато більше цивільних застосувань, ніж ядерна технологія, але вона не є повсюдною, як у випадку з інформаційними технологіями. Спектр біологічних матеріалів й обладнання, які можуть виробляти дуже небезпечний патоген, набагато більший, ніж у ядерних технологій, але, навіть з урахуванням прогресу науки не такий поширений, як комп'ютери, які використовують для здійснення кібератак. Кількість міжнародних акторів, що зацікавлені в біологічному керуванні, продовжує розширюватися далеко за межі тих, хто займається ядерною діяльністю, але не охоплює всі рівні суспільства, як у випадку з інформаційними технологіями.

Ураховуючи ці відмінності, не дивно, що паралельне порівняння типів заходів управління, які були прийняті в цих технологічних сферах, виявляє найбільше спільного між ядерною та біологічною технологіями. Різні міжнародні та національні заходи були прийняті для того, щоб запобігти використанню ядерної та біологічної технології подвійного призначення для озброєння. Договір про нерозповсюдження ядерної зброї (ДНЯЗ) та Конвенція про біологічну зброю (КБТЗ) посідають центральне місце в цих зусиллях, утілюючи як норму проти руйнівного застосування цих технологій, так і конкретні зобов'язання, які надають їй юридичної сили. На національному рівні багато країн ухвалили законодавство, що передбачає кримінальну відповідальність за діяльність, заборонену договорами, й у випадку ДНЯЗ дає можливість МАГАТЕ проводити інспекції та моніторинг своєї цивільної ядерної діяльності.

Набагато ширший спектр міжнародних і національних зусиль спрямовано на контроль доступу до ядерних і біологічних матеріалів, обладнання й інформації подвійного використання. Деякі з них, наприклад діяльність Комітету Цангера, ГЯП й Австралійської групи з узгодження експортного контролю, зосереджені на тому, щоб заборонити іншим країнам доступ до технологій, які можуть бути використані для розроблення ядерної та біологічної зброї, і тому є важливими доповнення до ДНЯЗ і КБТЗ. Запобігання поширенню зброї та пов'язаних з нею технологій в інші країни також було початковою метою Спільної програми зменшення загрози США Нанна – Лугара, що допомогла Росії й іншим колишнім радянським республікам забезпечити безпеку ядерних, біологічних та інших матеріалів, демонтувати колишні об'єкти біологічної зброї, і перенаправити колишніх учених-зброєзнавців на мирну діяльність.

Багато інших заходів, особливо після 11 вересня, спрямовані на те, щоб позбавити терористів доступу до технологій, які можна використовувати для розроблення ядерної та біологічної зброї. Це було зроблено різними способами. Наприклад, згідно з Резолюцією 1540 Ради Безпеки ООН (РБ ООН), усі держави – члени ООН зобов'язані ухвалити національне законодавство, щоб запобігти отриманню терористами матеріалів, обладнання й інформації для ядерної, біологічної та іншої зброї. Інші заходи, такі як Ініціатива з безпеки розповсюдження (ІБПР) і База даних МАГАТЕ щодо незаконного обігу розроблені, щоб допомогти країнам відстежувати та забороняти незаконні поставки матеріалів подвійного використання. До цього долучилися навіть міжнародні галузеві групи: експортери атомних електростанцій і дві промислові асоціації синтетичної біології взяли на себе зобов'язання перевіряти замовлення клієнтів на товари подвійного призначення, які вони продають. На національному рівні антитерористичне законодавство в Сполучених Штатах та інших країнах посилило внутрішній контроль за біологічними матеріалами й установами, а також за особами, які мають до них доступ. Подібні зусилля були вжиті для забезпечення безпеки вітчизняних ядерних установок і матеріалів.

Нарешті, міжнародні та національні заходи були розроблені для сприяння безпечному поводженню та використанню ядерної та біологічної технології подвійного використання. Це охоплює керівні принципи ядерної безпеки, видані МАГАТЕ, і керівні принципи біобезпеки та біозахисту, видані Всесвітньою організацією охорони здоров'я (ВООЗ). Він також містить кодекси етики та поведінки, оприлюднені різними міжнародними та національними науковими організаціями, щоб перешкоджати деструктивному застосуванню біології. На додаток до цих необов'язкових заходів, країни – члени Європейського Союзу (ЄС) запровадили контроль безпечного поводження з генетично модифікованими організмами на основі нормативних актів і директив ЄС, а Ізраїль і Данія запровадили законодавство, що вимагає попереднього перегляду та схвалення певних категорій подвійних – використовувати біологічні дослідження, що можуть викликати занепокоєння щодо безпеки (Davis, 2002).

На відміну від ядерної та біологічної зброї, кіберзброя не була заборонена міжнародним договором і фактично щоденно використовується широким колом учасників від підлітків-хакерів до національних урядів. Деякі із цих видів використання були дуже руйнівними для комерційних й економічних інтересів, але досі не

призвели до людських жертв. Експерти з міжнародного права стверджують, що закони війни та Статут ООН застосовують до кіберпростору і, як такі, деякі види використання кіберзброї заборонені. Однак навіть такі уряди, як Сполучені Штати, що поділяють цю думку, не бажають відмовлятися від можливості використання кіберзброї (Mani, 2021). Ба більше, як показує досвід атаки комп'ютерного хробака Stuxnet на іранську ядерну програму, законність цього використання кіберзброї виглядає дуже різною залежно від того, хто є ініціатором чи метою атаки.

Тож не дивно, що було вжито лише кілька заходів управління, щоб спробувати запобігти деструктивному застосуванню інформаційних технологій. На міжнародному рівні сорок сім держав, які є учасниками Будапештської конвенції про кіберзлочинність, погодилися прийняти національне законодавство, що передбачає кримінальну відповідальність за певну поведінку в кіберпросторі, наприклад несанкціонований доступ до комп'ютера або незаконне перехоплення даних. Багато із цих країн, як учасники Вассенаарської домовленості, також контролюють експорт певних предметів подвійного призначення, які можуть бути використані в кіберзброї, наприклад обладнання, пов'язане з програмним забезпеченням для захисту від проникнення або системами мережевого спостереження. На національному рівні законодавство різних країн також забороняє певне несанкціоноване використання інформаційних технологій, зокрема і для отримання доступу до комп'ютерів або перехоплення електронних комунікацій (Mozur, 2015). У Сполучених Штатах Асоціація обчислювальних машин товариство комп'ютерних професіоналів (ACM) також випустило кодекс етики для своїх членів, що забороняє їм використовувати комп'ютерну технологію у спосіб, який завдає шкоди.

Отже, ситуція, яка склалась в управлінні технологіями подвійного використання, поставила перед міжнародним порядком нові виклики. Як було визначено в статті раніше, зусилля з управління в кожній із трьох технологічних сфер зіткнулися із серйозними складнощами. Деякі є прямим результатом технічних міркувань. Очевидно, це стосується кіберсфери, де відсутність перешкод, таких як конкретні матеріали або дії, пов'язані зі зброєю, робить зусилля з управління розробленням кіберзброї майже неможливими. Виявлення роботи з неядерними компонентами ядерної зброї також є технічно складним, оскільки така діяльність не має очевидних ознак, на відміну від роботи з ядерним матеріалом, що залишає надто помітні сліди.

Інші проблеми можуть бути пов'язані з науково-технічним прогресом. Це особливо відчувається в біологічній сфері, де синтетична біологія збільшує кількість потенційних агентів загрози, типів обладнання, що використовується для їхнього розроблення, і діапазон залучених практиків, таким чином значно ускладнюючи зусилля з контролю за передаванням або доступом до біологічних агентів і технології (Brody,1996). Економічні інтереси також зіграли важливу роль у блокуванні прийняття пропозицій щодо управління. Це можна побачити у ворожому ставленні країн-експортерів ядерних реакторів до посилення умов, за яких реактори або певні компоненти реакторів можуть бути передані іншим країнам. Це також стало очевидним у протидії біотехнологічної та фармацевтичної промисловості США інспекціям на місці під час невдалих спроб укласти протокол відповідності для зміцнення КБТЗ.

Інші проблеми відображають інтереси безпеки. Дворівнева система КБТЗ щодо тих, хто має та не має ядерної зброї, була необхідною, оскільки п'ять ядерних держав на момент укладання договору не бажали відмовитися від володіння ядерною зброєю. Рішення сьогодення щодо закупівель й операційна політика цих країн демонструють, що вони продовжують розглядати володіння ядерною зброєю як необхідне у військових цілях. Інтереси безпеки також зіграли свою роль у небажанні Сполучених Штатів чи будь-якої іншої країни офіційно обмежити або заборонити використання кіберзброї, яку можна застосовувати різними способами, часто без розкриття джерела атаки.

Нарешті, політичні міркування також мали значний вплив на зусилля з управління подвійним призначенням. Країни, що розвиваються, загалом не поділяють занепокоєння Заходу щодо ризиків, пов'язаних із біологічними дослідженнями подвійного призначення, і в деяких випадках вважають зусилля з управління не більш ніж завуальованою спробою відмови від технологій. Те ж саме стосується ядерної галузі, де країни, які не мають доступу до технологій збагачення та переробки, відмовилися від права на їхнє придбання, і навіть деякі держави, які володіють такими технологіями, не бажали обмежувати свою здатність набувати нових форм у майбутньому. Зусилля щодо управління кіберзброєю також розглядають із невеликим почуттям терміновості, оскільки, на відміну від ядерної чи біологічної зброї, кіберзброю не вважають зброєю масового знищення, розповсюдження та використання якої необхідно блокувати як на міжнародному, так і на національному рівнях.

Дискусія і висновки

Зазначені фактори допомагають пояснити природу різних заходів управління, які були прийняті в цих трьох технологічних сферах. Вони також підкреслюють, чому загальний підхід до управління є неможливим, коли йдеться про управління ризиками від технологій подвійного використання. Це не означає, що концепція технології подвійного використання не корисна і від неї слід відмовитися. Навпаки, як показано у статті, концепція надає цінний аналітичний інструмент для ідентифікації й оцінки технологій, які потенційно можуть призвести до великомасштабних втрат людей або шкоди комерційним чи економічним інтересам, навіть якщо вони продовжують використовуватися для законних цілей. Аналізуючи три приклади із цієї категорії технологій, стають очевидними багато уроків для інших сфер їхнього використання.

Отже, варто зауважити, що уряди навряд чи підтримають обмеження на використання ними технологій подвійного призначення, якщо ставки не будуть достатньо високими. Натепер найбільше значення мали можливі ризики для людського життя. Це допомагає пояснити готовність такої кількості технологічних власників погодитися відмовитися від розроблення ядерної та біологічної зброї, а також відповідну відсутність інтересу міжнародної спільноти до обмеження розроблення та використання кіберзброї. Також за відсутності справжньої та широкої згоди щодо загрози уряди навряд чи підтримають обмеження на придбання та використання технологій подвійного призначення, якщо винагорода за це також не буде достатньо високою. І це демонструє активне просування країн, які не мають доступу до ядерних і біологічних технологій, гідної компенсації за відмову від придбання ядерної та біологічної зброї. Це також демонструє досвід кіберзброї, базова інформаційна технологія якого вже широко доступна по всьому світу, у такий спосіб обмежуючи переваги не лише безпеки, але й будь-які тех-

нологічні переваги, які можуть виникнути внаслідок підтримки обмежень на технології, що використовуються для кіберзброї. Нарешті, якщо уряди й інші відповідні зацікавлені сторони не розглядатимуть управління технологіями подвійного призначення як колективну відповідальність, зусилля з управління відповідними ризиками, найімовірніше, будуть обмеженими. Це демонструє відсутність ентузіазму щодо сміливих пропозицій зі зміцнення режиму нерозповсюдження ядерної зброї, таких як пропозиція колишнього директора МАГАТЕ Мохамеда Ель-Барадея щодо інтернаціоналізації ядерного паливного циклу. Це також демонструється тим, що вчені та наукові організації надають перевагу самоврядуванню, а не незалежному нагляду, а також кодексам поведінки й іншим добровільним заходам, а не правовим вимогам для врегулювання проблем щодо певних типів біологічних досліджень подвійного використання. І це демонструє небажання національних урядів й індустрії інформаційних технологій підтримувати інші заходи, окрім експортного контролю та кодексів поведінки, для розв'язання проблеми кіберзброї.

Список використаних джерел

Смирнова, Н. В. (2017, 5 березня). Трансфер технологій як засіб формування національної моделі інноваційного розвитку. *Інвестиції: практика та досвід*, 39–41.

Bennett, David, & Leseure, Michel. (2007). University to business technology transfer – UK and USA comparisons.*Technovation*. 27(3), 145–155.

Brody, R. J. (1996). *Effective partnering: a report to congress on federal technology partnerships*. Washington DC.

Davis, Julie, Hirschfield, & Sanger, David, E. (2015, September 26). U.S. and China Agree to Rein in State-Sponsored Computer Thefts. *New York Times*.

Home – The Wassenaar Arrangement. *The Wassenaar Arrangement*. http://www.wassenaar.org

International Nuclear Information System (INIS) | IAEA. *International Atomic Energy Agency | Atoms for Peace and Development*. https://www.iaea.org/resources/databases/inis

Mani, K. A. (2021). Options for the Biden Administration to Prevent Iran from Developing a Nuclear Weapon. *Brandeis University Law Journal*, 8(1), 13. https://doi.org/10.26812/bulj.v8i1.482

Moon, D.-h. (2003). North Korea's nuclear weapons program: verification priorities and new challenges.*Office of Scientific and Technical Information* (OSTI). https://doi.org/10.2172/876296

Mozur, Paul (2015, October 19). Cybersecurity Firm Says Chinese Hackers Keep Attacking U.S. Companies. *New York Times*.

Ruttan, V. W. (2004). The role of the public sector in technology development: generalisations from general purpose technologies. *International Journal of Biotechnology*, 6(4), 301. https://doi.org/10.1504/ijbt.2004.005502

Sandevski, T. (2003). Book Review: Ian Davis, The Regulation of Arms and Dual-Use Exports. Germany, Sweden and the UK (Oxford: Oxford University Press, 2002). *Millennium: Journal of International Studies*, 32(3), 741–743. https://doi.org/10.1177/03058298030320030432

Sanger, David, E. (2015, September 26). *Path Set by U.S. and China to Limit Security Breaches May Be Impossible to Follow*. New York Times. https://www.nytimes.com/2015/09/26/world/asia/limiting-security-breaches-may-be-impossible-task-for-us-and-china.html

Soderbery, Rob. (2013, January 7). *How Many Things Are Currently Connected to the 'Internet of Things' (IoT)?* Forbes. http://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/.

The Australia Group. *The Australia Group introduction*. https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/introduction.html

References

Bennett, David, & Leseure, Michel. (2007). University to business technology transfer – UK and USA comparisons. *Technovation*. 27(3). 145–155.

Brody, R. J. (1996). *Effective partnering: a report to congress on federal technology partnerships*. Washington DC.

Davis, Julie, Hirschfield, & Sanger, David, E. (2015, September 26). U.S. and China Agree to Rein in State-Sponsored Computer Thefts. *New York Times*.

Home – The Wassenaar Arrangement. *The Wassenaar Arrangement*. http://www.wassenaar.org.

International Nuclear Information System (INIS) | IAEA. *International Atomic Energy Agency | Atoms for Peace and Development*. https://www.iaea.org/resources/databases/inis

Mani, K. A. (2021). Options for the Biden Administration to Prevent Iran from Developing a Nuclear Weapon. *Brandeis University Law Journal*, 8(1), 13. https://doi.org/10.26812/bulj.v8i1.482

Moon, D.-h. (2003). North Korea's nuclear weapons program:verification priorities and new challenges.*Office of Scientific and Technical Information* (OSTI). https://doi.org/10.2172/876296

Mozur, Paul (2015, October 19). Cybersecurity Firm Says Chinese Hackers Keep Attacking U.S. Companies. *New York Times*.

Ruttan, V. W. (2004). The role of the public sector in technology development: generalisations from general purpose technologies. *International Journal of Biotechnology*, 6(4), 301. https://doi.org/10.1504/ijbt.2004.005502

Sandevski, T. (2003). Book Review: Ian Davis, The Regulation of Arms and Dual-Use Exports. Germany, Sweden and the UK (Oxford: Oxford University Press, 2002). *Millennium: Journal of International Studies*, 32(3), 741–743. https://doi.org/10.1177/03058298030320030432

Sanger, David, E. (2015, September 26). *Path Set by U.S. and China to Limit Security Breaches May Be Impossible to Follow*. New York Times. https://www.nytimes.com/2015/09/26/world/asia/limiting-security-breaches-may-be-impossible-task-for-us-and-china.html

Smirnova, N. V. (2017, March 5). Technology transfer as a means of forming a national model of innovative development. *Investments: Practice and Experience*, 39–41 [in Ukrainian].

Soderbery, Rob. (2013, January 7). *How Many Things Are Currently Connected to the 'Internet of Things' (IoT)?* Forbes. http://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot

The Australia Group. *The Australia Group introduction*. https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/introduction.html

Отримано редакцією журналу / Received: 23.11.23
Прорецензовано / Revised: 22.12.23
Схвалено до друку / Accepted: 23.01.24

Arina RUBAN, PhD Student
ORCID ID: 0009-0006-3165-4623
e-mail: 29ruban@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ANALYSIS OF TRENDS IN THE TRANSFER OF DUAL-PURPOSE TECHNOLOGIES IN THE GLOBAL ECONOMY

B a c k g r o u n d . ***In recent decades, an international system of export control of both military products and TPP has been formed. Due to objective reasons, this system is constantly changing, which requires appropriate adaptation of national legislation and administrative mechanisms. In view of this, an important scientific and practical task is the study of trends in the development of the international export control system, in particular in relation to the TPP. This is necessary for the development of measures aimed at deepening international cooperation and increasing the effectiveness of TPP export control at the national level.***

M e t h o d s . ***The following methods were used: analytical, retrospective, comparative.***

R e s u l t s . ***The article specifies the essence and features of the implementation of export control of dual-purpose technologies.***

C o n c l u s i o n s . ***Export control, as a set of norms of international law, contractual and political obligations aimed at reducing the risk of the use of military force, non-proliferation of weapons of mass destruction, means of their delivery and countering terrorism, is an important component of the international security regime. The relevance of export control is determined by two factors: the possibility of export control to contribute to the interests of international security and the possibility of achieving their own national interests by the states that apply it.***

K e y w o r d s : ***Dual-use technologies, IAEA, nuclear weapons, cyber weapons, biological weapons, export control.***

Автор заявляє про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The author declares no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.