

Кімачук Христина Михайлівна,
аспірант навчально-наукового
інституту міжнародних відносин
Київського національного
університету імені Тараса Шевченка

**ТРАНСФОРМАЦІЯ СИСТЕМИ ЕКСПОРТНОГО КОНТРОЛЮ
ТОВАРІВ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ ТА ПОДВІЙНОГО
ВИКОРИСТАННЯ В УМОВАХ ЦИФРОВІЗАЦІЇ:
МІЖНАРОДНО-ПРАВОВІ АСПЕКТИ ТА ЗАБЕЗПЕЧЕННЯ
НАЦІОНАЛЬНОЇ БЕЗПЕКИ**

В умовах глобальних трансформацій сучасності цифровізація виступає не лише провідником прогресу, а й чинником виникнення нових безпекових викликів. Традиційні механізми державного та міжнародного експортного контролю, що історично базувалися на фізичному переміщенні товарів через митний кордон, стикаються з проблемою нематеріальних передач технологій військового призначення та подвійного використання. Швидкий розвиток дистанційних форм співпраці, штучного інтелекту (ШІ), хмарних обчислень та адитивних технологій (3D-друк) потребує переосмислення правових засад контролю за міжнародними передачами товарів військового призначення (ТВП) та подвійного використання (ПВ). У контексті збройної агресії проти України та активізації санкційних режимів питання вдосконалення національного та міжнародного правового регулювання експортного контролю ТВП та ПВ набуває особливої актуальності [1; 2].

Дослідження проведено з використанням загальнонаукових та спеціально-юридичних методів, таких як аналіз і синтез, системний підхід, порівняльно-правовий метод та метод правової інтерпретації. За допомогою зазначених методів досліджено законодавство України та інших країн у сфері експортного контролю ТВП та ПВ, виявлено прогалини у регулюванні нематеріальних передач технологій в епоху ШІ та кіберзагроз, а також запропоновано способи вдосконалення системи експортного контролю України з урахуванням міжнародних практик.

Насамперед варто розглянути ст. 333 Кримінального кодексу України (ККУ), якою передбачена відповідальність за порушення порядку здійснення міжнародних передач товарів, що підлягають державному експортному контролю [3]. Диспозиція цієї норми є

blankетною, що створює труднощі під час кваліфікації злочинів, пов'язаних із цифровими передачами знань [4].

Основна прогалина полягає у складності доведення об'єктивної сторони злочину, коли передача технології (технічних даних або технічної допомоги) відбувається через хмарні сервіси чи зашифровані месенджери, що не залишає чіткого «фізичного сліду» [1; 3]. Крім того, чинна редакція недостатньо враховує специфіку «уявного експорту» (deemed export) – розкриття технологій іноземцям всередині країни [5, с. 17–19]. Ще одним ускладненням є неможливість документування кримінального правопорушення відповідно до ст. 333 ККУ, а саме незаконну передачу технологій військового призначення або подвійного використання, якщо вона здійснюється за межами України (відрадження українських делегацій за кордон, академічна мобільність тощо).

Крім того, варто звернути увагу й на товари і технології, які не внесені до контрольних списків, але можуть бути використані в програмах створення зброї масового знищення та інших військових цілях. Відповідно до ст. 10 Закону України «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання» [6], такі товари можуть підлягати державному експортному контролю, якщо, серед іншого, експортеру стало відомо про їх нецільове кінцеве використання. Таке формулювання ст. 10 уможливорює приховування суб'єктами господарювання фактів обізнаності у вищезгаданій інформації. У цьому контексті варто звернути увагу на Спільний перелік товарів високого пріоритету (Common High Priority Items List), опублікований США, ЄС, Японією та Великою Британією [7]. До переліку входять 50 товарів, ідентифікованих шестизначними кодами Гармонізованої системи (HS-codes), які мають велику значимість для російського озброєння, такі як інтегральні схеми, модулі радіочастотних приймачів, верстати з числовим програмним керуванням тощо, але водночас не включені до контрольних списків.

Міжнародно-правове регулювання експортного контролю здійснюється в рамках чотирьох режимів нерозповсюдження: Вассенаарської домовленості щодо контролю за експортом звичайних озброєнь та товарів і технологій подвійного використання, Режиму контролю за ракетними технологіями, Групи ядерних постачальників та Австралійської групи. Варто зазначити, що учасниками вказаних режимів експортного контролю не є всі країни світу. Крім того, у рамках цих режимів не передбачені механізми притягнення до відповідальності суб'єктів міжнародного права, які порушили їх положення. Положення

та контрольні списки всіх чотирьох режимів також не актуалізовані у відповідності до умов сучасності.

Наприклад, поява хмарних лабораторій, використання ІІІ та віддалений доступ до досліджень у сфері біотехнологій та інноваційних хімічних розробок є новим викликом для Австралійської групи. Це вимагає перегляду контрольних списків в рамках режиму, обговорення застосування вимог щодо ліцензування до передачі даних та надання послуг через програмне забезпечення у взаємодії між хмарними лабораторіями та користувачами, а також сприяння діалогу між різними режимами експортного контролю щодо роботи зі стартапами та компаніями, що розробляють ІІІ, які впливають на нерозповсюдження хімічної та біологічної зброї [8].

Варто звернути увагу на проблему незаконних передач нематеріальних технологій, яка виникла не лише внаслідок розвитку цифрового середовища, а й існує досить давно. До проблем, пов'язаних з цифровізацією, належать використання віртуальних приватних мереж, даркнету, зашифрованих каналів комунікації, що унеможлиблює контроль змісту повідомлень. Крім того, трансфер нематеріальних технологій (знань) може здійснюватися через онлайн-курси, дослідницькі хаби чи хмарні платформи, що не передбачено дією механізмів дозволів на експорт. Тому відсутність алгоритмів виявлення порушень створює загрозу витоку технологій подвійного використання.

До традиційних шляхів нематеріальних передач технологій належать міжнародні науково-технічні обміни, академічна мобільність, створення спільних науково-технологічних центрів, міжнародні конференції та інші профільні заходи. Американський дослідник, доктор К. Форд, називає одне з таких явищ «військово-цивільною інтеграцією», проаналізувавши візову політику США у відповідь на загрозу викрадення американських технологій студентами з КНР з метою посилення військової потужності своєї держави [9]. Варто зазначити, що правоохоронні органи України теж виявляли спроби незаконного трансферу технологій представниками КНР [10]. У таких ситуаціях забезпечення функціонування експортного контролю насамперед залежить від ефективної організації контррозвідувального режиму всередині країни [11, ст. 6, п. 2].

Ще однією загрозою залишається 3D-друк, який дає змогу передавати «цифрові схеми» для виготовлення зброї безпосередньо в країні призначення [12, с. 52].

В умовах цифрової трансформації традиційний експортний контроль потребує вдосконалення механізмів регулювання передач нематеріальних технологій, що вимагає закріплення як в національному законодавстві, так і в міжнародному праві понять «уявного експорту»

та алгоритмів документування «цифрового сліду» в зашифрованих месенджерах і хмарних сервісах. Для ефективної протидії сучасним загрозам необхідно модернізувати контрольні списки міжнародних режимів експортного контролю та розглянути можливість формування переліків товарів високого пріоритету, зокрема цивільних виробів, у рамках кожного з режимів. Запобігання витоку знань через академічну мобільність, онлайн-курси або 3D-друк потребує посилення контррозвідувального режиму всередині країни та адаптації ліцензійних вимог до послуг у сфері ІІІ та інноваційних технологій. Отже, реформування системи експортного контролю, як на національному, так і на міжнародному рівнях має забезпечувати не лише фізичний нагляд за переміщенням ТВП і ПВ, а й правове регулювання глобальних цифрових інформаційних потоків.

Список використаних джерел

1. Bromley M., Maletta G. The challenge of software and technology transfers to non-proliferation efforts. *Implementing and Complying with Export Controls* / Stockholm International Peace Research Institute. April 2018. URL: https://www.sipri.org/sites/default/files/2018-04/sipri1804_itt_software_bromley_et_al.pdf.
2. Bilousova O. Challenges of Export Controls Enforcement: How Russia Continues to Import Components for Its Military Production / KSE Institute. 2024. URL: <https://kse.ua/wp-content/uploads/2024/01/Challenges-of-Export-ControlsEnforcement.pdf>.
3. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>.
4. Науково-практичний коментар до статті 333 Кримінального кодексу України. URL: https://protocol.ua/ua/kriminalniy_kodeks_ukraini_stattya_333/.
5. Nardon L. Technology strategies in China and the United States, and the challenges for European companies / French Institute of International Relations. 2020. URL: https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/nardon_technology_strategies_china_us_2020.pdf.
6. Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання : Закон України від 20 лют. 2003 р. № 549-IV. URL: <https://zakon.rada.gov.ua/laws/show/549-15#Text>.
7. Bureau of Industry and Security. Common high priority items list (CHPL). URL: <https://www.bis.gov/licensing/country-guidance/common-high-priority-items-list-chpl>.
8. Brockmann K., Héau L., Maletta G. Cloud Labs and Other New Actors in the Biotechnology Ecosystem: Export Control Challenges and Good Practices in Outreach / Stockholm International Peace Research Institute. May 2025. URL: https://www.sipri.org/sites/default/files/2025-05/eunpdc_no_98.pdf.
9. Ford C. A. Technology Transfers to the PRC Military and U.S. Countermeasures: Meeting Security Threats with New Presidential Proclamation. June 5, 2020. URL: <https://www.newparadigmsforum.com/p2631>.

10. Ukraine detains Chinese spies tasked with stealing Neptune missile technology. *The Kyiv Independent*. 2025. URL: <http://web.archive.org/web/20260329172359/https://kyivindependent.com/ukraine-detains-2-chinese-nationals-suspected-of-spying-on-neptun-missile-technology-sbu-says-06-2025/>.

11. Про контррозвідувальну діяльність : Закон України від 26 груд. 2002 р. № 374-IV. URL: <https://zakon.rada.gov.ua/laws/show/374-15#Text>.

12. Кімачук Х. М. Міжнародно-правове регулювання сфери експортного контролю товарів військового призначення та подвійного використання : випускна кваліфікаційна робота / Київський національний торговельно-економічний університет. Київ, 2019. 66 с.

Синоверський Роман Іванович,
аспірант кафедри політики
у сфері боротьби зі злочинністю
та кримінального права Карпатського
національного університету
ім. В. Стефаника

ЗАХИСТ ЦИВІЛЬНОГО НАСЕЛЕННЯ В УМОВАХ ЗБРОЙНИХ КОНФЛІКТІВ ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Захист цивільного населення в умовах збройних конфліктів є одним із ключових напрямів забезпечення національної безпеки України, що зумовлено сучасними викликами, пов'язаними з повномасштабною збройною агресією та трансформацією характеру воєнних загроз. У таких умовах безпека людини, її життя, здоров'я та основоположні права набувають статусу пріоритетної цінності державної політики.

Національна безпека визначається як стан захищеності держави від зовнішніх і внутрішніх загроз, що забезпечує стабільний розвиток і благополуччя населення [1, с. 58].

Крім того, управління національною безпекою передбачає організацію, координацію та контроль за різними аспектами безпеки, такими як оборона, економіка, правоохоронна діяльність та екологія. Важливими складовими є: розвиток національних стратегій безпеки; взаємодія з міжнародними організаціями та союзниками; створення міжвідомчих механізмів для оперативного реагування на загрози [2, с. 85].