

В. О. Западинчук,

здобувач вищої освіти третього (освітньо-наукового) рівня

ORCID ID: <https://orcid.org/0009-0007-1827-7250>

ТЕОРЕТИКО-ПРАВОВІ МОДЕЛІ ГАРМОНІЗАЦІЇ ПРАВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ТА ВИМОГ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: МІЖНАРОДНИЙ ДОСВІД І УКРАЇНСЬКИЙ КОНТЕКСТ

Державний університет «Київський авіаційний інститут»

проспект Любомира Гузара, 1, 03058, Київ, Україна

E-mail: vlad-z9@ukr.net

Мета: виявити та теоретико-правово систематизувати моделі гармонізації прав інтелектуальної власності з вимогами національної безпеки, зіставивши зарубіжні підходи (США, ЄС та мультисторонні форуми) й адаптуючи їх до українського контексту. **Методи дослідження:** нормативно-правовий аналіз (зокрема ст. 73 Угоди ТРІПС, режим секретності винаходів у США, ініціативи ЄС щодо кризового ліцензування), історико-правовий та компаративний підходи, системно-структурне моделювання взаємодії інструментів і інституцій, аналітико-синтетичні процедури узагальнення емпіричних даних та формування рекомендацій. **Результати:** виокремлено три архетипи – (1) патентна секретність як механізм недопущення витоку критичних технологій; (2) кризове управління ІВ (примусове/відкрите ліцензування) для оперативного масштабування життєво важливих розробок; (3) «двоколіїні» корпоративні стратегії балансування патентів і ноу-хау. Показано, що секретність знижує ризики розголошення, але пригнічує комерціалізацію; кризове ліцензування прискорює доступ і виробництво, однак підвищує розвідувально-експортні ризики у високій інтенсивності конфліктах; українська практика фрагментована (нечіткі правила розсекречення, відсутність компенсацій за «секретні патенти», обмежена підтримка приватних оборонних інноваторів). **Обговорення:** обґрунтовано гібридну модель для України, що передбачає прозорі процедури секретності й розсекречення зі справедливою винагородою авторам, гнучкі інструменти кризового ліцензування з часовими та предметними запобіжниками, а також безпеково-екрановану експортну політику; окреслено проблемні питання для подальшої дискусії – критерії та строки розсекречення, механізми компенсації й судового захисту, межі «відкритих ліцензійних зобов'язань» у воєнних умовах, стандарти вибору між патентом і ноу-хау для приватного сектору, інтеграція управління ІВ у архітектуру національної безпеки.

Ключові слова: інтелектуальна власність; національна безпека; гармонізація прав; примусове ліцензування; режим секретних винаходів; кризове управління.

Постановка проблеми та її актуальність. У сучасних умовах національна безпека виходить далеко за межі традиційних військових завдань і охоплює економічну стабільність, технологічний суверенітет, захист критичної інфраструктури та інформаційну безпеку. Водночас права інтелектуальної власності (ІВ) базуються

на ексклюзивності та створенні правових методів для стимулювання інновацій. Ця подвійна логіка породжує внутрішній конфлікт: занадто жорсткі обмеження можуть уповільнювати доступ до критичних розробок у надзвичайних ситуаціях, тоді як надмірна лібералізація загрожує витоком технологій до потенційного противни-

ка. Отже, постає завдання теоретико-правової гармонізації цих двох полюсів – створення механізмів, що би зберігали інноваційний імпульс і водночас забезпечували оперативний захист національних інтересів.

Актуальність теми посилюється в епоху «полікризи», коли одночасно діють пандемічні, кліматичні, кібернетичні й геополітичні виклики. В Україні, що перебуває в стані постійної безпекової загрози, ця проблема набуває особливої гостроти і специфіки, оскільки багато технологічних розробок мають одночасно комерційний і оборонний характер.

Станом на зараз в межах як міжнародного, так і національних законодавств найбільш актуальними є два основні підходи: по-перше, модель секретних об'єктів права інтелектуальної власності, тобто таких, що містять інформацію, віднесenu до державної таємниці; по-друге, концепції кризового управління інтелектуальною власністю із використанням примусового ліцензування під час надзвичайних ситуацій [1]. Українські дослідники звертають увагу на відсутність чіткої системи інтеграції інтересів розробників в рамки захисту національної безпеки [2], що створює розрив між теоретичними моделями та існуючим нормативно-правовим регулюванням. Таким чином, необхідний комплексний огляд і синтез цих підходів для розробки гібридної парадигми, здатної врахувати національні особливості й посилені безпекові ризики.

Аналіз досліджень і публікацій з проблеми. Узгодження прав інтелектуальної власності з пріоритетами національної безпеки розглядається у вітчизняній і зарубіжній літературі переважно крізь призму двох рамок: режимів секретності винаходів та кризового управління правами ІВ. Українські автори акцентують на інституційних лакунах і нестачі інтеграції ІВ у систему безпекового менеджменту (зокрема, пропонуються зміни до ролей суб'єктів нацбезпеки та підходів до охорони ІВ), окремо аналізуючи правову природу «секретних» об'єктів і практичні труднощі їх застосування. Міжнародний дискурс зосереджено на винятку безпеки в ст. 73 Угоди ТРІПС, історичних і сучасних механізмах примусових/відкритих

ліцензій у надзвичайних ситуаціях (від практик мобілізації патентів у воєнний час до моделей пулінгу технологій під час пандемій), а також на емпіричних ефектах патентної секретності для інноваційного циклу та комерціалізації. Разом із тим у більшості робіт бракує деталізованих рішень щодо українських процедур: чітких критеріїв і строків розсекречення, компенсацій за обмеження майнових прав у режимі секретності, алгоритмів кризового ліцензування в умовах високої інтенсивності конфлікту, інтеграції ІВ у архітектуру нацбезпеки та узгодження цих механізмів з експортним контролем; поза належною увагою часто лишається і ризикорієнтоване поєднання патентів і ноу-хау у приватному секторі оборонних технологій. Саме заповнення цих прогалин і становить предмет цього дослідження.

Метою статті є виявлення та теоретико-правова систематизація моделей гармонізації прав інтелектуальної власності та вимог національної безпеки на основі зарубіжного досвіду та їх адаптація до українського контексту. Досягнення поставленої мети передбачає вирішення таких дослідницьких завдань:

1. Систематизувати ключові теоретико-правові підходи до балансування прав інтелектуальної власності і безпекових пріоритетів у різні історичні періоди.

2. Проаналізувати механізми режиму «секретних винаходів», кризового управління правами інтелектуальної власності та інших інструментів у США, ЄС і на рівні міжнародних організацій.

3. Оцінити переваги й ризики застосування кожного з інструментів для забезпечення інноваційного потенціалу та оперативного реагування під час надзвичайних ситуацій.

4. Виявити законодавчі та інституційні прогалини в українській системі захисту оборонних технологій і прав ІВ.

5. Розробити рекомендації щодо формування гібридної парадигми гармонізації інтелектуальної власності і нацбезпеки з урахуванням національних особливостей та поточних викликів.

Виклад основного матеріалу дослідження. Сучасний науковий дискурс зосереджений на пошуку моделей, які дозволяють узгодити екс-

ксклюзивні інтереси прав інтелектуальної власності (ІВ) із пріоритетами національної безпеки. В умовах, коли національна безпека охоплює не лише військову сферу, а й економічну стабільність, технологічний суверенітет та захист критичної інфраструктури, постає конфлікт між приватним та суспільним інтересом. Процес утвердження «суспільства знань» зміщує центр ваги на сектор безпеки не лише в розвитку фундаментальної й прикладної науки та формуванні майбутніх соціальних і професійних еліт, але й у відповідальності за інтерпретацію, поширення та застосування нових знань [3], тож держава мусить враховувати інтелектуальний потенціал при формуванні безпекової стратегії.

Під час узгодження захисту інтелектуальної власності та забезпечення національної безпеки постає складна дилема: з одного боку, надійний правовий захист інновацій підсилює оборонний потенціал держави, а з іншого – надмірна ексклюзивність патентних прав може ускладнити своєчасний доступ до критично важливих технологій у періоди криз та надзвичайних ситуацій. Це лише один, хоча й суттєвий, аспект проблеми; водночас не менш важливим є саме державний контроль над особливо значущими розробками, що реалізується через обмеження прав власників на комерційне використання їхньої інтелектуальної власності.

З одного боку, застосування таких обмежень гарантує, що стратегічні технології не потраплять до потенційного ворога – ця модель де-факто вже застосовується в Україні, зокрема через режим суворого експортного контролю [4]. З іншого ж – довготривалі перешкоди в реалізації майнових прав призводять до економічних збитків для винахідників і гальмують розвиток галузі. Саме тому вирішення проблеми бачиться в розробленні концептуальних підходів балансування, які одночасно враховують потреби національної безпеки й належний захист майнових прав суб'єктів інтелектуальної власності.

Історична еволюція парадигм демонструє поступове формування механізмів такого балансування. Наприклад, уряди могли на час війни дозволяти промисловцям вільно використовувати запатентовані розробки для потреб оборони

без згоди правовласника, особливо що стосується майнових прав іноземних суб'єктів. Як доводять Йорг Батем, Нікола Біанкі та Петра Мозер, за Законом про торгівлю з ворогом 1917 року американська влада конфіскувала загалом 4706 патентів у США, які належали німецьким власникам, і видала невиключні ліцензії на рівних умовах із виплатою роялті будь-якій добросовісній американській особі чи корпорації, щоб спрямувати їх на потреби оборони та відновлення промисловості [5].

Пізніше, у період холодної війни, був інституціоналізований режим «секретних винаходів» – держава отримала право засекречувати окремі патентні заявки з міркувань безпеки. У США це оформлено Актом про секретність винаходів 1951 року, за яким тисячі патентів щорічно підпадають під секретні накази, що забороняють публічне розкриття чутливих розробок. Повідомляється, що станом на 2024 рік в США діяв 6471 такий секретний наказ [6]. Основна мета механізму секретності – не допустити витоку критичних технологій до потенційного противника.

Хоча модель патентної секретності ефективно утримує важливі розробки від розголошення, емпіричні дослідження демонструють її негативні побічні ефекти: примусова секретність обмежувала комерціалізацію та перешкоджала подальшим інноваціям [7]. Інакше кажучи, винаходи, на які накладено секретні накази, не тільки відкладають вихід продукту на ринок, а й створюють «прогалини» в наступних поколіннях інновацій, знижуючи ефективність кумулятивного розвитку технологій.

У свою чергу, концептуальна модель режиму кризового управління інтелектуальною власністю, окреслена зокрема Д. Шармою та колегами, пропонує тимчасово пом'якшувати або адаптувати виключні права під час надзвичайних ситуацій – пандемій, воєн чи інших загроз – щоб дати змогу швидко розширити виробництво критично важливих технологій. Досвід COVID-19 показав, що держава мусить мати в арсеналі як примусове ліцензування, так і механізми стимулювання «відкритих ліцензійних зобов'язань», аби забезпечити безперервний доступ до життєво необхідних розробок і ком-

понентів. О. Макаревич наголошує: задля захисту національної безпеки уряди мають бути готові тимчасово послаблювати патентний режим, відкриваючи шлях до масового виробництва засобів індивідуального захисту та інших необхідних продуктів.

Практичне втілення цієї моделі передбачає поєднання кількох інструментів. По-перше, примусове ліцензування дає змогу організувати серійний випуск технологій навіть без згоди правоутримувача. По-друге, спрощений обмін інноваціями між державними й приватними структурами різко скорочує час виходу на виробничі потужності. По-третє, спеціальні компенсаційні фонди мінімізують фінансові втрати правовласників і зменшують ризик затяжних судових спорів. Нарешті, добровільні відкриті ліцензії, коли компанії зобов'язуються тимчасово надавати свої розробки на безоплатній основі, формують культуру відповідального інноваційного співробітництва.

Світові ініціативи, започатковані під час пандемії, засвідчили ефективність такого підходу: сотні компаній погодилися ділитися патентами та технічною інформацією, що дало змогу оперативно наростити виробничі обсяги й урятувати життя. Отже, «режим кризового управління» пропонує збалансований алгоритм реагування, який одночасно захищає права інтелектуальної власності та забезпечує суспільні інтереси в умовах глобальних викликів [1; 8].

На наднаціональному рівні даний підхід до балансу між інтелектуальною власністю та безпекою інституційно знайшов відображення у нормах міжнародного права. Відповідно до статті 73 Угоди ТРІПС (1994) держави-члени Світової організації торгівлі можуть «уживати будь-які дії, які вони вважають необхідними для захисту своїх істотних інтересів безпеки» навіть тоді, коли такі дії відхиляються від загальних зобов'язань з охорони прав ІВ. Формулювання винятку повторює клаузули про національну безпеку, що походять ще з ГАТТ 1947, і охоплює три категорії: (і) операції з поділюваними матеріалами чи вихідною сировиною; (іі) торгівлю зброєю, боєприпасами й товарами подвійного призначення, що прямо або опосередковано постачають військові формування;

(ііі) дії, учинені «в часи війни або іншої надзвичайної ситуації у міжнародних відносинах». Крім того, пункт (с) дозволяє державі відступити від режиму охорони прав інтелектуальної власності для виконання обов'язків за Статутом ООН щодо підтримання міжнародного миру та безпеки [9].

У відповідь на виклики пандемії та загрозу розриву ланцюгів постачання критичних товарів у березні 2025 року Рада Європейського Союзу та Європейський парламент досягли попередньої згоди щодо Регламенту про примусове ліцензування у кризових ситуаціях, встановивши «уніональну ліцензію крайнього заходу», яка дозволяє за відсутності своєчасної добровільної угоди використовувати запатентовані винаходи без згоди правовласника для забезпечення внутрішнього ринку критично важливими продуктами; при цьому преференцію надають добровільним домовленостям, а успіх переговорів має бути визначений у чітко встановлені строки, аби уникнути затягування процедури. Регламент охоплює всі типи патентів (національні, європейські та єдиної дії), застосовується в усьому просторі ЄС і гарантує, що комерційна таємниця не підлягає автоматичному розкриттю; окремо виключаються з-під дії норми газ, напівпровідники та оборонні продукти, що свідчить про прагнення збалансувати інноваційні стимули та безпекові пріоритети [10].

На глобальному рівні Всесвітня організація охорони здоров'я та її партнери у травні 2020 року започаткували COVID-19 Technology Access Pool (C-TAP) для прискорення, розширення доступу та рівномірного розповсюдження вакцин, ліків і діагностичних засобів шляхом добровільної передачі ліцензій і формування патентних пулів; C-TAP забезпечує платформу для обміну ноу-хау, спрощує укладення трансферних угод і закладає прецедент для подібних механізмів у критичних секторах, зокрема в оборонній промисловості, де вже обговорюються ідеї створення «пулу технологій» в межах НАТО для кіберзахисту на засадах взаємного доступу та інформаційного обміну [11].

Водночас у контексті збройного протистояння впровадження режиму кризового управління інтелектуальною власністю може створити фа-

тальні вразливості для національної безпеки. Досвід поточної війни показує, що російська армія вже неодноразово здійснювала не лише інженерно-технічне знімання зразків, а й їхнє масове відтворення задля власних потреб; відкритий же доступ до ліцензій значно спростить цю практику, позбавивши оборонні структури України критичного часу на розробку захищених рішень і дозволивши противнику оперативно масштабувати наші винаходи з мінімальними витратами ресурсів. У таких умовах навіть тимчасове пом'якшення виключних прав може стати каталізатором технологічної експортної диверсії, коли інновації, що мали слугувати захисту населення або військових формувань, раптово опиняться в арсеналі агресора. Будь-яке рішення про відкриті або примусові ліцензії має супроводжуватися ретельною оцінкою потенційних загроз і обмежувальними механізмами, що мінімізують ризик несанкціонованого копіювання та передачі технологій у вороже середовище.

Важливим аспектом проблеми є адаптація самими компаніями своєї ІВ-стратегії до умов підвищених безпекових ризиків. У контексті діяльності приватних підприємств в оборонній сфері критичною стає оцінка, які саме інновації доцільно оформити як патентні винаходи, а які – захищати в режимі комерційної таємниці (ноу-хау). З одного боку, реєстрація винаходу чи корисної моделі забезпечує компанії ексклюзивне право на використання технології, можливість ліцензування, а також привабливість для інвесторів завдяки чіткому документальному оформленню та «товарному знаку» інновації; натомість така процедура вимагає повного розкриття технічних рішень у патентному описі, підпадає під часові та територіальні обмеження й передбачає значні реєстраційні й підтримувальні витрати. З іншого боку, захист ноу-хау дозволяє утримувати технологію в недоступному форматі без публікації та без часових або географічних меж, але водночас вимагає впровадження суворих внутрішніх протоколів безпеки (NDA, кіберзахист, моніторинг доступу) та не гарантує правового імунітету від незалежного створення аналогічного рішення сторонніми розробниками. Ключовим є принцип «first-

come-first-served», за яким патентні права надаються тому, хто першим подав заявку, тоді як ноу-хау, незареєстроване й невідкрите, може бути відтворене третьою стороною, якщо вона розробить схожий технологічний підхід. Отже, приватні підприємства в оборонній сфері використовують ризик-орієнтований портфельний підхід, аналізуючи комерційну цінність, складність відтворення та безпекові ризики для кожного винаходу: для найбільш уразливих і стратегічно важливих напрацювань застосовують ноу-хау, а для тих, що потребують залучення капіталу та створення правової монополії, – патентують. Така подвійна стратегія водночас забезпечує технологічну перевагу й зберігає гнучкість у разі екстреного державного чи колективного використання розробок під час надзвичайних викликів [12].

В сучасних українських дослідженнях національної безпеки наголошується на тому, що ефективність державної системи захисту критичних технологій значною мірою залежить від глибокої інтеграції питань інтелектуальної власності в структуру безпекового менеджменту. Зокрема, Олександр Зайківський та Олександр Оністрат у праці «Система національної безпеки та питання інтелектуальної власності» підкреслюють, що «за роки незалежності в Україні так і не створено державну систему, яка своєчасно аналізувала б наявні та можливі загрози і виклики національній безпеці у цій сфері та адекватно реагувала б на них розробленням і здійсненням ефективних заходів щодо захисту інтересів держави, авторів об'єктів права інтелектуальної власності (ОПІВ) і замовників цих об'єктів». На їхню думку, вирішальним є розширення функцій суб'єктів системи національної безпеки України – Верховної Ради України та Президента України – шляхом додавання функцій захисту національних інтересів у сфері інтелектуальної власності, а систему охорони інтелектуальної власності визначити складовою сфери забезпечення національної безпеки та оборони [2].

Дійсно, лише в 2023–2024 роках Міністерством оборони України розпочато системні заходи з удосконалення політики в галузі інтелектуальної власності в оборонному секторі, зо-

крема шляхом проведення детального аналізу існуючої системи захисту прав інтелектуальної власності та вивчення найкращих міжнародних практик. До цього часу формування відповідної політики відзначалося фрагментарністю, а відсутність єдиного реєстру або банку даних оборонних патентів і технологій унеможливлювало узагальнене планування на рівні уряду. Незважаючи на обґрунтовані вимоги секретності, державні органи повинні мати доступ до узагальненої інформації про статус розробок: які рішення захищено шляхом патентного захисту, які зберігаються у формі ноу-хау та які придбані у закордонних партнерів. Відсутність такої «карти технологій» гальмує ефективне розподілення ресурсів і визначення пріоритетів у процесах імпортозаміщення.

Залишаються недостатніми і механізми для приватних розробників у сфері оборонних розробок, які б забезпечували повноцінний захист їхніх економічних інтересів. До 2022 року приватні підприємства мали обмежений доступ до участі в державних оборонних проєктах, що зумовлювало непривітні умови, серед яких зокрема затягнуті бюрократичні процедури та відсутність гарантій щодо отримання ліцензій на експортні операції. Попри відкриття оборонних замовлень для приватних виробників після початку широкомасштабної агресії, правові рамки в даній сфері залишаються непрозорими. Зокрема, в разі патентування винаходу виникає ризик обмеження прав державою в інтересах безпеки, тоді як у разі збереження розробки в статусі ноу-хау чи комерційної таємниці розробка фактично втрачає можливість залучення інвестицій через продаж ліцензій. Існуючий механізм секретних патентів демонструє і інші практичні труднощі – наприклад, пов'язані з відсутністю чітких критеріїв розсекречення винаходів у разі втрати реальної загрози національній безпеці. Коли розробка приймається на озброєння або її характеристики вже відомі, продовження її перебування в режимі секретності призводить до марної витрати терміну охорони патенту: власник не може ні оприлюднити технічні рішення, ні ліцензувати розробку, в той час як строки правової охорони спливають. Рішення про розсекречення залежить

виключно від суб'єктивної оцінки державного експерта, що створює ризик «консервації» технологій і унеможливлює їх реалізацію навіть за наявності такої потреби [13]. Крім того, вітчизняне законодавство досі не передбачає механізмів описаної раніше практики компенсації авторам секретних розробок. У результаті, в умовах закритого експорту озброєння, винахідники змушені розраховувати винятково на державне замовлення, що породжує нормативно-інституційні прогалини, які нині частково заповнюються неформальними інструментами (волонтерські фонди, грантові програми, міжвідомчі ініціативи), але вимагають офіційного врегулювання, зокрема через організацію спеціалізованих програм підтримки приватних підприємств в сфері оборони, як то податкові пільги чи державні гранти.

В умовах широкомасштабної агресії в Україні дійсно було запроваджено низку точкових ініціатив, спрямованих на посилення механізмів захисту та управління інтелектуальною власністю в оборонній сфері. Наприклад, платформа Bravel, створена навесні 2023 року як міжвідомчий кластер Defense Tech, об'єднала Міністерство цифрової трансформації, оборони, економіки та інші профільні агенції, надаючи приватним розробникам єдине «вікно» для подання проєктів, фінансової підтримки, доступу до полігонів та менторства з питань патентування й експортного контролю. Додатково, механізми підтримки військових інновацій було інтегровано до правових режимів Дія.City. Водночас, відсутність злагодженої системи взаємодії між суб'єктами інтелектуальної власності та державними структурами, що захищають національні інтереси, призводить до фрагментарності впроваджених заходів. Ініціативи Bravel та інших платформ лише частково полегшують процес впровадження та захисту оборонних розробок, але не вирішують питання відсутності комплексного нормативно-правового регулювання з урахуванням західного досвіду та сучасних моделей. Такий правовий вакуум залишається нагальною проблемою, що потребує системного підходу та інтеграції кращих міжнародних практик.

Висновки. Аналіз правових режимів, покликаних поєднати захист інтелектуальної власності з потребами національної безпеки, засвідчує, що жодна з існуючих моделей не є універсальною. Механізм патентної секретності, що сформувався у сучасному вигляді ще у середині XX століття, дозволив державам ефективно ізолювати критичні технології від доступу потенційного противника, проте водночас значно обмежив можливості комерціалізації та наступної інноваційної активності. Натомість більш гнучка модель кризового управління, яка оформилась у періоди глобальних викликів – як-от пандемія COVID-19 – продемонструвала ефективність у розгортанні виробничих потужностей і мобілізації технологій на користь суспільного інтересу, але зазнала критики через ризики порушення правової визначеності для правовласників і послаблення стимулів до інновацій.

Показовим є те, що навіть найбільш розвинені юрисдикції, як-от США чи Європейський Союз, досі продовжують адаптувати свої підходи, намагаючись досягти балансу між відкритістю і контролем. Від запровадження масових режимів конфіскації патентів у роки Першої світової війни до механізмів добровільного обміну ліцензіями в умовах пандемії – всі ці моделі демонструють гнучкість, але й обмеженість, коли йдеться про довгострокову стратегію в умовах затяжної високотехнологічної війни.

У такому контексті український досвід постає як особливо складний: країна змушена діяти в умовах постійної загрози, обмежених ресурсів і водночас – необхідності інтегруватися в глобальні технологічні та економічні мережі. Наявна фрагментарність регуляторних підходів, обмеженість процедур секретності, повна відсутність окремих механізмів та слабка інтеграція приватного сектору на нормативно-правовому рівні свідчать про незавершеність правової архітектури.

Актуальним видається не механічне запозичення іноземних моделей, а створення власної гібридної парадигми – з урахуванням національної специфіки та потреб воєнного часу. Така модель має поєднувати елементи посиленого захисту критичних технологій (з оновленими,

юридично чіткими процедурами засекречення, розсекречення та компенсації авторам), інструменти швидкої мобілізації інновацій в умовах надзвичайної ситуації (примусове ліцензування, платформи спрощеного доступу), а також стратегічно керовану політику відкритого експорту – з метою підтримки економіки, залучення міжнародних партнерів і формування нових технологічних альянсів.

Відтак, захист інтелектуальної власності в оборонній сфері потребує не так жорсткого обмеження чи лібералізації, як чіткої інтеграції у національну безпекову стратегію. Це означає переосмислення ролі ІВ у структурі воєнної економіки, визнання її ваги для технологічного суверенітету та формування умов, за яких наукова й інженерна думка працює на користь держави без шкоди для свободи інновацій.

Зрештою, йдеться про формування інтегрованої, проактивної стратегії, яка не просто реагує на ризики, а створює умови для цілеспрямованого розвитку оборонних технологій як важеля національного суверенітету. У цьому ключі захист інтелектуальної власності перестає бути виключно правовим завданням – він трансформується у компонент довгострокової безпекової політики, де кожне технічне рішення супроводжується політичним, економічним і стратегічним осмисленням його наслідків.

Література

1. Sharma D., et al. The Changing Role of Innovation for Crisis Management in Times of COVID-19: An Integrative Literature Review. 2022. URL: <https://www.sciencedirect.com/science/article/pii/S2444569X22001160> (дата звернення: 22.05.2025).
2. Зайківський О.Б., Оністрат О.А. Система національної безпеки та питання інтелектуальної власності. *Захист прав інтелектуальної власності*. 2021. № 1. С. 39–47. URL: <http://uran.inprojournal.org/article/view/234187> (дата звернення: 21.05.2025).
3. Кузьменко А.О. Інтелектуальна власність та національна безпека: роль академічної доброчесності. *Науковий вісник Дніпровського державного університету внутрішніх справ*. 2024. № 2. С. 310–315. URL:

<https://doi.org/10.31733/2078-3566-2024-2-310-315> (дата звернення: 21.05.2025).

4. Deutsche Welle. Павліченко: «Летальна зброя з України не вивозиться». 2022. URL: <https://www.dw.com/uk/holova-derzheksportkontroliu-ukraina-ne-eksportuie-zbroiu-ale-deshcho-vyvozytsia/a-62457677> (дата звернення: 21.05.2025).

5. Baten J., Bianchi N., Moser P. Does Compulsory Licensing Discourage Invention? Evidence from German Patents after World War I. Research Briefs in Economic Policy. 2015. No. 37. Washington: Cato Institute. URL: <https://doi.org/10.3386/w21442> (дата звернення: 21.05.2025).

6. Federation of American Scientists. Invention Secrecy. Washington: Federation of American Scientists. б. д. URL: <https://sgp.fas.org/othergov/invention/index.html> (дата звернення: 22.05.2025).

7. Gross R. The Hidden Costs of Securing Innovation: The Manifold Impacts of Compulsory Invention Secrecy. NBER Working Paper No. 25545. Лютий 2019; оновлено квітень 2022. С. 4–5. URL: <https://doi.org/10.3386/w25545> (дата звернення: 22.05.2025).

8. Макаревич О. Інтелектуальні права виробників засобів індивідуального захисту в умовах загрози національній безпеці: між захистом прав інтелектуальної власності та потребою в відкритих інноваціях. *Право. Людина. Довкілля*. 2024. Т. 15. № 4. С. 47–60. URL: <https://doi.org/10.31548/law/4.2024.47> (дата звернення: 21.05.2025).

9. Світова організація торгівлі. Угода про торговельні аспекти прав інтелектуальної власності (ТРИПС): укладена 15 квіт. 1994 р.; набула чинності 1 січ. 1995 р. Женева: Світова організація торгівлі, 1994. Ст. 73.

10. Рада Європейського Союзу; Європейський парламент. Регламент (ЄС) .../2025 Європейського парламенту та Ради від 13 берез. 2024 р. «Про примусове ліцензування у кризових ситуаціях та про внесення змін до Регламенту (ЄС) № 816/2006». *Офіційний журнал Європейського Союзу*. 2025. № С 1 P9_TA(2024)0143. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AC_20250103 (дата звернення: 21.05.2025).

11. World Health Organization. COVID-19 Technology Access Pool (C-TAP): A Global Platform for Voluntary Licensing of COVID-19 Health Technologies. Geneva: WHO. 2020. URL: <https://www.who.int/initiatives/covid-19-technology-access-pool/what-is-c-tap> (дата звернення: 21.05.2025).

12. Мальнев Б., Колесниченко Д. Invention vs. Know-How for Defense Startups: Pros & Cons. The Legal Industry Reviews: Ukraine. 2025. 17 лют. URL: https://www.ey.com/en_ua/insights/defense-tech/invention-vs-know-how-for-defense-startups-pros-cons (дата звернення: 22.05.2025).

13. Андрощук Г.О., Копил Я.В. Інститут секретних винаходів у забезпеченні національної безпеки держави: проблемні питання. *Інформація і право*. 2023. № 2(45). С. 172–185.

References

1. Sharma Dimple, et al. The Changing Role of Innovation for Crisis Management in Times of COVID-19: An Integrative Literature Review. 2022. URL: <https://www.sciencedirect.com/science/article/pii/S2444569X22001160> (accessed May 22, 2025).

2. Zaikivskyi O.B., Onistrat O.A. Systema natsionalnoi bezpeky ta pyttannia intelektualnoi vlasnosti. *Zakhyst prav intelektualnoi vlasnosti*. 2021. No. 1. S. 39–47. URL: <http://uran.inprojournal.org/article/view/234187> (accessed May 21, 2025).

3. Kuzmenko A.O. Intelektualna vlasnist ta natsionalna bezpeka: rol akademichnoi dobrochesnosti. *Naukovyi visnyk Dniprovskogo derzhavnoho universytetu vnutrishnikh sprav*. 2024. No. 2. S. 310–315. URL: <https://doi.org/10.31733/2078-3566-2024-2-310-315> (accessed May 21, 2025).

4. Deutsche Welle. Pavlichenko: «Letalna zbroya z Ukrainy ne vyvozytsya». 2022. URL: <https://www.dw.com/uk/holova-derzheksportkontroliu-ukraina-ne-eksportuie-zbroiu-ale-deshcho-vyvozytsia/a-62457677> (accessed May 21, 2025).

5. Baten Joerg, Nicola Bianchi, and Petra Moser. Does Compulsory Licensing Discourage Invention?

Evidence from German Patents after World War I. Research Briefs in Economic Policy. 2015. No. 37. Washington: Cato Institute. URL: <https://doi.org/10.3386/w21442> (accessed May 21, 2025).

6. Federation of American Scientists. Invention Secrecy. Washington: Federation of American Scientists. n.d. URL: <https://sgp.fas.org/othergov/invention/index.html> (accessed May 22, 2025).

7. Gross Robert. The Hidden Costs of Securing Innovation: The Manifold Impacts of Compulsory Invention Secrecy. NBER Working Paper. 2019. No. 25545 (February; revised April 2022). S. 4–5. URL: <https://doi.org/10.3386/w25545> (accessed May 22, 2025).

8. Makarevych O. Intelektualni prava vyrobnykiv zasobiv indyvidualnoho zakhystu v umovakh zahrozy natsionalnii bezpetsi: mizh zakhystom prav intelektualnoi vlasnosti ta potreboyu v vidkrytykh innovatsiiakh. *Pravo. Liudyna. Dovkillia*. 2024. T. 15. No. 4. S. 47–60. URL: <https://doi.org/10.31548/law/4.2024.47> (accessed May 21, 2025).

9. World Trade Organization. Agreement on Trade-Related Aspects of Intellectual Property Rights. Concluded April 15, 1994; entered into force January 1, 1995. Geneva: World Trade Organization. 1994.

10. Council of the European Union and European Parliament. Regulation (EU) .../2025 of the European Parliament and of the Council of 13 March 2024 on Compulsory Licensing in Crisis Situations and Amending Regulation (EC) No. 816/2006. *Official Journal of the European Union*. 2025. No. C 1 P9_TA(2024)0143. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AC_20250103 (accessed May 21, 2025).

11. World Health Organization. COVID-19 Technology Access Pool (C-TAP): A Global Platform for Voluntary Licensing of COVID-19 Health Technologies. Geneva: WHO. 2020. URL: <https://www.who.int/initiatives/covid-19-technology-access-pool/what-is-c-tap> (accessed May 21, 2025).

12. Malniev B., Kolesnichenko D. Invention vs. Know-How for Defense Startups: Pros & Cons. The Legal Industry Reviews: Ukraine. 2025. February 17. URL: https://www.ey.com/en_ua/insights/defense-tech/invention-vs-know-how-for-defense-startups-pros-cons (accessed May 22, 2025).

13. Androshchuk H.O., Kopyl Ya.V. Instytut sekretnykh vynakhodiv u zabezpechenni natsionalnoi bezpeky derzhavy: problemni pytannia. *Informatsiia i pravo*. 2023. No. 2(45). S. 172–185.

Vladyslav Zapadynchuk

THEORETICO-LEGAL MODELS FOR HARMONIZING INTELLECTUAL PROPERTY RIGHTS AND NATIONAL SECURITY: INTERNATIONAL EXPERIENCE AND THE UKRAINIAN CONTEXT

State University «Kyiv Aviation Institute»
Liubomyra Huzara Avenue, 1, 03058, Kyiv, Ukraine
E-mail: vlad-z9@ukr.net

Purpose: to identify and systematize, in a theoretico-legal perspective, the models for harmonizing intellectual property (IP) rights with national security requirements by comparing foreign approaches (the USA, the EU and multilateral fora) and adapting them to the Ukrainian context. **Research methods:** normative legal analysis (including Art. 73 of the TRIPS Agreement, the U.S. invention secrecy regime, and EU initiatives on crisis licensing), historical-legal and comparative approaches, system-structural modeling of the interactions between instruments and institutions, and analytic-synthetic procedures for generalizing empirical data and deriving recommendations. **Results:** three archetypes are distinguished – (1) patent secrecy as a mechanism to prevent leakage of critical technologies; (2) crisis IP governance (compulsory/open licensing) for rapid scale-up of essential developments; (3) “dual-track” corporate strategies that balance patents and know-how. It is shown that secrecy reduces disclosure risks but suppresses commercialization; crisis licensing accelerates access and production, yet increases intelligence and export-diversion risks in high-intensity conflicts; Ukrainian practice is fragmented (unclear declassification rules, no compensation for “secret patents,” limited support for private defense innovators). **Discussion:** a hybrid model for Ukraine is substantiated that provides for transparent secrecy and declassification procedures with fair remuneration to authors, flexible crisis-licensing tools with temporal and subject-matter safeguards, and a security-screened export policy; problematic issues for further debate are outlined – criteria and timelines for declassification, compensation and judicial-protection mechanisms, the limits of “open licensing commitments” in wartime, standards for choosing between patenting and know-how in the private defense sector, and the integration of IP governance into the national security architecture.

Key words: intellectual property; national security; rights harmonization; compulsory licensing; invention secrecy regime; crisis governance.

Стаття надійшла до редакції 02.09.2025