

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

В. С. ХВОСТЕНКО, канд. екон. наук, доц.

КОНСТРУКТОРСЬКА ДОКУМЕНТАЦІЯ В ОПК: ПРОБЛЕМИ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ (частина 2)

Резюме. У статті досліджується трансформація ролі конструкторської документації (КД) в оборонно-промисловому комплексі (ОПК) України в умовах сучасних безпекових викликів і цифровізації інженерних процесів. Обґрунтовано, що КД перестає виконувати виключно технічну функцію та набуває ознак стратегічного активу, що поєднує інженерний, правовий і безпековий складники. Метою дослідження є комплексний аналіз правового статусу КД як об'єкта інтелектуальної власності (ІВ), виявлення системних проблем її регулювання та визначення напрямів удосконалення моделі управління в ОПК України. Методологічним підґрунтям дослідження є системний і порівняльно-правовий аналіз, а також елементи кейс-стаді, зокрема у сфері MilTech та експортного контролю. У результаті дослідження встановлено, що чинна система управління КД в Україні характеризується фрагментарністю, нормативною неоднорідністю та недостатньою інтеграцією з міжнародними стандартами (ISO, NATO STANAG). Виявлено проблему “зависання” ІВ в умовах режиму секретності, що обмежує можливості комерціалізації, залучення інвестицій і використання сучасних цифрових технологій проектування. Доведено, що відсутність ефективних механізмів гармонізації стандартів, управління правами ІВ і регулювання експортних процесів створює суттєві перешкоди для інтеграції України в глобальні оборонні та виробничі екосистеми. У межах дослідження запропоновано інтегровану VRMN-модель функціонування конструкторської документації в ОПК, що формалізує взаємодію між розробником, державою, PLM-інформаційним середовищем, виробником і замовником у межах єдиного життєвого циклу КД. На відміну від традиційних документо-орієнтованих підходів, запропонована модель розглядає КД як стратегічний цифровий актив, інтегрований у процеси управління інтелектуальною власністю, забезпечення режиму секретності, цифрового управління інженерними даними, виробничого циклу, експлуатації та експортного контролю. Наукова новизна дослідження полягає в комплексному розгляді КД як міждисциплінарного об'єкта, що функціонує на перетині інженерії, економіки, права ІВ і національної безпеки, а також у формуванні концепції її трансформації на стратегічний актив. Практичне значення отриманих результатів полягає у визначенні напрямів реформування системи управління КД, спрямованих на підвищення ефективності функціонування ОПК і його інтеграцію в міжнародні технологічні та безпекові середовища.

Ключові слова: конструкторська документація, інтелектуальна власність, оборонно-промисловий комплекс, стандартизація, експортний контроль, кодифікація НАТО, нематеріальні активи.

Частина 2. ЦИФРОВА ТРАНСФОРМАЦІЯ КД В ОПК: VRMN-МОДЕЛЬ ЖИТТЄВОГО ЦИКЛУ ТА PLM-ПІДХОДИ

7.4. Конфлікти правових режимів та практичні проблеми використання КД. Розглянемо вузлові точки, де виникають труднощі з охороною КД. **Конфлікт між патентним правом і режимом секретності.** Зазвичай патент передбачає оприлюднення винаходу в обмін на правову охорону. У випадку секретних винаходів цей принцип порушується [21]. Проблема: винахідник отримує охоронний документ (секретний патент), але не може вільно розпоряджатися ним на ринку. Наслідок: обмеження можливостей комерціалізації. Винахідник стає “заручником” держави як єдиного замовника.

Складність ведення КД у цифровому форматі. Сучасна конструкторська документація — це не просто креслення, а складні

3D-моделі (BIM- / PLM-системи). Проблема: вимоги до захисту інформації (КСЗІ) часто є застарілими й не встигають за темпами оновлення програмного забезпечення для проектування. Працювати в CAD-системах у “закритих контурах” без доступу до хмарних оновлень чи бібліотек компонентів надзвичайно важко. Ризик: витік даних через використання несертифікованого ПЗ або складність інтеграції різних вузлів від декількох секретних розробників.

Проблема “Винахід подвійного призначення”. Межа між цивільним і військовим винаходом стає дедалі тоншою (наприклад, алгоритми ШІ або дрони). Колізія: якщо розробник створив технологію за приватні кошти, а держава згодом наклала гриф “Секретно”,

то постає питання щодо *справедливої компенсації*. Механізми оцінки вартості секретної КД в Україні та світі залишаються недосконалими.

Передача прав і розсекречення. З часом технології застарівають, а гриф секретності потрібно знімати. Бюрократичні перепони полягають у тому, що процес розсекречення КД часто триває роками. Коли документація нарешті стає доступною для цивільного сектору, технологія вже може бути неактуальною. Втрата кадрового потенціалу полягає в тому, що автори секретних винаходів не можуть публікувати наукові праці, що гальмує їхню професійну кар'єру в академічному середовищі [21; 22]. Практика роботи з секретною КД в Україні найчастіше зосереджена в ОПК та аерокосмічній галузі. Розглянемо декілька типових сценаріїв, які ілюструють реальні проблеми та механізми регулювання:

Сценарій 1: “Винахід подвійного призначення”. Приватне КБ розробило інноваційну систему навігації для дронів, що базується на новому алгоритмі обробки сигналу. Процес: під час подання заявки до “Укрпатенту” (HOIPI), експерт бачить, що технологія підпадає під “Звід відомостей, що становлять державну таємницю”. Результат: заявці присвоюється гриф “Таємно”. Розробник отримує патент на секретний винахід [23]. Проблема: розробник планував продати цю систему агрохолдингам для моніторингу полів, але тепер він не має права показувати КД цивільним замовникам або вивозити зразок на міжнародну виставку без процедури розсекречування, що може тривати роками.

Сценарій 2: Передача КД між підприємствами. На державному підприємстві розроблено новий тип броні. Для серійного виробництва документацію потрібно передати на приватний завод-субпідрядник. Практична складність: приватний завод не може просто отримати PDF-файли електронною поштою. Він зобов'язаний отримати допуск до державної таємниці (пройти перевірку Служби безпеки України (СБУ)), а також створити режимно-секретний орган (РСО) — спеціальний відділ із сейфами, загратованими вікнами та спецзв'язком. Облік КД ведеться в журналах під підпис; копіювання кожної сторінки суворо регламентоване. Конфлікт: витрати на утримання РСО часто перевищують прибуток від самого замовлення для малих підприємств.

Сценарій 3: Судовий спір про винагороду. Інженер працював над секретним двигуном у державному науково-дослідному інституті (НДІ). Винахід впровадили в серійне виробництво ракети, але автор не отримує відрахувань (роялті). Судова практика: оскільки КД секрет-

на, адвокат інженера не може просто прийти до суду і показати *креслення як доказ використання винаходу*. Рішення: суд має проходити в закритому режимі, а всі учасники (суддя, адвокати, патентні повірені, експерти) повинні мати відповідну форму допуску. Це робить захист прав винахідників секретних об'єктів одним із найскладніших процесів у юриспруденції.

Реальні кейси (історико-правовий контекст). Ракетобудування: КД на паливні системи; термін секретності КД (наприклад, розробки 1970-х рр.) часто продовжується автоматично, хоча технології вже відомі світу, що заважає музеєфікації чи цивільному експорту.

Матеріалознавство: сплави для броні; склад сплаву захищений як секретний винахід, але КД на процес плавки часто губиться під час ліквідації заводів у 1990-х рр. через неможливість передачі до приватних архівів.

Криптографія: алгоритми шифрування; винахідник не може опублікувати наукову статтю про свій метод, що гальмує його академічну кар'єру заради національної безпеки.

7.5. Втрати КД та їх вплив на національну безпеку. Майже 20 підприємств ОПК залишилися на непідконтрольній Україні частині Донбасу — заводи з виробництва вибухівки, патронів, електроніки тощо. Угрупування “ЛНР” та “ДНР” заявили про створення власного ОПК. Головне, на що вони полювали, — це технологічна документація на виробництво, а не саме обладнання. На жаль, вона втрачена і потрапила до рук ворога [24]. Росіянам вдалося викрасти унікальну розробку заводу “Топаз” — комплекс радіоелектронної боротьби (РЕБ) “Мандат” вартістю 10 млн дол. США. На тактичному рівні він призначений для визначення та фіксації радіостанцій і засобів радіозв'язку, що працюють в ультракороткохвильовому та короткохвильовому діапазонах, безпосередньо на лінії зіткнення. Однак є підприємства, які евакуювали, зокрема разом із технологічною документацією. На початку російсько-української війни Росія разом зі своїми нелегальними військовими формуваннями остаточно знищила донецький завод “Топаз” — підприємство, що розробляло та виготовляло складні радіотехнічні комплекси. Унікальна система радіотехнічної розвідки “Кольчуга” — це розробка заводу “Топаз” та його команди. На заводі на момент виробництва “Кольчуг”, під час розроблення, модернізації цих станцій була робоча КД як у паперовому вигляді, так і на електронних носіях — на відповідних серверах і комп'ютерах. Важливо, що в системі розроблення та поставлення на виробництво ОВТ опосередковано функціонує страховий фонд України, у межах якого частина КД

за результатами всіх дослідно-конструкторських робіт архівується та передається. У ДК “Укроборонпром” є документація цього страхового фонду. Унікальність системи “Кольчуга” полягає не в залізі, апаратній частині, антенах чи якихось специфічних приладах, хоч і тут є певні нюанси. Неповторністю цієї станції є математика, програмне забезпечення (ПЗ), унікальна обробка отриманих сигналів, створення ехосигналів або шумових радіолокаційних портретів різних цілей, які випромінюють радіохвилі. Конструкція “Кольчуги-М” захищена 8 патентами на винаходи та 12 технологічними ноу-хау. Найважливіше місце серед них посідає технологія мікроелектроніки, на основі якої виробляється 96 збірок, які застосовуються в “Кольчугі-М” [25]. Приватна компанія НБК “Спеціальне конструкторське бюро «Таргет»” демонструвала на XVI Міжнародній спеціалізованій виставці “Зброя та безпека 2019” автоматизовану станцію радіотехнічної розвідки “Кольчуга” РДФ 360. Це повністю нова станція, створена за участю розробників старої “Кольчуги”, після того як держава не змогла відновити її виробництво на НБК “Іскра”. Представляв розробку на виставці заступник директора НБК “Таргет” д-р тех. наук В. В. Яковлев. Це відомий фахівець, ім’я якого згадується також серед розробників СРР “Кольчуга” та лауреатів Державної премії України за розробку і впровадження в серійне виробництво нового покоління комплексу дальньої радіотехнічної розвідки стратегічного призначення “Кольчуга”, а також у патенті на винахід UA № 97271 на станцію радіотехнічної розвідки, виданому в 2012 р., і патенті на винахід UA № 116610 “Комплекс ідентифікації джерел випромінювання”, виданому в 2018 році.

Зазначимо, що вітчизняні науково-виробничі установи, створені ними технології та КД уже давно є об'єктами протиправних посягань іноземних спецслужб. Так, у липні 2011 р. контррозвідка СБУ затримала двох співробітників Торгово-економічної місії КНДР, які намагалися отримати таємні розробки в галузі ракетобудування. За шпигунство їх засудили до 8 років позбавлення волі.

За матеріалами кримінального провадження, кваліфікованого за ст. 114 КК України (шпигунство), професор Сіанського НДІ сучасної хімії здійснював шпигунську діяльність на Дніпропетровщині: організував збір науково-технічної та технологічної документації в галузі бойового ракетобудування, щоб передати її іноземній організації. Юаньцзе здобув освіту в Китайській військовій науковій академії та Фізико-хімічному інституті Академії наук Росії. Він працював у військовій промисловій корпорації, що

спеціалізується на виробництві озброєння, і був нагороджений премією першого ступеня Міноборони КНР “За науково-технічний прогрес армії”. Під час відряджень до України Шу Юаньцзе під прикриттям офіційного науково-технічного співробітництва намагався підкупити групу вітчизняних науковців та схилити їх до “конфіденційного співробітництва”. Офіс Генерального прокурора 28 серпня 2020 р. оприлюднив інформацію: “10 років позбавлення волі — Верховний Суд визнав справедливим покарання шпигуну”. Верховний Суд погодився з доводами Офісу Генерального прокурора та визнав справедливими рішення судів попередніх інстанцій стосовно громадянина КНР, якого було засуджено до 10 років позбавлення волі за шпигунську діяльність. Вирок шпигуну набув законної сили [26].

У 2025 р. в Україні засудили за шпигунство агента іноземної розвідки, який купив і намагався передати “роботодавцям” секретну технічну документацію на український літак. Іноземець у 2022 р. в'їхав на територію України та здійснював шпигунську діяльність. У 2024 р. він налагодив контакт з інженером державного підприємства, запропонувавши йому 1 млн дол. США за технічну документацію на один із вітчизняних літаків. Інженер передав йому флешку з документами, позначеними грифом “Таємно”, які містили інформацію, що становить державну таємницю. Після передачі флешносія агента затримали співробітники СБУ. Його визнали винним (ч. 1, ст. 114 КК України) у збиранні з метою передачі представникам іноземної розвідки технічної документації щодо конструкції вітчизняного літака та засудили до 6 років позбавлення волі [27].

Кваліфікація та санкції за вчинення злочину. Шпигунство є однією з форм об'єктивної сторони складу державної зради (ст. 111 КК України) та самостійним складом злочину (ст. 114 КК України). Відмінність між ними полягає лише в суб'єкті: суб'єктом державної зради у формі шпигунства може бути лише громадянин України, а суб'єктом шпигунства як самостійного складу злочину може бути іноземець або особа без громадянства.

Ст. 114 КК України передбачає відповідальність за шпигунство. У ній зазначено, що передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю, якщо ці дії вчинені іноземцем або особою без громадянства, караються позбавленням волі на строк від 8 до 15 років. Звільняється від кримінальної відповідальності особа, яка припинила діяльність, передбачену частиною

першою цієї статті, та добровільно повідомила органи державної влади про вчинене, якщо внаслідок цього і вжитих заходів було відвернено заподіяння шкоди інтересам України.

Безпосереднім об'єктом шпигунства є зовнішня безпека України, її суверенітет, територіальна цілісність і недоторканність, обороноздатність, державна, економічна чи інформаційна безпека. Предметом цього злочину є відомості, що містять державну таємницю, вичерпний перелік яких міститься в Законі України “Про державну таємницю” від 21 січня 1994 р. (у редакції від 21 вересня 1999 р.). Згідно з цим Законом, державною таємницею визнається певний вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки та техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані в порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою. Ці відомості мають гриф секретності, що визначає його ступінь. Спеціальним уповноваженим органом державної влади у сфері забезпечення охорони державної таємниці є СБУ. З об'єктивного боку шпигунство може проявлятися у двох формах: 1) передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю; 2) збиранні таких відомостей із метою передачі іноземній державі, її організаціям або їх представникам.

Шпигунство чи економічне шпигунство? [26]. Термін “шпигунство” (часто в поєднанні з прикметниками: “промислове”, “економічне”, “комерційне”, “корпоративне”, “науково-технічне”) означає в загальних рисах активні протиправні дії, спрямовані на збирання або розкрадання цінної інформації, закритої для доступу сторонніх осіб. Проте спектр трактування терміна, використовуваного з цими прикметниками, досить широкий: від твердження, що це майже тотожні поняття, до вибудовування ієрархічної схеми взаємозв'язку цих понять (типу “економічне шпигунство” — ширше поняття, яке охоплює такі його підвиди, як промислове, виробниче, науково-технічне, комерційне шпигунство тощо). У США і деяких інших державах ці поняття визначені законодавчо. Так, відповідно до Закону США “Про економічне шпигунство” (The Economic Espionage Act, EEA), прийнятого в 1996 р., і коментарів до нього під економічним шпигунством (Economic espionage) розуміють здійснення суб'єктом зловмисних дій, пов'язаних із: 1) крадіжкою, незаконним присвоєнням, а також отриманням шляхом обману або шахрайства інформації, що становить

комерційну таємницю (секрет виробництва); 2) копіюванням, відтворенням, знищенням, скасуванням і передачею (зокрема через мережу) інформації, що становить комерційну таємницю (секрет виробництва); 3) отриманням інформації, що становить комерційну таємницю (секрет виробництва) з усвідомленням того, що вона була присвоєна чи змінена без відповідного на те дозволу, з метою надання вигоди (переваги) іноземному уряду, державному органу чи агенту. Таким чином, під промисловим шпигунством (Industrial espionage or Theft of trade secrets) розуміють ті самі дії, але вчинені з метою завдання шкоди власникові інформації, що становить комерційну таємницю, пов'язану з виробництвом продукту, що постачається на внутрішній і міжнародний ринки шляхом надання економічної вигоди суб'єкту, який не є власником інформації, що становить комерційну таємницю. Залежно від того, чи мало місце економічне (крадіжка промислових секретів на користь іноземних держав) або промислове шпигунство (крадіжка промислових секретів із комерційною метою), законодавство США визначає відповідні види покарання. Якщо йдеться про діяльність спецслужб і державних структур на зовнішньому ринку — це економічна розвідка. Коли крадіжкою технологій за кордоном займаються приватні фірми — це промислове шпигунство. А в разі, коли технології викрадають одна в одній компанії однієї країни, прийнято говорити про ділову (конкурентну) розвідку, що може використовувати як незаконні способи промислового шпигунства, так і легальні методи конкурентної розвідки. Шпигуном може бути громадянин, який перебуває на службі в розвідці іншої держави, або особа, завербована вороже налаштованою державою для отримання необхідних даних, що доступні йому завдяки виконанню службових обов'язків або обійманню певної посади.

У законодавстві України до 2004 р. також існувало поняття “комерційне шпигунство”. Згідно зі ст. 231 КК України, присвяченій захисту комерційної таємниці, комерційне шпигунство розумілось як “умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю, з метою розголошення, або іншого використання цих відомостей”. Але після внесення змін до статті від 16 грудня 2004 р., у зв'язку з розширенням складу злочину, до якого, окрім комерційної таємниці, було віднесено і банківську таємницю, законодавець вилучив поняття “комерційного шпигунства”. Як зазначає давньокитайський вислів: “Те, що не названо, не існує”.

Аналіз, проведений американською контррозвідкою, показує, що в 58 % випадків економічне і промислове шпигунство здійснювалося

за завданнями зарубіжних компаній, у 22 % — в інтересах іноземних урядів і в 20 % — приватних і державних зарубіжних наукових центрів і лабораторій [26].

Запровадження політики управління ІВ в ОПК України. Уряд нещодавно затвердив політику управління ІВ в ОПК України [28]. Важливе місце в цьому документі відведено КД. Зокрема Кабінет Міністрів України доручив Міноборони України разом з іншими заінтересованими центральними органами виконавчої влади та державними замовниками у сфері оборони: створити єдину інформаційну систему науково-дослідних і дослідно-конструкторських робіт, результатів інтелектуальної діяльності та технологій військового призначення та подвійного використання, *конструкторської документації* на виробі військового призначення у взаємодії з реєстрами *конструкторської документації* на озброєння, військову та спеціальну техніку протягом 9 місяців із дня набрання чинності цим розпорядженням; наповнити єдину інформаційну систему науково-дослідних і дослідно-конструкторських робіт, результатів інтелектуальної діяльності та технологій військового призначення та подвійного використання, *конструкторської документації* на виробі військового призначення у взаємодії з реєстрами *конструкторської документації* на озброєння, військову та спеціальну техніку протягом 12 місяців із дня припинення чи скасування воєнного стану.

7.6. Інтегрована BPMN-модель управління життєвим циклом конструкторської документації в ОПК. З метою систематизації процесів створення, обігу, захисту та використання КД в ОПК доцільно представити інтегровану процесну модель функціонування КД на основі нотації BPMN 2.0. Використання BPMN-підходу дає змогу формалізувати міжорганізаційну взаємодію, інформаційні потоки, контрольні точки прийняття рішень, а також механізми правового, безпекового та регуляторного контролю між учасниками оборонної екосистеми.

Ключовою особливістю запропонованої моделі є розгляд КД не лише як елемента технічного документообігу, а й як комплексного носія результатів інтелектуальної діяльності, технологічного знання, критичних інженерних рішень і виробничого досвіду. У цьому контексті КД одночасно є: об'єктом правової охорони; елементом режиму секретності; джерелом виробничих та експлуатаційних даних; носієм технологій подвійного та оборонного призначення; основою життєвого циклу продукції в ОПК.

На відміну від традиційних моделей документообігу, у межах запропонованого підходу КД розглядається як стратегічний цифровий

актив, який акумулює результати інженерної діяльності, об'єкти права ІВ, елементи ноу-хау і критичні технологічні рішення. Саме наявність у КД таких об'єктів зумовлює необхідність інтеграції процесів захисту ІВ, режиму секретності, цифрового управління інженерними даними, експортного контролю та підтримки життєвого циклу виробу в межах єдиної процесної моделі.

Запропонована модель охоплює взаємодію головних учасників життєвого циклу КД, а саме: розробника; держави / регулятора; PLM-інформаційної системи; виробника; замовника (партнера). У межах моделі КД розглядається не лише як технічний документ, а як комплексний стратегічний актив, що: містить результати інтелектуальної діяльності; може підпадати під режим державної таємниці; є елементом цифрового виробничого середовища; постає об'єктом експортного контролю; забезпечує підтримку життєвого циклу виробу; формує основу технологічного суверенітету та інженерної спадковості в ОПК.

Традиційна система функціонування КД в ОПК України історично формувалася в межах документ-орієнтованої парадигми, успадкованої переважно від радянської системи ЄСКД. У такій моделі КД розглядалася насамперед як набір технічних документів і креслень, необхідних для виготовлення виробу, а не як комплексний цифровий актив, інтегрований у життєвий цикл продукції.

Класична модель характеризувалася: фрагментарністю інформаційних потоків; паперово-орієнтованим документообігом; локальним зберіганням документації; низьким рівнем інтеграції між учасниками процесу; відсутністю єдиного цифрового середовища; слабкою простежуваністю змін і модифікацій; ізолюваністю механізмів захисту ІВ і режиму секретності.

Кожен суб'єкт — конструкторське бюро, виробник, архів, регулятор або військовий замовник — фактично працював із власною копією документації, що ускладнювало синхронізацію змін, контроль актуальності версій та аудит модифікацій. Значна частина процесів здійснювалася з використанням паперових носіїв, локальних серверів чи ізольованих файлових сховищ без централізованого контролю життєвого циклу даних.

У межах традиційного підходу питання ІВ зазвичай не інтегрувалися безпосередньо в процес створення та обігу КД. Об'єкти ІВ часто ідентифікувалися вже після завершення розробки виробу або взагалі залишалися без належної правової охорони. У результаті виникали: конфлікти щодо належності прав; передача КД без ліцензійних механізмів; втрата контролю над

критичними технологіями; відсутність системної інвентаризації ІВ.

Окремою проблемою була ізолюваність режиму секретності від цифрових інженерних процесів. Захист інформації переважно базувався на фізичних механізмах контролю: режимно-секретних органах; паперових журналах обліку; сейфовому зберіганні; територіальних обмеженнях доступу. Така модель істотно ускладнювала цифровізацію, сповільнювала міжорганізаційну кооперацію та обмежувала використання сучасних CAD/PLM-платформ.

Водночас традиційна система фактично не забезпечувала повноцінного зворотного зв'язку (feedback-loop) між етапами експлуатації виробу та оновленням КД. Дані бойового застосування, результати тестування, інформація про відмови або модернізацію часто системно не інтегрувалися в документацію, що призводило до втрати інженерного досвіду та ускладнювало розвиток виробу.

Експортний контроль також функціонував переважно як зовнішня адміністративна процедура, не інтегрована в життєвий цикл КД. У результаті процес передачі документації іноземним партнерам супроводжувався дублюванням перевірок, затримками та додаткови-

ми трансформаціями документації під вимоги окремих ринків.

Запропонована BPMN-модель (рис. 1) принципово змінює підхід до розуміння та функціонування КД в ОПК. У межах нової моделі КД перестає розглядатися виключно як статичний комплект креслень або сукупність технічних документів і трансформується в стратегічний цифровий актив, інтегрований у повний життєвий цикл виробу. Такий підхід передбачає відмову від традиційної документ-орієнтованої парадигми та перехід до lifecycle-oriented моделі, у межах якої КД функціонує як центральний носій інженерних знань, результатів інтелектуальної діяльності та критичних технологічних рішень.

На відміну від класичної системи, де окремі процеси існували ізолювано один від одного, запропонована модель забезпечує інтеграцію інженерних процесів, механізмів управління правами ІВ, режиму секретності, цифрового PLM-середовища, виробничого циклу, експортного контролю та експлуатаційних даних у межах єдиної системи функціонування КД. У результаті документація супроводжує виріб на всіх етапах його існування — від розроблення та виробництва до експлуатації, модернізації та міжнародного технологічного обігу.

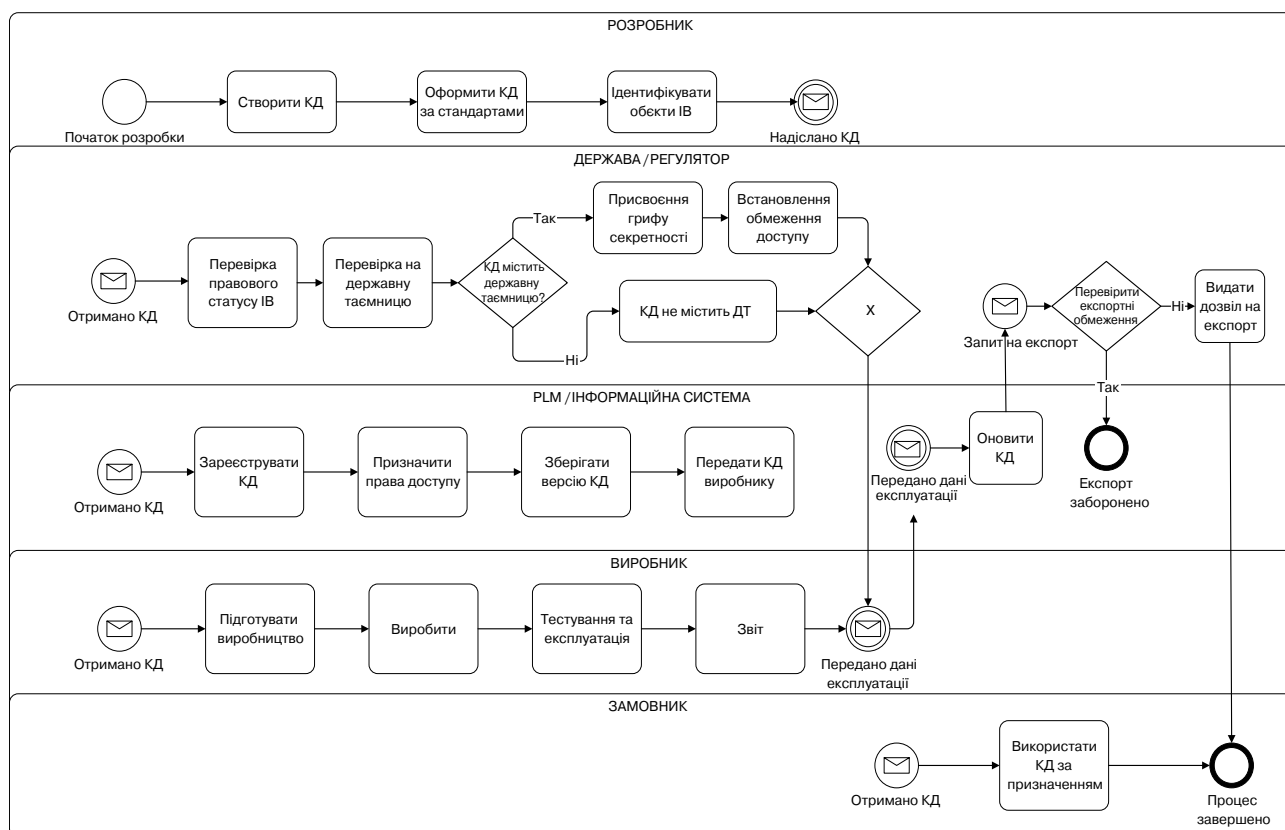


Рис. 1. Інтегрована BPMN 2.0-модель управління життєвим циклом КД в ОПК

Процес функціонування моделі починається в блоці "Розробник". На цьому етапі створюється КД, що містить технічні рішення, креслення, специфікації, програмні компоненти та інші інженерні дані. Після створення КД оформлюється відповідно до встановлених стандартів і нормативних вимог. Далі виконується ідентифікація об'єктів права інтелектуальної власності, у межах якої визначаються елементи документації, що можуть охоронятися авторським правом, патентним правом, режимом охорони комерційної таємниці або ноу-хау.

На відміну від традиційного підходу, у запропонованій моделі ідентифікація об'єктів ІВ інтегрується безпосередньо в процес створення КД, що дає змогу забезпечити ранню фіксацію прав на результати інженерної діяльності та мінімізувати ризики втрати технологій. Після завершення первинного формування КД відбувається її передача державному регулятору. На цьому етапі здійснюється перевірка правового статусу об'єктів ІВ, а також аналіз документації щодо наявності відомостей, що становлять державну таємницю. Якщо КД містить секретну інформацію, їй присвоюється відповідний гриф секретності та встановлюються обмеження доступу. Якщо державна таємниця відсутня, то документація переходить до наступного етапу без застосування спеціального режиму захисту.

Таким чином, у моделі реалізовано інтеграцію правового режиму ІВ із механізмами безпекового та регуляторного контролю, що є критично важливим для оборонної сфери, де технологічні рішення одночасно мають економічну, стратегічну та безпекову цінність. Після завершення перевірок документація інтегрується в PLM/інформаційну систему. На цьому етапі здійснюється: реєстрація КД; управління правами доступу; контроль версій; централізоване зберігання; аудит змін; простежуваність процесів модифікації; передача КД виробнику. PLM-система є центральним елементом цифрового управління життєвим циклом виробу та забезпечує цілісність, актуальність і контрольованість інженерних даних протягом усього періоду існування продукції. У цьому контексті КД перетворюється з набору статичних документів на динамічний цифровий актив, інтегрований у процеси виробництва, модернізації, експлуатації та післяпродажного супроводу.

На відміну від традиційної системи, режим секретності в межах BPMN-моделі перестає бути ізольованим механізмом фізичного контролю та інтегрується в цифрову governance-модель через: контроль доступу; управління правами користувачів; централізовану реє-

страцію документації; аудит дій користувачів; traceability змін.

На етапі виробництва КД використовується для підготовки виробництва, виготовлення продукції, проведення тестування та експлуатації виробу. Важливим складником моделі є формування зворотного зв'язку у вигляді експлуатаційних даних, які передаються назад до PLM-системи та використовуються для оновлення КД.

Такий feedback-loop забезпечує: безперервність життєвого циклу документації; накопичення інженерного досвіду; адаптацію виробу до реальних умов експлуатації; врахування результатів бойового застосування; підтримку процесів модернізації та вдосконалення продукції.

Принципово новим елементом моделі є інтеграція експлуатаційного середовища в процес управління КД, унаслідок чого документація набуває динамічного характеру та постійно адаптується до практичного досвіду використання виробу. У моделі також реалізовано механізм експортного контролю. У разі передачі продукції або КД іноземному партнеру формується запит на експорт. Державний регулятор здійснює перевірку експортних обмежень, відповідності міжнародним режимам контролю та оцінку ризиків передачі критичних технологій. Якщо експорт дозволено, то видається відповідний дозвіл і документація може використовуватися партнером або замовником за призначенням. Якщо експорт заборонено, процес завершується на етапі регуляторного обмеження.

На відміну від традиційної системи, експортний контроль у запропонованій моделі інтегрується безпосередньо в життєвий цикл КД і постає одним із регуляторних checkpoint-процесів, що забезпечує: контроль передачі критичних технологій; відповідність міжнародним режимам контролю; підтримку interoperability з партнерами НАТО; підготовку КД до міжнародного технологічного обігу.

Запропонована BPMN-модель демонструє інтеграцію: процесів управління ІВ; режиму секретності; цифрового документообігу; PLM-підходів; управління життєвим циклом продукції; експортного контролю; механізмів traceability та compliance; взаємодії між учасниками оборонної екосистеми.

Таким чином, запропонована BPMN-модель формує новий підхід до управління КД, у межах якого документація розглядається як: engineering asset; IP asset; security asset; lifecycle asset; knowledge asset; елемент defense governance-екосистеми. У результаті відбувається перехід від фрагментарного документообігу до інтегрованої цифрової системи управління

технологічними знаннями та життєвим циклом продукції в ОПК.

У перспективі запропонована модель може бути використана як концептуальне підґрунтя для: створення цифрових платформ управління КД; побудови інтегрованих PLM-систем оборонного призначення; розвитку систем defense IP governance; гармонізації українських підходів із стандартами НАТО у сфері lifecycle management та interoperability; формування цифрової інфраструктури управління критичними технологіями в ОПК України.

ВИСНОВКИ

Проведене дослідження дає змогу дійти висновку, що КД в ОПК України перебуває в стані трансформації від суто технічного ресурсу до комплексного стратегічного активу, який поєднує інженерний, правовий та безпековий складники. Така трансформація зумовлена як внутрішніми чинниками (цифровізація, розвиток технологій подвійного призначення), так і зовнішніми викликами, пов'язаними з інтеграцією в глобальні оборонні та виробничі екосистеми. Встановлено, що чинна система управління КД в Україні характеризується структурною фрагментарністю, нормативною неоднорідністю та недостатньою інтеграцією з міжнародними стандартами. Збереження елементів ЄСКД у поєднанні з частковою імплементацією стандартів ISO не забезпечує належного рівня інтероперабельності, що створює технічні бар'єри для участі українських підприємств у глобальних ланцюгах створення доданої вартості, зокрема у сфері MilTech. Особливу увагу варто приділити проблемі правового режиму КД як об'єкта ІВ. Відсутність системного підходу до ідентифікації, обліку, оцінки та управління правами на КД, а також недостатня інтеграція інструментів ІВ у діяльність оборонних підприємств призводять до втрати економічної цінності таких активів, зниження інвестиційної привабливості та обмеження можливостей комерціалізації.

Критичним викликом є режим секретності, який, за відсутності ефективних механізмів балансування, призводить до феномену "зависання" ІВ. У таких умовах КД втрачає власності активу, здатного до обігу: обмежується доступ до інвестицій, ускладнюється трансфер технологій, звужуються можливості використання сучасних цифрових інженерних рішень. Окрім того, це створює дисбаланс у правах розробників, які фактично позбавлені можливості повноцінної комерціалізації результатів своєї діяльності.

Встановлено, що практики засекречування та розсекречування КД потребують суттєвого

вдосконалення, оскільки їхня реалізація часто характеризується надмірною дискреційністю та відсутністю чітких часових меж. Це призводить до штучного обмеження обігу технологій, зокрема подвійного призначення, та стримує їх використання в цивільному секторі.

Окремим напрямом проблематики є обмеження цифровізації інженерних процесів в умовах режиму секретності. Нemoжливість повноцінного використання сучасних CAD/PLM-систем, зокрема хмарних рішень, знижує ефективність розробки, збільшує витрати часу та ресурсів, а також поглиблює технологічний розрив із провідними індустриальними країнами.

У контексті зовнішньоекономічної діяльності встановлено, що неузгодженість стандартів, складність процедур експортного контролю та відсутність усталених підходів до оцінки вартості КД як НМА створюють додаткові перешкоди для експорту оборонної продукції та технологій. Це обмежує можливості інтеграції України до міжнародних оборонних екосистем і знижує ефективність використання наявного технологічного потенціалу.

У межах дослідження запропоновано інтегровану BPMN-модель функціонування КД в ОПК, яка дає змогу формалізувати взаємодію між розробником, державою, PLM-інформаційним середовищем, виробником і замовником у межах єдиного життєвого циклу КД. На відміну від традиційних документорієнтованих підходів, запропонована модель розглядає КД як стратегічний цифровий актив, інтегрований у процеси управління ІВ, режиму секретності, цифрового управління інженерними даними, виробничого циклу, експлуатації та експортного контролю.

Запропонована модель демонструє необхідність переходу від фрагментарного документообігу до підходу, орієнтованого на життєвий цикл (integrated lifecycle-oriented), у межах якого КД супроводжує виріб на всіх етапах його існування — від створення та виробництва до експлуатації, модернізації, міжнародної передачі та накопичення експлуатаційного досвіду. Особливе значення в межах моделі має feedback-loop, що забезпечує повернення експлуатаційних даних до PLM-середовища та формування безперервного циклу оновлення КД.

Важливим результатом дослідження є обґрунтування необхідності інтеграції механізмів управління ІВ безпосередньо в процес створення та функціонування КД. У запропонованому підході об'єкти ІВ розглядаються як невіддільний структурний елемент КД, що потребує одночасного врахування правових, технологічних і безпекових аспектів їх використання.

З огляду на викладене, удосконалення системи функціонування КД в ОПК України має здійснюватися на основі комплексного підходу, що передбачає: гармонізацію національних стандартів із міжнародними стандартами ISO та стандартами NATO (STANAG) з метою забезпечення інтероперабельності; формування цілісної системи управління правами ІВ на КД, зокрема їхню ідентифікацію, облік, оцінку та комерціалізацію; запровадження прозорих і регламентованих процедур засекречування та періодичного перегляду рівня секретності; створення компенсаційних механізмів для розробників у разі обмеження прав на використання результатів інтелектуальної діяльності; розвиток захищеної цифрової інфраструктури для обігу КД між суб'єктами ОПК; удосконалення процедур експортного контролю з урахуванням необхідності стимулювання технологічного експорту та інтеграції України до міжнародних оборонно-технологічних (defense-tech) екосистем.

Таким чином, ефективна трансформація системи функціонування КД є необхідною умовою підвищення конкурентоспроможності ОПК України, забезпечення його інтеграції до міжнародних виробничих та оборонних мереж, розвитку технологічного суверенітету держави та реалізації потенціалу КД як стратегічного ресурсу національної безпеки, інноваційного розвитку та економічного зростання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андрощук Г. О. Інтелектуальна власність в оборонній промисловості: стан, тенденції, проблеми та шляхи розв'язання. *Часопис Київського університету права*. 2025. № 2. С. 113–122. DOI: <https://doi.org/10.36695/2219-5521.2.2025.17>.
2. Андрощук Г. О., Хвостенко В. С. Управління інтелектуальною власністю в оборонно-промисловому комплексі. *Інформація і право*. 2026. № 1 (56). С. 107–127. DOI: [https://doi.org/10.37750/2616-6798.2026.1\(56\)](https://doi.org/10.37750/2616-6798.2026.1(56)).
3. Муравський А. Шмигаль розповів про безпрецедентне зростання спроможностей українського ОПК. *Економічна правда*. 2026. 9 січня. URL: <https://epravda.com.ua/biznes/shmigal-rozpoviv-pro-bezprecedentne-zrostantnya-spromozhnostey-ukrajinskogo-opk-816351/>.
4. Терлецький Т. В., Кайдик О. Л., Ткачук А. А., Речун О. Ю. Основи технічної документації: навч. посіб. для студентів технічних спеціальностей / за заг. ред. Т. В. Терлецького. Луцьк: ІВВ Луцького НТУ, 2021. 126 с. URL: <https://surl.li/phhagu>.
5. Капіца Ю. М., Шахбазян К. С., Махновський Д. С. Права інтелектуальної власності у договорах наукових установ на виконання досліджень та розробок / за ред. Ю. М. Капіци. Київ: Академперіодика, 2024. 460 с. URL: E-Book-Prava_int_vlasnosti.
6. Гевко Б. М., Гевко І. Б. Управління процесом розробки і освоєння виробництва нових виробів: підручник. Тернопіль: ТНТУ ім. І. Пулюя, 2015. 200 с. URL: <https://elartu.tntu.edu.ua/handle/123456789/16691>.
7. Щербина В. Ю. Методологія проектування: конспект лекцій. Київ: НТУУ “Київський політехнічний інститут імені Ігоря Сікорського”, 2018. С. 8–13. URL: <https://surl.li/auwxnm>.
8. Андрощук Г. О. Інноваційні адитивні технології 3D-друку: економіко-правові аспекти регулювання / НАПрН України, НДІ інтелект. власності. Київ: Інтерсервіс, 2018. 99 с.
9. ДСТУ 3321:2003. Система конструкторської документації. Терміни та визначення основних понять. Київ: Держспоживстандарт України, 2005. 51 с. URL: <https://www.tsatu.edu.ua/ettp/wp-content/uploads/sites/25/3-dstu-33212003.pdf>.
10. Ванін В. В., Бліок А. В., Гнітецька Г. О. Оформлення конструкторської документації: навч. посіб. Київ: Каравела, 2023. 200 с.
11. ДСТУ В 15.201:2022. Система керування життєвим циклом озброєння та військової техніки. Тактико-технічне (технічне) завдання на виконання дослідно-конструкторської роботи. Загальні вимоги до побудови, змісту, викладення, оформлення, видання та коригування. Зміна № 1 (ІПС № 3-2025). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=114785.
12. Рочняк В. Як кодифікують зброю в країнах НАТО та Україні. *Міністерство оборони України*. 2025. 29 липня. URL: <https://mod.gov.ua/explanation/yak-kodifikuyut-zbroyu-v-krayinah-nato-ta-ukrayini>.
13. Свідерська Я. Як кодифікувати свою військову розробку? Покрокова інструкція для виробників. *Економічна правда*. 2025. 6 січня. URL: <https://epravda.com.ua/experts/yak-kodifikuvati-svoyu-viyskovu-rozrobku-pokroкова-instrukciya-dlya-virobnikiv-801623/>.
14. Покотило О. Міноборони оновило онлайн-сервіс кодифікації озброєння: відповіді на поширені питання виробників. *DEFENDER MEDIA*. 2025. 10 черв. URL: <https://thedefender.media/uk/2025/06/mod-updated-developers-platform/>.
15. Опенько О. У 2025 році кодифіковано понад 350 зразків техніки: скільки вироблено в Україні. *Delo.ua*. 2025. 1 квіт. URL: <https://delo.ua/news/u-2025-roci-kodifikovano-ponad-350-novix-zrazkiv-viiskovoyi-tehniki-87-z-yakiv-vitcziznyanogo-virobnictva-444059/>.
16. Міноборони спростило кодифікацію озброєння та пришвидшило постачання нових розробок до армії. *Юридична газета*. 2026. 2 берез. URL: <https://yur-gazeta.com/golovna/minoboroni-sprostili-kodifikaciyu-ozbroennya-ta-prishvidshili-postachannya-novih-rozrobok-do-armiyi.html>.
17. Андрощук Г. О., Давимука С. А. Інтелектуальна власність у науково-технічній сфері: методи та принципи вартісної оцінки: монографія. Київ: Парламентське видавництво, 2014. 304 с. URL: <https://librarygo.lpnu.ua/?elbook=intelektualna-vlasnist-u-naukovo-tehnichnij-sferi-metody-ta-pryncyipy-vartisnoyi-ocznky>.
18. ТОП-15 корупційних ризиків в управлінні підприємствами ДК “Укроборонпром” та шляхи їх подолання. Стратегічний аналіз корупційних ризиків. *Національне агентство з питань запобігання корупції*. 2021. 44 с. URL: <https://nazk.gov.ua/wp-content/uploads/2021/11/NAZK-1.pdf>.
19. Канарьова Н. Технічні умови як об'єкт авторського права. *Дебет-кредит*. 2018. № 33. URL: <https://online.dtki.ua/2018/33/56796>.
20. Пам'ятка з питань охорони та захисту інтелектуальної власності для розробників товарів оборонного призначення. *Український національний офіс інтелектуальної власності та інновацій*

- (УКРХОІВІ). 2025. 20 с. URL: https://nipo.gov.ua/wp-content/uploads/2025/05/IP_pamiatka_rozrobnykam_tovariv_oboronnogo_pryznachennia-web.pdf.
21. Андрощук Г. О. Інститут секретних винаходів як фактор забезпечення національної безпеки. *Наука та наукознавство*. 2020. № 4. С. 24–43. URL: <http://jnas.nbuv.gov.ua/article/UJRN-0001201766>.
 22. 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. DOI: [https://doi.org/10.37750/2616-6798.2023.2\(45\).282338](https://doi.org/10.37750/2616-6798.2023.2(45).282338).
 23. Андрощук Г. О. Секретні винаходи: проблеми експертизи заявок. *Наука, технології, інновації*. 2025. № 1. С. 79–93. DOI: <http://doi.org/10.35668/2520-6524-2025-1-09>.
 24. Пагулич Р., Головін Є. Як працюють захоплені військові заводи під контролем угруповань “ЛНР” та “ДНР”? *Радіо “Свобода”*. 2018. 8 жовт. URL: <https://www.radiosvoboda.org/a/29530434.html>.
 25. Шинко А. “Кольчуга”: приватна компанія розробила свою версію станції. *Ukrainian Military Pages*. 2019. 16 жовт. URL: <https://www.ukrmilitary.com/2019/10/kolchuga.html>.
 26. Андрощук Г. Вирок Верховного Суду України китайському шпигуну-науковцю: 10 років позбавлення волі. *Юридична газета*. 2020. 4 верес. URL: <https://yur-gazeta.com/publications/practice/inshe/virok-verhovnogo-sudu-ukrayini-kitayskomu-shpigununaukovcyu-10-rokiv-pozbavlennya-voli.html>.
 27. “Купував за \$1 млн секретні дані”. В Україні тюремний термін отримав агент іноземної розвідки. *NV Україна*. 2025. 4 лист. URL: <https://nv.ua/ukr/ukraine/events/shpigunstvo-v-oboronomu-sektori-v-ukrayini-do-uv-yaznennya-zasudili-agenta-inozemnoji-rozvidki-50557762.html>.
 28. Про затвердження політики управління інтелектуальною власністю в оборонно-промисловому комплексі України: розпорядження Кабінету Міністрів України від 10 квіт. 2026 р. № 342-р. URL: <https://zakon.rada.gov.ua/laws/show/342-2026-%D1%80#Text>.
- ## REFERENCES
1. Androshchuk, H. O. (2025). Intelektualna vlasnist v oboronni promyslovosti: stan, tendentsii, problemy ta shliakhy rozv'yazannia [Intellectual property in the Defense Industry: Status, Trends, Problems and Solutions]. *Chasopys Kyivskoho universytetu prava* [law Review of Kyiv University of Law], 2, 113-122. DOI: <https://doi.org/10.36695/2219-5521.2.2025.17>.
 2. Androshchuk, H. O. & Khvostenko, V. S. (2026). Upravlinnia intelektualnoi vlasnistiu v oboronno-promyslovomu kompleksi [Intellectual property management in the defense-industrial complex]. *Informatsiia i pravo* [Information and law], 1 (56), 107-127. DOI: [https://doi.org/10.37750/2616-6798.2026.1\(56\)](https://doi.org/10.37750/2616-6798.2026.1(56)).
 3. Muravskiy, A. (January 9, 2026). Shmyhal rozpoviv pro bezpretsedentne zrostannia spromozhnosti ukrainskoho OPK [Shmyhal spoke about the unprecedented growth of the capabilities of the Ukrainian Defense Industry]. *Economic Truth*. Retrieved from: <https://epravda.com.ua/biznes/shmihal-rozpoviv-pro-bezpretsedentne-zrostannya-spromozhnostey-ukrajinskogo-opk-816351/>.
 4. Terletskiy, T. V., Kaidyk, O. L., Tkachuk, A. A., & Rechun O. Iu.; Terletskiy, T. V. (Eds.). (2021). Osnovy tekhnichnoi dokumentatsii: Navchalnyi posibnyk dlia studentiv tekhnichnykh spetsialnosti [Fundamentals of Technical Documentation: A textbook for students of technical specialties]. Lutsk, 126 p. Retrieved from: <https://surl.li/pfhagu>.
 5. Kapitsa, Yu. M., Shakhbazian, K. S., & Makhnovskiy, D. S.; Kapitsa, Yu. M. (Eds.). (2024). Prava intelektualnoi vlasnosti u dohovorakh naukovykh ustanov na vykonannia doslidzhen ta rozrobok [Intellectual property rights in contracts between scientific institutions for the performance of research and development]. Kyiv, 460 p. Retrieved from: E-Book-Prava_int_vlasnosti [in Ukr.].
 6. Hevko, B. M., & Hevko, I. B. (2015). Upravlinnia protsesom rozrobky i osvoennia vyrobnytstva novykh vyrobiv [Managing the process of developing and mastering the production of new products]. Ternopil, 200 p. Retrieved from: <https://elartu.tntu.edu.ua/handle/123456789/16691> [in Ukr.].
 7. Shcherbyna, V. Yu. (2018). Metodolohiia proektuvannia [Design methodology: lecture notes]. Kyiv, 8-13. Retrieved from: <https://surl.li/auwxnm>. [in Ukr.].
 8. Androshchuk, H. O. (2018). Innovatsiini adytyvni tekhnolohii 3D-druku: ekonomiko-pravovi aspekty rehuliuвання [Innovative additive 3D printing technologies: economic and legal aspects of regulation]. Kyiv, 99 p. [in Ukr.].
 9. DSTU3321: 2003 (2005). Systema konstruktorskoj dokumentatsii. Terminy ta vyznachennia osnovnykh poniat. [Design documentation system. Terms and definitions of basic concepts]. Kyiv, 51 p. Retrieved from: <https://www.tsatu.edu.ua/ettp/wp-content/uploads/sites/25/3-dstu-33212003.pdf> [in Ukr.].
 10. Vanin, V. V., Bliok, A. V., & Hnitska, H. O. (2023). Oformlennia konstruktorskoj dokumentatsii [Design documentation preparation]. Kyiv, 200 p. [in Ukr.].
 11. DSTU V 15.201:2022. Systema keruvannia zhytievym tsyklom ozbroiennia ta viiskovoi tekhniky. Taktyko-tekhnichne (tekhnichne) zavdannia na vykonannia doslidno-konstruktorskoj roboty. Zahalnyi vymohy do pobudovy, zmistu, vykladennia, oformlennia, vydannia ta koryhuvannia. Zmina № 1 (IPS № 3-2025) [DSTU V 15.201:2022 Life cycle management system for weapons and military equipment. Tactical and technical (technical) task for the performance of research and development work. General requirements for construction, content, presentation, design, publication and correction. Amendment No. 1 (IPS No. 3-2025)]. Retrieved from: https://online.budstandart.com.ua/catalog/doc-page.html?id_doc=114785 [in Ukr.].
 12. Rochniak, V. (July 29, 2025). Yak kodyfikuiut zbroiu v krainakh NATO ta Ukraini [How weapons are codified in NATO countries and Ukraine]. *Ministerstvo oborony Ukrainy*. Retrieved from: <https://mod.gov.ua/explanation/yak-kodyfikuyut-zbroiyu-v-krayinah-nato-ta-ukrayini> [in Ukr.].
 13. Sviderska, Ya. (January 6, 2025). Yak kodyfikuvaty svoiu viiskovu rozrobku? Pokrokovia instruktsiia dlia vyrobnykiv [How to codify your military developers? A step-by-step guide for manufacturers]. *Economic Truth*. Retrieved from: <https://epravda.com.ua/experts/yak-kodyfikuvaty-svoyu-viyskovu-rozrobku-pokrokovia-instrukciya-dlya-virobnikiv-801623/> [in Ukr.].
 14. Pokotylo, O. (June 10, 2025). Minoborony onovlo onlain-servis kodyfikatsii ozbroiennia: vidpovidi na poshyreni pytannia vyrobnykiv [The Ministry of Defense has updated the online service for weapons codification: answers to frequently asked questions]

- from manufacturers]. *DEFENDER MEDIA*. Retrieved from: <https://thedefender.media/uk/2025/06/mod-updated-developers-platform/> [in Ukr.].
15. Openko, O. (April 1, 2025). V 2025 rotsi kodyfikovano ponad 350 zrazkiv tekhniki: skilky vyrobлено v Ukraini [In 2025, more than 350 types of equipment were codified: how many were produced in Ukraine]. *Delo.ua*. Retrieved from: <https://delo.ua/news/u-2025-roci-kodyfikovano-ponad-350-novix-zrazkiv-viiskovoyi-tekhniki-87-z-yakix-vitciznyanogovirobnictva-444059/> [in Ukr.].
 16. (2026). Minoborony sprostily kodyfikatsiiu ozbroiennia ta pryshvydshyly postachannia novykh rozrobok do armii [The Ministry of Defense simplified the codification of weapons and accelerated the supply of new developments to the army]. *Yurydychna hazeta* [Legal newspaper], March 2. Retrieved from: <https://yur-gazeta.com/golovna/minoborony-sprostili-kodyfikatsiyu-ozbroennya-ta-prishvidshili-postachannya-novykh-rozrobok-do-armiyi.html> [in Ukr.].
 17. Androshchuk, H. O., & Davymuka, S. A. (2014). Intelktualna vlasnist u naukovu-tekhnichnii sferi: metody ta pryntsyipy vartisnoi otsinky [Intellectual property in the scientific and technical sphere: methods and principles of valuation]. Kyiv, 304 p. Retrieved from: <https://librarygo.lpnu.ua/?elbook=intelektualna-vlasnist-u-naukovu-tekhnichnij-sferi-metody-ta-pryncypy-vartisnoyi-oczinky> [in Ukr.].
 18. (2021). TOP-15 koruptsiinykh ryzykiv v upravlinnia pidpriemstvamy DK "UKROBORONPROM" ta shliakhy yikh podolannia. Stratehichnyi analiz koruptsiinykh ryzykiv [TOP-15 corruption risks in the management of enterprises of the State Enterprise "UKROBORONPROM" and ways to overcome them. Strategic analysis of corruption risks]. *Natsionalne ahentstvo z pytan zapobihannia koruptsii*. 44 p. Retrieved from: <https://nazk.gov.ua/wp-content/uploads/2021/11/NAZK-1.pdf> [in Ukr.].
 19. Kanarova, N. (2018). Tekhnichni umovy yak ob'ekt avtorskoho prava [Technical specifications as an object of copyright], *Debet-kredyt* [Debit-credit], 33. Retrieved from: <https://online.dtki.ua/2018/33/56796> [in Ukr.].
 20. (2025). Pamiatka z pytan okhorony ta zakhystu intelektualnoi vlasnosti dlia rozrobnykiv tovariv oboronnoho pryznachennia [Memorandum on the protection and enforcement of intellectual property for developers of defense products]. *Ukrainskyi natsionalnyi ofis intelektualnoi vlasnosti ta innovatsii*. 20 p. Retrieved from: https://nipo.gov.ua/wp-content/uploads/2025/05/IP_pamiatka_rozrobnykam_tovariv_oboronnoho_pryznachennia-web.pdf [in Ukr.].
 21. Androshchuk, H. O. (2020). Instytut sekretnykh vynakhodiv yak faktor zabezpechennia natsionalnoi bezpeky [The Institute of Secret Inventions as a Factor in Ensuring National Security]. *Nauka ta naukoznavstvo* [Science and scientific studies], 4, 24-43. Retrieved from: <http://nas.nbuv.gov.ua/article/UJRN-0001201766> [in Ukr.].
 22. Androshchuk, H. O. & Kopyl, Ya. V. (2023). Instytut sekretnykh vynakhodiv u zabezpechenni natsionalnoi bezpeky derzhavy: problemni pytannia [The Institute of Secret Inventions in Ensuring National Security of the State: Problematic Issues]. *Informatsiia i pravo* [Information and law], 2 (45), 172-185. DOI: [https://doi.org/10.37750/2616-6798.2023.2\(45\).282338](https://doi.org/10.37750/2616-6798.2023.2(45).282338) [in Ukr.].
 23. Androshchuk, H. O. (2025). Sekretni vynakhody: problemy ekspertyzy zaiavok [Secret application examination problems]. *Nauka, tekhnolohii, innovatsii* [Science, technology, innovation], 1, 79-93. DOI: <http://doi.org/10.35668/2520-6524-2025-1-09> [in Ukr.].
 24. Pahulych, R., Holovin, Ye. (October 8, 2018). Yak pratsiuut zakhopleni viiskovi zavody pid kontrolem uhrupovan "LNR" ta "DNR"? [How do captured military factories under the control of the "LPR" and "DPR" groups operate?]. *Radio Liberty*. Retrieved from: <https://www.radiosvoboda.org/a/29530434.html> [in Ukr.].
 25. Shynko, A. (October 16, 2019). "Kolchuga": pryvatna kompaniia rozroblyla svoiu versiiu stantsii ["Kolchuga": a private company has developed its own version of the station]. *Ukrainian Military Pages*. Retrieved from: <https://www.ukrmilitary.com/2019/10/kolchuga.html> [in Ukr.].
 26. Androshchuk, H. O. (2020). Vrok Verkhovnoho Sudu Ukrainy kytaiskomu shpyhunu-naukovtsiu: 10 rokiv pozbavlennia voli [Supreme Court of Ukraine sentences Chinese spy scientist to 10 years in prison]. *Yurydychna hazeta* [Legal newspaper], September 4. Retrieved from: <https://yur-gazeta.com/publications/practice/inshe/vrok-verhovnogo-sudu-ukrayini-kitayskomu-shpigununaukovcyu-10-rokiv-pozbavlennya-voli.html> [in Ukr.].
 27. (2025). "Kupuvav za \$1 mln sekretni dani". V Ukraini tiuremnyi termin otrymav ahent inozemnoi rozvidky ["I bought secret data for \$1 million." A foreign intelligence agent received a prison sentence in Ukraine]. *HV Ukraine, November 4*. Retrieved from: <https://nv.ua/ukr/ukraine/events/shpigunstvo-v-oboronnomu-sektori-v-ukrayini-do-uv-yaznennya-zasadili-agenta-inozemnoji-rozvidki-50557762.html> [in Ukr.].
 28. (2026). Pro zatverdzhennia polityky upravlinnia intelektualnoiu vlasnistiu v oboronno-promyslovomu kompleksi Ukrainy: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 10 kvitnia 2026 r. № 342-r. [On approval of the intellectual property management policy in the defense-industrial complex of Ukraine: Resolution of the Cabinet of Ministers of Ukraine dated April 10, 2026 No. 342-r.]. Retrieved from: <https://zakon.rada.gov.ua/laws/show/342-2026-%D1%80#Text> [in Ukr.].

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

V. S. KHVOSTENKO, PhD in Economics, Associate Professor

DESIGN DOCUMENTATION IN THE DEFENSE INDUSTRY: INTELLECTUAL PROPERTY ISSUES (part 2)

Abstract. The article examines the transformation of the role of design documentation (CD) in the defense-industrial complex (DIC) of Ukraine in the context of modern security challenges and digitalization of engineering processes. It is substantiated that CD ceases to perform an exclusively technical function and acquires the

features of a strategic asset that combines engineering, legal and security components. The purpose of the study is a comprehensive analysis of the legal status of CD as an object of intellectual property (IP), identifying systemic problems of its regulation and determining directions for improving the management model in the defense-industrial complex of Ukraine. The methodological basis of the study is a systemic and comparative legal analysis, as well as elements of a case study, in particular in the field of MilTech and export control. As a result of the study, it was established that the current CD management system in Ukraine is characterized by fragmentation, regulatory heterogeneity and insufficient integration with international standards (ISO, NATO STANAG). The problem of “freezing” of IP in conditions of secrecy regime was revealed, which limits the possibilities of commercialization, attraction of investments and use of modern digital design technologies. It is proved that the lack of effective mechanisms for harmonization of standards, management of IP rights and regulation of export processes creates significant barriers for Ukraine’s integration into global defense and production ecosystems. The study proposes an integrated BPMN model of the functioning of design documentation in the defense industry, which formalizes the interaction between the developer, the state, the PLM information environment, the manufacturer and the customer within a single CD life cycle. Unlike traditional document-oriented approaches, the proposed model considers CD as a strategic digital asset integrated into the processes of intellectual property management, secrecy regime, digital engineering data management, production cycle, operation and export control. The scientific novelty of the study lies in the comprehensive consideration of CD as an interdisciplinary object that functions at the intersection of engineering, economics, IP law and national security, as well as in the formation of the concept of its transformation into a strategic asset. The practical significance of the results obtained lies in determining the directions of reforming the CD management system aimed at increasing the efficiency of the functioning of the defense industry and its integration into international technological and security environments.

Keywords: design documentation, intellectual property, defense-industrial complex, standardization, export control, NATO codification, intangible assets.

ІНФОРМАЦІЯ ПРО АВТОРІВ

Андрощук Геннадій Олександрович — канд. екон. наук, доц., голов. н. с., Науково-дослідний інститут інтелектуальної власності НАПрН України; вул. Казимира Малевича, 11, корп. 4, м. Київ, Україна, 03680; +38 (044) 200-08-76; genandro1@gmail.com; ORCID: 0000-0003-0781-9740

Хвостенко Владислав Сергійович — канд. екон. наук, доцент, доцент кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”; патентний повірений; вул. Кирпичова, 2, Харків, 61000; +38 (068) 214-14-68; vladyslav.khvostenko@gmail.com; ORCID: 0000-0002-6436-4159

INFORMATION ABOUT THE AUTHORS

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; 11, Kazymyra Malevycha Str., building 4, Kyiv, Ukraine, 03680; genandro1@gmail.com; +38 (044) 200-08-76; ORCID: 0000-0003-0781-9740

Khvostenko V. S. — PhD in Economics, Associate Professor, Associate Professor of the Department of Cybersecurity, National Technical University “Kharkiv Polytechnic Institute”; Patent Attorney; 2, Kyrpychova Str., Kharkiv, Ukraine, 61000; +38 (068) 214-14-68; vladyslav.khvostenko@gmail.com; ORCID: 0000-0002-6436-4159



Надійшла до редакції 20.05.2026

Прийнята до друку 03.08.2026

Опубліковано 30.09.2026

