Інформаційна довідка
щодо перспективного розвитку оборонних інновацій*

Анотація. *В інформаційній довідці розглянуто питання удосконалення законодавства у сфері інноваційної діяльності сил оборони, прискорення розробки, фінансування та впровадження новітніх військових технологій (зокрема штучного інтелекту, безпілотних систем та РЕБ) безпосередньо на полі бою в контексті законопроєкту за реєстр. № 15215 від 01.05.2026.*

З урахуванням кращих європейських практик та закордонних напрацювань запропоновано комплекс заходів, спрямованих на створення єдиної, прозорої та гнучкої екосистеми управління й фінансування оборонних інновацій, яка гармонізує національне законодавство із стандартами й принципами НАТО та ЄС.

Ключові слова: *національна безпека, вітчизняний сектор оборонних технологій, інноваційна діяльність у сфері оборони, оборонна промисловість, інвестиційна привабливість, технологічний потенціал держави, стартап.*

Вступ

В умовах збройної агресії російської федерації проти України технологічне оновлення та інноваційний розвиток оборонного сектору мають важливе значення для зміцнення національної безпеки й обороноздатності держави. Цей вектор досліджень перебуває у постійному полі зору Дослідницької служби[1].

Європейська інтеграція України, зокрема відкриття переговорів за Кластером 6 «Зовнішні відносини», що охоплює питання спільної зовнішньої політики та політики безпеки й оборони Європейського Союзу, актуалізує потребу в подальшому вдосконаленні національного законодавства з урахуванням права ЄС та відповідних європейських підходів у цій сфері.

Важливим чинником розвитку оборонних спроможностей України є здатність оперативно розробляти, випробовувати та впроваджувати технологічні рішення відповідно до потреб сил оборони. Особливістю вітчизняного сектору оборонних технологій є скорочення часу від розроблення технічного рішення до його застосування в бойових умовах. Цьому сприяють взаємодія державних інституцій із приватними розробниками, залучення інженерного потенціалу та адаптація інновацій до змін на полі бою.

До пріоритетних напрямів розвитку оборонних технологій належать удосконалення безпілотних і роботизованих систем, застосування технологій штучного інтелекту, розвиток цифрових систем управління бойовими діями, посилення кібербезпеки та вдосконалення засобів збирання й обміну розвідувальною інформацією. Реалізація цих напрямів потребує не лише технологічних рішень, а й належного нормативно-правового забезпечення, яке

---

[1] Дослідницька служба Верховної Ради вивчила досвід військових технологічних парків країн НАТО. *Голос України.* 31.10.2026. URL: https://www.golos.com.ua/article/393304; Інформаційна довідка щодо законодавчого забезпечення діяльності військових технологічних парків у деяких державах-членах НАТО: досвід для України. *Дослідницька служба Верховної Ради України*. URL: https://research.rada.gov.ua/uploads/documents/33138.pdf

сприятиме розвитку інновацій, залученню приватного сектору та ефективній взаємодії учасників відповідної діяльності.

За таких умов законодавче регулювання інноваційної діяльності у сфері оборони має забезпечувати належні правові засади розроблення, випробування та впровадження новітніх технологій, оптимізацію відповідних процедур, визначення повноважень залучених суб'єктів і розширення можливостей фінансування. Водночас спрощення процедур має поєднуватися з дотриманням вимог безпеки та забезпеченням ефективного використання ресурсів.

Зазначені питання є предметом проєкту Закону України «Про внесення змін до деяких законодавчих актів України щодо інноваційної діяльності сил оборони» (реєстр. № 15215 від 01.05.2026). Ним передбачається створення комплексної системи управління інноваціями у сфері оборони, удосконалення процесу її фінансування та зростання спроможностей сил оборони, що у перспективі надасть змогу значно підвищити технологічну оборонну конкурентоспроможність України та забезпечити національну безпеку держави. Водночас завданнями законопроєкту визначено: запровадити термінологію, пов'язану із інноваціями у сфері оборони; визначити перспективні шляхи формування та реалізації інноваційної політики у сфері оборони; визначити суб'єктів, які залучаються до інноваційної діяльності у сфері оборони; встановити особливості регулювання інноваційної діяльності у сфері оборони; розширити спектр можливостей щодо фінансування інноваційної діяльності у сфері оборони.

У зв'язку з цим пропонується внести зміни до статі 15 Закону України «Про національну безпеку», статей 3, 10, 11, 12 Закону України «Про оборону України», статей 1, 30 Закону «Про оборонні закупівлі», статей 1, 3, 6, 9, 11, 12 Закону України «Про інноваційну діяльність».

З огляду на викладені в законопроєкті пропозиції, вважаємо за доцільне зазначити таке.

Основна частина

Попри позитивну ідею та цілеспрямованість представленого законопроєкту, існують певні ризики щодо нього.

Так, запропонований у законопроєкті механізм фінансової підтримки інноваційної діяльності у сфері оборони, потребує оцінки з огляду на прозорість відбору проєктів, обґрунтованість розподілу бюджетних коштів та контроль за результатами їх реалізації.

Насамперед доцільно зазначити, що надання державної фінансової підтримки або грантів без обов'язкової державної реєстрації відповідних інноваційних проєктів, за відсутності альтернативних механізмів обліку та перевірки, може ускладнити забезпечення прозорості й об'єктивності їх відбору. Зокрема, недостатня визначеність критеріїв оцінювання, порядку ухвалення рішень і вимог до заявників може створювати передумови для дискреційного розподілу коштів та нерівних умов доступу до державної підтримки.

Відсутність єдиного механізму обліку інноваційних розробок також може ускладнювати перевірку їхньої унікальності, визначення стадії готовності та встановлення факту попереднього фінансування аналогічних розробок за рахунок бюджетних коштів. Це створює ризик дублювання фінансування та нераціонального використання державних ресурсів.

Окремої уваги потребує визначення умов надання фінансової підтримки та відповідальності за результати виконання інноваційних проєктів. Якщо порядок фінансування не передбачатиме чітких етапів реалізації, критеріїв оцінювання досягнутих результатів, механізмів моніторингу та наслідків невиконання встановлених зобов'язань, виникає ризик фінансування розробок, які не досягнуть визначеного рівня технологічної готовності або не відповідатимуть потребам сил оборони.

Отже, для мінімізації зазначених ризиків важливо забезпечити нормативну визначеність критеріїв відбору інноваційних проєктів, процедур ухвалення рішень про фінансування, механізмів обліку та перевірки розробок, а також контролю за цільовим використанням коштів і досягненням передбачених результатів. Водночас відсутність обов'язкової державної реєстрації сама по собі не свідчить про неналежність механізму фінансування, якщо законодавством передбачено дієві альтернативні інструменти обліку, оцінювання та контролю.

Існує й ризик інституційної монополізації оборонних інновацій та знищення успішної моделі децентралізованого ринку оборонних технологій. Так, у положеннях законопроєкту передбачається внесення доповнення до статті 10 Закону України «Про оборону України», у якому пропонується надати Міністерству оборони України повноваження щодо створення у його структурі спеціального уповноваженого органу або визначення структурного підрозділу, безпосередньо підпорядкованого органу військового управління або установу чи суб'єкта господарювання, що належить до його сфери управління, який матиме статус інноваційного органу Міністерства оборони України та реалізуватиме державну інноваційну політику у сфері оборони. За таких умов створення нового спеціального інноваційного органу в структурі Міністерства оборони України призведе до монополізації галузі, оскільки цей орган (підрозділ) самостійно та одноосібно координуватиме та відбиратиме перспективні інноваційні розробки. Надання Міністерству оборони України одноосібного права створювати підконтрольний інноваційний орган із повним циклом повноважень (від добору до координації) прямо загрожує горизонтальним зв'язкам, які є основою українського технологічного прориву. Це може призвести до надмірної концентрації повноважень в одній структурі та вірогідно уповільнити темпи інновацій, знизити мотивацію у незалежних інженерних команд працювати з державою. Замість того, щоб діяти за зразком Агентства передових оборонних дослідницьких проєктів США (DARPA),[2] де рішення приймаються колегіально із залученням незалежної наукової та військової спільноти, запропонована модель формує ризик побудови жорсткої вертикальної монополії, що своєю

[2] Defense Advanced Research Projects Agency (DARPA). URL: https://www.darpa.mil

чергою суперечить пріоритетам життєдіяльності вітчизняного сектору оборонних технологій, який досяг колосального успіху саме завдяки своїй децентралізації, адаптивності та налагодженим горизонтальним зв'язкам.

Запровадження механізмів прискореного випробування оборонних інновацій та спрощення обміну інформацією між державними інституціями й приватними розробниками потребує належного нормативного забезпечення захисту інформації. За відсутності чітких вимог до організації такого обміну, розмежування доступу та захисту інформаційних систем може виникнути ризик несанкціонованого доступу до технічної документації, програмного забезпечення, результатів випробувань та інших відомостей про новітні оборонні розробки.

Особливого значення це питання набуває під час випробувань у бойових умовах, коли оперативне доопрацювання технологічних рішень передбачає обмін інформацією між військовослужбовцями та цивільними інженерами. Недостатній рівень захищеності каналів зв'язку, інформаційних систем і засобів зберігання даних може створювати передумови для витоку відомостей про технічні характеристики розробок, виявлені вразливості, особливості їх застосування та результати тестування. Такі відомості можуть становити інтерес для розвідувальних і кібернетичних підрозділів противника.

Додаткові ризики пов'язані з можливим захопленням або втратою дослідних зразків безпілотних систем та інших технічних засобів. Якщо прототипи не матимуть належних механізмів захисту даних, зокрема криптографічного захисту інформації, контролю доступу та безпечного зберігання програмного забезпечення, це може створювати умови для отримання сторонніми особами доступу до технічних даних і програмних компонентів розробки.

Тому особливої уваги потребує нормативне визначення вимог до захищених каналів обміну інформацією, розмежування прав доступу, фіксації дій користувачів, захисту технічної документації та програмного забезпечення, а також перевірки спроможності розробників дотримуватися встановлених вимог безпеки. Водночас такі вимоги мають бути диференційовані залежно від категорії інформації, рівня ризику та характеру інноваційного проєкту. Це дасть змогу поєднати оперативність випробувань із необхідним рівнем захисту відомостей, розголошення яких може негативно вплинути на обороноздатність держави.

Слід зазначити, що у державах Європейського Союзу регуляторна політика у сфері оборонних інновацій базується на принципах прозорої конкуренції, децентралізації та державно-приватного партнерства, де держава виступає замовником, а не монополістом-розпорядником. Європейська модель у цій сфері консолідовано об'єднує державу, бізнес-структури та наукову спільноту, а впровадження такого підходу в Україні є критично важливим для інтеграції вітчизняного сектору оборонних технологій у європейський та євроатлантичний простір. У європейських державах цей баланс інтересів та

недопущення монополізму забезпечуються завдяки чіткому розподілу ролей між державою та приватним оборонним сектором.

У Європейському оборонному агентстві[3] (EDA) функціонує Хаб оборонних інновацій (HEDI 2.0)[4], який не підпорядковує собі розробників оборонних технологій та інновацій, а діє виключно як координатор усієї оборонної екосистеми. Застосування європейського передового регуляторного досвіду у цій площині передбачає: наявність прозорої конкуренції, оскільки саме через Європейський оборонний фонд фінансування виділяється за прозорими процедурами, де критерії оцінки визначені заздалегідь, що у свою чергу нівелює ризик «ручного» розподілу коштів без обов'язкової реєстрації; наявність децентралізації, що передбачає проведення оцінки проєктів саме незалежними експертними комісіями, а не уповноваженим державним органом в особі Міністерства оборони України, оскільки держава лише координує процес з метою стимулювання малих та середніх приватних розробників і активно залучає інвесторів, гарантує викуп оборонних технологій на умовах контракту, якщо вони відповідають встановленим критеріям та вимогам, але не втручається у внутрішні процеси розробників і гарантує суворий захист конфіденційної інформації у спільних цифрових ІТ-системах.

Зокрема у цьому контексті показовим залишається досвід Німеччини, де продемонстровано суцільну децентралізацію: оцінку та сертифікацію проводять незалежні науково-дослідницькі інституції наприклад, Fraunhofer[5], а не військовослужбовці чи державні службовці Міноборони. Досвід Німеччини є класичним прикладом того, як передача експертних функцій цивільному науковому сектору дозволяє уникнути корупції та заангажованості. Інститути товариства Fraunhofer (зокрема ті, що спеціалізуються на оборонних дослідженнях, як-от *Fraunhofer VVS*) виступають в ролі незалежного арбітра та оцінюють реальну технологічну готовність й кіберзахищеність розробки ще до того, як вона потрапить на розгляд до керівництва Бундесверу або Федерального відомства із озброєння (BAAINBw).

У сучасних реаліях під час війни базовий принцип децентралізації варто впровадити через наступні кроки: залучення вітчизняних наукових та ІТ-інституцій, що передбачає проведення ними оцінки програмного забезпечення, алгоритмів та технологій штучного інтелекту для БПЛА чи систем кодування РЕБ за участю незалежних експертів, із залученням наукової спільноти, представників закладів вищої освіти, провідних українських ІТ-кластерів та сертифікованих лабораторій із кібербезпеки.

У контексті опанування та імплементації кращих європейських практик щодо мінімізації ризиків витоку конфіденційних даних, слід вказати на позитивний французький досвід у цій площині. Французьке агентство оборонних

[3] European Defence Agency (EDA). URL: https://eda.europa.eu
[4] Hub for EU Defence Innovation (HEDI). URL: https://eda.europa.eu/what-we-do/research-technology/hedi
[5]Fraunhofer. URL: https://www.emft.fraunhofer.de/?gad_source=1&gad_campaignid=24257308688&gbraid=0AAAAA-1LqfsOkScPTl_T3Dy3oEjMvGNU_&gclid=EAIaIQobChMI9ejJjIm8lwMVamWRBR0

інновацій[6] дозволяє приватним компаніям тестувати оборонну продукцію та інноваційні зразки зброї, але одночасно зобов'язує їх виконувати підвищені вимоги у сфері гарантування кібербезпеки, у зв'язку з чим вони розробляють відповідне програмне забезпечення виключно у захищеному хмарному середовищі, що адмініструється державою. Завдяки перенесенню процесів розробки в контрольоване державою середовище, Агентство оборонних інновацій Франції вирішує низку особливо стратегічно важливих завдань. Так, усі комерційні розробники програмного забезпечення, які отримують фінансування чи допуск до тестування зразків зброї, зобов'язані зберігати документацію виключно у захищеній державній хмарі. У Франції запроваджено ізольований контур тестування, що передбачає передачу даних під час випробувань, яка кодується за військовими стандартами і відразу потрапляє до захищеного реєстру. Зберігання інформації у хмарах, які адмініструються державою, автоматично фіксує авторство кожної стрічки коду та будь-яку зміну, внесену приватним розробником. Такий підхід захищає від несанкціонованого копіювання розробок як результатів інтелектуальної власності з боку державних службовців, військовослужбовців. Французька модель, яка отримала назву «регуляторної пісочниці» (Regulatory Sandbox) у захищеній хмарі є ідеальним паритетним балансом, який дозволяє не гальмувати оборонні інновації бюрократією, але повністю перекриває канали та можливості для будь-якого ворожого шпигунства з метою отримання доступу до секретної інформації. Французький підхід переконливо доводить, що держава не повинна забороняти чи обмежувати приватних розробників, проте має створити для них безпечний цифровий ландшафт, який сприятиме швидкому створенню оборонних технологій без загрози несанкціонованого витоку державних секретів. Впровадження французької концепції в Україні є критично важливим для захисту вітчизняного ІТ-контуру від постійних кібератак з боку російських хакерських угруповань або російських спецслужб.

Для мінімізації безпекових ризиків, у контексті представленого законопроєкту, необхідним є запровадження сучасних механізмів спрощеного обміну інформацією між державою та приватним оборонним сектором із дотриманням балансу між оперативністю передачі даних та заходами у сфері охороною державної таємниці. По-перше, це спільний запуск за участю Міністерства оборони України та Міністерства цифрової трансформації України Єдиної національної платформи оборонних технологій, яка функціонує як захищений віртуальний простір на базі технологічної інфраструктури бойової екосистеми «Delta». По-друге, допуск приватних розробників до швидких випробувань на полі бою або надання їм грантової підтримки має здійснюватися виключно за умови проходження ними кібер-комплаєнсу шляхом обов'язкового підключення до захищеного контуру Платформи під державним контролем. Водночас обов'язковий обмін інформацією через це хмарне середовище має застосовуватися виключно на етапах серійного виробництва та допуску до

[6] Agence de l'innovation de défense (AID). URL: https://www.defense.gouv.fr/aid

експлуатації. На етапах проведення досліджень, розробки (R&D) та первинних випробувань стартапам дозволяється використовувати сертифіковані комерційні захищені хмарні сховища.

Висновки

Представлений законопроєкт є актуальним та прогресивним, адже має спрямованість на реформування сфери оборонних інновацій, створення передумов задля максимального залучення приватного оборонного сектору для розробки новітніх оборонних технологій в умовах правового режиму воєнного стану.

Defense Tech – екосистема в Україні – є ключовим елементом національної безпеки, а для її збереження та динамічного розвитку необхідно підтримувати баланс між двома важливими факторами: децентралізацією (яка забезпечує гнучкість, живучість та швидкість інновацій) та державним регулюванням (яке гарантує безпеку даних, нерозповсюдження технологій та координацію зусиль).

З урахуванням необхідності збереження децентралізованої Defense Tech екосистеми, ефективного використання бюджетних коштів, у законопроєкті доцільно урахувати пропозиції щодо антикорупційних, інституційних та контррозвідувальних запобіжників, наведені в Таблиці 1.

Таблиця 1

№ з/п	Категорія ризику	Ключова вразливість	Запропоновані запобіжники
1.	Антикорупційний	Фінансування без здійснення державної реєстрації; «ручний» розподіл грантів, дублювання розробок у різних структурах; відсутність відповідальності за кінцевий результат	Розподіл фінансування на транші за етапами із запровадженням жорсткої прив'язки до створення діючого бойового зразка, ретельний аудит здійснення фінансування кожного проєкту
2.	Інституційний	Створення органу або підрозділу в структурі Міністерства оборони України, який на власний розсуд відбирає та координує розробки, руйнуючи горизонтальну екосистему та закладений принцип децентралізації	Перехід до колегіальної моделі управління шляхом створення Наглядової ради в структурі Міністерства оборони України із залученням незалежних експертів та науковців, IT-спільноти та представників бойових бригад (кінцевих споживачів)
3	Контррозвідувальний	Потенційний витік конфіденційної інформації, зокрема характеристик та специфікацій новітніх розробок зброї завдяки використанню ПК та звичайних	Запуск Єдиної національної платформи оборонних технологій як захищеного простору на базі інфраструктури бойової екосистеми

		месенджерів стартапами, перехоплення частот/телеметрії ворогом за допомогою РЕР під час швидких тестів на лінії бойового зіткнення	«Delta», запровадження обміну технічною документацією виключно через захищений контур державної хмари (Military-grade Cloud), обов'язкове криптографічне шифрування даних на самих прототипах (бортових носіях РЕБ, БПЛА та роботизованих комплексів), інтеграція алгоритмів автоматичного знищення польотних логів для запобігання витоку інформації у випадку їх втрати чи захоплення ворогом

Дослідницька служба
Верховної Ради України

** Цей документ підготовлений Дослідницькою службою Верховної Ради України як довідковий інформаційно-аналітичний матеріал. Інформація та позиції, викладені у документі, не є офіційною позицією Верховної Ради України, її органів або посадових осіб. Цей документ може бути цитований, відтворений та перекладений для некомерційних цілей за умови відповідного посилання на джерело.*