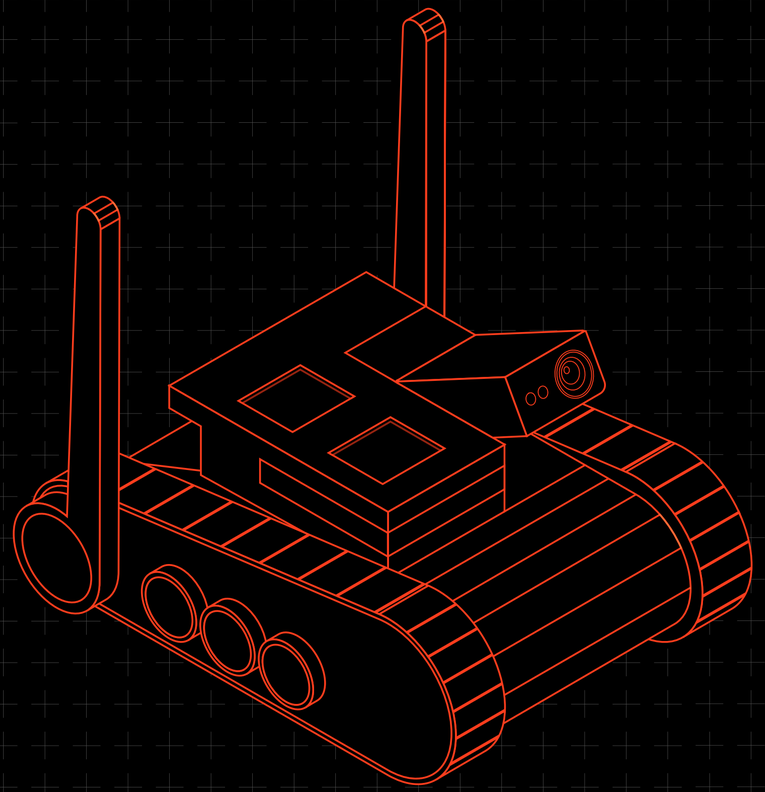
10 РОКІВ УКРАЇНСЬКОГО DEFENSE TECH



Великий огляд ринку
оборонних технологій
України

Інженери, технології, зброя, IT-рішення — український Defense Tech, або ж сектор оборонних технологій, з 2014 року став одним з визначальних факторів оборони України.

За підтримки:

BRDO
Офіс ефективного регулювання

BRDO — незалежний аналітичний центр із командою понад 100 експертів, які працюють у сферах економіки, права, публічного управління, галузевого регулювання та оборонної політики. BRDO створює цифрові рішення для держави, бере участь у розробці реформ і допомагає впроваджувати прозорі правила — від розвитку підприємництва до зміцнення обороноздатності.

В умовах нерівного кількісного протистояння українців з російським агресором саме інженерний талант і технологічна перевага, разом з відвагою українських воїнів на полі бою, є важливим драйвером не тільки військових операцій, а й економіки.

Уже зараз деякі наші співрозмовники називають сектор оборонних технологій new black, а український бізнес, який всіма можливими засобами підтримує армію, у повоєнній Україні зможе засвоїти та імплементувати талановиті розробки інженерів і конструкторів воєнного часу.

Цей огляд присвячується їм — українським героям-оборонцям, які тримають фронт, і всім представникам оборонного сектору, що постачає «крила», тепловізори, РЕБи, цифрові продукти, системи ситуаційної розвідки, роботизовані комплекси та інші інновації захисникам.

Також вся команда AIN дякує Офісу ефективного регулювання BRDO і його Сектору «Оборонна політика», які систематично підтримують розробку цифрових рішень для війська. Цей огляд став можливим завдяки вашій всебічній допомозі.

МЕТОДОЛОГІЯ

До огляду потрапила українська сфера оборонних технологій та її розвиток з 2014-го — року початку війни росії проти України. До українських компаній ми зарахували ті, які були створені в Україні, мають центри розробки в Україні або їх створили українці.

В огляді беремо фокус на приватні компанії у сфері Defense Tech, до яких ми відносимо:

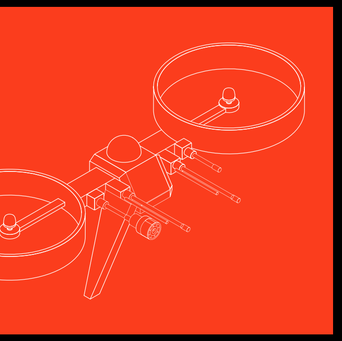
- розробки нової хвилі, зокрема дрони, програмі рішення, навчальні інструменти;
- також стартапи, які працюють у сфері гуманітарного розмінування, протезування та застосунків для військових і ветеранів.

У межах огляду ми аналізуємо і державну сферу оборонних технологій — заводи, конструкторські бюро тощо, які націлені на hardware і виробляють зброю і техніку — для ширшої картини розуміння оборонної сфери.

Під час роботи над розділом про екосистему українських Defense Tech розробок фактчекінг і консультування проводили керівний партнер Angel One Venture Fund Іван Петренко та співзасновник й голова ГО «Аеророзвідка» Ярослав Гончар. Редакція вдячна за цю допомогу.

Під час проведення огляду щодо російської галузі Defense Tech ми використовували як публічні дані, так і дані, що стали публічними унаслідок витоків і соціальної інженерії. Концептуальне спрямування цього огляду спирається на інтерв'ю з експертами, а також вивчення академічної і публіцистичної літератури щодо функціонування російських владних структур і промисловості. Усі твердження, наявні в цій публікації, були підтверджені кількома джерелами, якщо така можливість існувала. Водночас ці твердження є аналізом ворожого середовища, тож не можуть розглядатися як істинні.

Команда AIN свідома того, що огляд не є вичерпним через сенситивність певної інформації під час воєнного стану.

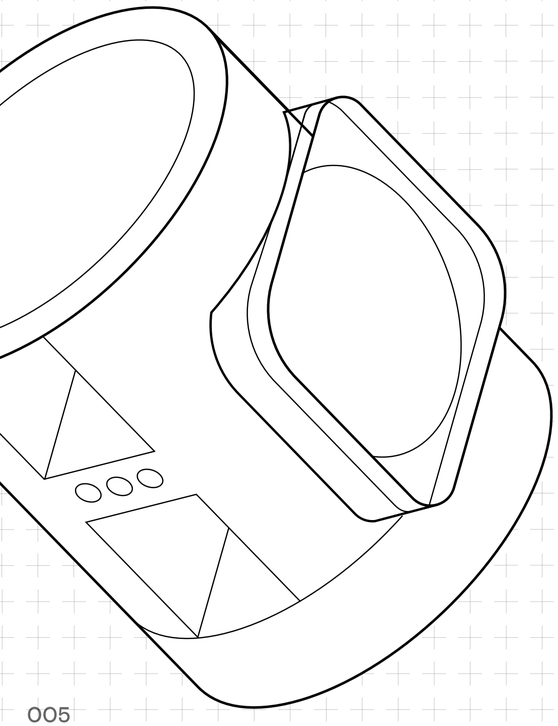


ЗМІСТ

005 Стан оборонної сфери та оборонних технологій в Україні в 2014 році
019 Загальний огляд екосистеми
029 Рейтинг Defense Tech компаній
053 Від знезброєння до стандартів НАТО: як цифровізували галузь
083 Порівняння українського Defense Tech з іноземним
096 Реалії та поточні проблеми сфери
122 Розмова з військовими
149 Робота держави у сфері: регулювання, розробки, закупівлі
157 Штучний інтелект у Defense Tech сфері
167 Кібербезпека і її роль у повоєнній Україні
177 Російський Defense Tech
196 Лабораторії в університетах
212 Ринок праці в українському Defense Tech
222 Як Defense Tech технології змінять цивільні бізнеси
232 Перспективи Defense Tech після закінчення війни

ПОЧАТОК ВІЙНИ РОСІЇ ПРОТИ УКРАЇНИ У 2014 РОЦІ: ЯКИЙ СТАН ОБОРОННОЇ СФЕРИ ТА ОБОРОННИХ ТЕХНОЛОГІЙ МИ МАЛИ

ТОРУВАТИ ШЛЯХ: ПЕРШИЙ РОЗДІЛ З ІСТОРІЇ УКРАЇНСЬКОГО DEFENSE TECH



«А що робити з тисячами кілометрів кордону та підготовкою росії до вторгнення? Коли зайдуть зранку з боку Чернігівської області, то до вечора вже у Києві будуть!». Так станом на 28 лютого 2014 року оцінював українську обороноздатність виконувач обов'язків міністра оборони України Ігор Тенюх.

Ми не знаємо, чи мав Тенюх рацію, проте точно мав підстави так вважати. Виконувач обов'язків міністра прослужив в українській армії у 1991-2010 роках і володів інформацією щодо її становища. І хоч на той час російське військо не було найбільш технологічним у світі, проте фактично з травня 2014 року над Донеччиною літали російські БпЛА «Орлан-10», у листопаді того ж року в тимчасово окупованому Донецьку був розгорнутий комплекс радіоелектронної боротьби 1РЛ257 «Красуха-4», а у січні 2015 року росіяни коригували вогонь по Маріуполю, застосовуючи радіостанції супутникового зв'язку Р-438 «Бєлозєр».

Саме технологічне відставання України від ворога на той момент стало поштовхом до розвитку оборонних технологій і запустило перший етап формування української Defense Tech екосистеми.

■ Початок війни росії проти України у 2014 році

У НЕБІ: З УНІВЕРСИТЕТУ НА ФРОНТ

Чи були в українському війську безпілотники до початку російського вторгнення? Так, були, застарілі радянські розвідувальні Ту-143. Публічно відомо про один пуск такого засобу восени 2014 року. Крім того, на зберіганні перебували Ту-141, які в радянський час вироблялися на Харківському авіаційному заводі. Проте їхній час слави настав уже після початку повномасштабного вторгнення, коли розвідувальні Ту-141 було модифіковано для завдання ударів по цілях на відстані понад 500 кілометрів.

Розробки безпілотників велися в університетах УРСР щонайменше з 1970-х років. Наприклад, група студентів одного з них у 1988 році створила «радіокерований літак», який міг перебувати в повітрі з двома кілограмами корисного навантаження протягом 30 хвилин на відстані до одного кілометра.

Після відновлення незалежності така діяльність тривала надалі. Особливої активності вона набула орієнтовно з 2008 року — після створення Науково-виробничого центр безпілотної авіації в тодішньому НАУ (зараз Київський авіаційний інститут, КАІ).

Тож не дивно, що, коли влітку 2014 року благодійний фонд «Крила Фенікса» закуповував безпілотники для новосформованого 3-го десантно-штурмового батальйону 79-ї окремої аеромобільної бригади, вибір припав на виріб саме одного з українських університетів. Фонд придбав і передав коптер, а військовослужбовці батальйону пройшли навчання в цьому університеті. Серед них був Олександр Грачов.

«Перше застосування цих безпілотників було на Чонгарському півострові, — розповідає він AIN. — Безпілотник мав гарну, як на той час, цифрову камеру, тому ми його періодично застосовували для спостереження за діями росіян». Згодом, під дією російських засобів РЕБ, дрон впав, після чого військовослужбовці повернули його на ремонт. Другий екземпляр цієї моделі Грачов отримав вже під час оборони Донецького аеропорту. Ці два борти досі існують і зберігаються бригадою.

Здавалося б, ці вироби продемонстрували, як на той час, непогані результати. Чому ж тоді розробнику не вдалося масштабувати виробництво?

■ Початок війни росії проти України у 2014 році

«Не вистачало грошей для закупівель, адже тоді ці безпілотники коштували досить багато. Можливо, розробникам не вистачило підприємницького хисту. Зрештою, це була державна установа, а держава загалом не дуже гарно справляється з розвитком інновацій, це просто її властивість»,

— ділиться думкою Неллі Стельмах, у 2014 році керівниця закупівель фонду «Крила Фенікса».

Зараз Стельмах продовжує закуповувати безпілотники, проте вже як військовослужбовиця 241-ї бригади територіальної оборони.

У НЕБІ: З АЕРОМОДЕЛЬНОГО СПОРТУ В НІГЕРІЮ

Таких закладів вищої освіти, які розробляли безпілотники, тоді була ціла низка. У 2014 році, після початку війни, їхні представники були присутні на нараді в Укроборонпромі, де презентували свої вироби.

Один з офіцерів Центрального науково-дослідного інституту озброєння та військової техніки ЗСУ так відреагував на ці презентації: «Скільки ми вас не запрошуємо на випробування, ніхто не приїздить». На той час він просто цікавився аеромодельним спортом і зі своїми майбутніми партнерами «час від часу зустрічався на полі, де літали на радіокерованих літачках», — зауважує він у розмові з AIN.

У цього кола друзів було бажання «допомогти своїй країні», розробивши безпілотник, який уже зараз буде готовий до виконання завдань на фронті. Тому швидко склали виріб і представили його.

«Ми отримали цілий звіт, військові печатки на ньому, підписи уповноважених офіцерів. Це нас вразило. Умовно кажучи, ми вчора грали з літачками, а сьогодні вже можемо виконувати бойові задачі», — пригадує В'юнник.

Цей виріб отримав назву «Фурія», який відтоді пройшов численні модифікації, проте і досі літає в небі Сходу України. Але не лише там. До початку повномасштабного вторгнення безпілотниками «Атлон Авіа» цікавилися в Королівстві Саудівська Аравія та в Нігерії. Після початку повномасштабного вторгнення до них «доєдналася вся Європа і навіть США». До того ж компанія зацікавлена не лише в експорті, а й в партнерствах з іноземними підприємствами, аби «об'єднуватися, створювати рішення разом, і виходити на нові ринки».

Напрям міжнародних партнерств — один із трьох, що разом складають стратегію компанії на випадок зменшення інтенсивності бойових дій. В'юнник переконаний, що навіть за таких умов українське військо закуповуватиме безпілотник «Атлон Авіа», адже вони «вже інтегровані у військову доктрину».

Водночас компанія хоче залишатися гнучкою, щоб перебувати в діалозі з державою та військом і відповідати новим викликам. Крім того, «Атлон Авіа» розглядає також і цивільні ринки для своїх дронів.

■ Початок війни росії проти України у 2014 році

У НЕБІ: ВІД КЛУБУ ЗА ІНТЕРЕСАМИ ДО ЦЕНТРУ КОМПЕТЕНЦІЙ

«Крила Феніксу» та «Атлон Авіа» — не єдині команди, які інвестували в безпілотники українського виробництва влітку 2014 року. Однією з найвідоміших є «Аеророзвідка», яку заснували загиблий навесні 2015 року Володимир Кочетков-Сукач, а також Натан Хазін, Дмитро Лісенбарт і Ярослав Гончар. Їхній шлях до українського дрона розпочався з модифікацій китайського.

«Одного разу Натан Хазін привіз дрон DJI Phantom 1. Це була ще геть нова модель, іграшкового рівня, з обмеженим радіусом польоту близько 500 метрів. Але ми побачили в ній потенціал, тож почали з модифікацій. Допомогу отримали від Комп'ютерної академії «ШАГ» в Києві. Її керівник Іван Довгаль разом із колегами допоміг створити перші підсилювачі сигналу — антени-бустери, які суттєво збільшили дальність польоту. Ми одразу почали тестувати ці рішення в зоні бойових дій — літали від підрозділу до підрозділу, показували їм відео, фото, допомагали орієнтуватися», — пригадує співзасновник «Аеророзвідки» Ярослав Гончар.

Завдяки цим експериментам ще до боїв за Іловайськ у 2014 році стало зрозуміло, що безпілотник цілком може бути інструментом розвідки. А як щодо ураження супротивника? Ідея розробити механізм скиду для дронів цивільного призначення виникла доволі випадково. З одного боку, «Аеророзвідка» експериментувала з транспортуванням вантажу. З другого — у Phantom був вбудований ліхтарик, заживлений від 5-вольтного елемента. Ліхтарик як такий потрібним не був, а от його живлення можна було би використати в інших цілях. Так засновники «Аеророзвідки» дійшли думки, що дрон може не лише нести вантаж, а і використовувати сервомеханізм для його скидання.

«Тоді це виглядало як хобі «клубу за інтересами», проте саме з таких експериментів і почалась технологічна еволюція українських БПЛА», — говорить голова організації Гончар.

■ Початок війни росії проти України у 2014 році

У НЕБІ: ВІД КЛУБУ ЗА ІНТЕРЕСАМИ ДО ЦЕНТРУ КОМПЕТЕНЦІЙ

Зараз «Аеророзвідка» продовжує бути каталізатором змін, проте робить це вже на системному рівні.

Так, у структурі НАТО існують центри компетенції, які діють за принципом «досвід не вважається засвоєним, якщо не відбулося змін» і працюють як міжнародні платформи з постійною ротацією фахівців з країн-членів. Тож «Аеророзвідка» запропонувала Міністерству оборони створити такий центр на національному рівні, проте в межах процесів євроатлантичної інтеграції. І на саміті НАТО у Вільнюсі в 2023 році Україна оголосила про прагнення створити центр компетенції роботизованих систем. Наразі команда «Аеророзвідки» працює над тим, аби отримати сертифікацію НАТО.

«Навіть за умов тимчасового перемир'я Україна повинна мати повні склади зброї, достатній запас безпілотників, перевірені рішення та систему навчання фахівців, які готові швидко діяти в разі ескалації», — говорить Ярослав Гончар.

У такому разі роль «Аеророзвідки» полягатиме в тому, щоб переконатися, що підготовка запасу засобів відбувалася не за принципом «затаритися всім», а враховувала накопичений досвід і потенціал технологій.

■ Початок війни росії проти України у 2014 році

У НЕБІ: ВІД ВОЛОНТЕРСТВА ДО ВИРОБНИЦТВА

Влітку 2014 року DJI Phantom можна було зустріти не лише у співзасновників «Аеророзвідки». Тоді ж про цей безпілотник дізнався Дмитро Ковальчук. Він привіз 30-й окремій механізованій бригаді бронежилети та їжу: такі на той час були потреби. Ковальчук переказує розмову, яка в нього відбулася на Луганщині із заступником командира бригади Сергієм Заболотним:

— Що вам ще треба? Чим допомогти?
— Привези нам коптерів, безпілотників.
— Що це таке?
— Погуглиш.

Ковальчук погуглив — і відтоді назавжди з безпілотниками. Спершу привіз цій бригаді Phantom. «Підняли ми цей безпілотник у військовій частині, політали на ньому на відстань до 400 метрів, щастя в усіх було таке, що словами не передати», — пригадує він.

Проте безпілотники коптерного типу мали обмеження щодо подальшого розвитку. Ковальчук вклав $15 000 у більший гексокоптер, проте цей борт було втрачено під час операцій під Луганським.

Рішення для цієї проблеми знайшли згодом, коли Ковальчук приєднався до благодійної організації Армія SOS, де познайомився з колишнім директором Одеського зоопарку та любителем безпілотників Юрієм Кучеренком.

«Ваші коптери — це не те, що нам треба. Нам потрібно літати на літаках», — пригадує Ковальчук його слова і каже, що тоді це важко було уявити. Проте Кучеренко привіз власний безпілотник літакового типу з пінопласту, тож Армія SOS почала застосовувати його. «Ми застосовували його і над Донецьким аеропортом, і під час деблокування Дебальцевого», — пригадує Ковальчук.

■ Початок війни росії проти України у 2014 році

Проте не лише Кучеренко передавав свій літак. До Армії SOS приходили й інші волонтери з інтересом до безпілотників і передавали власні дрони, тому «зоопарк» засобів зростав. У результаті, в розпорядженні Ковальчука наприкінці 2014 року було понад 20 типів різних дронів.

Такий асортимент призводив до невиправдано великих витрат на навчання, адже пілот мусив вміти пілотувати велику кількість дронів. Це підштовхнуло Армію SOS до розробки власного БпЛА.

Волонтери організації надихнулися «літаючим крилом» розробки французької компанії Lehmann Aviation і у 2015 році створили перші прототипи безпілотника «Валькірія». Відтоді польотні групи Армії SOS використовували цей БпЛА на Сході, а наприкінці 2017 року Міністерство оборони України допустило безпілотник до експлуатації.

Коли розпочалося повномасштабне вторгнення, Ковальчук повернувся в Україну з Іспанії і відновив свою роботу у складі польотної групи. Так опинився під Вугледаром, де проводив аеророзвідку для 53-ї окремої механізованої бригади. Проте до нього почали звертатися й суміжні підрозділи. Він переказує свою розмову з військовослужбовцями 55-ї окремої артилерійської бригади так:

— Що відбувається?
— Зараз більше ніхто не літає, всіх позбивали, всіх. Ти один лишився.
— Такого бути не може.
— Росіяни знищують борти швидше, ніж нам їх постачають.

Через це Ковальчук порадився з іншими членами Армії SOS та отримав від них дозвіл на масштабування виробництва «Валькірій» за умови, що усі групи організації будуть забезпечені літаками, а ремонт для військових здійснюватиметься безоплатно до кінця війни. Так виникла компанія «Бойові птахи України», а Ковальчук став її співзасновником. Тоді ж, у 2022 році, вдалося масштабувати виробництво з трьох літаків у місяць до 100.

■ Початок війни росії проти України у 2014 році

Зараз «Бойові птахи» виробляють не лише «Валькірії», а доволі широкий перелік різних типів безпілотників. Цьому сприяє те, що держава суттєво пришвидшила процедури випробування, кодифікації та отримання допуску до експлуатації.

«Це просто небо і земля порівняно з тим, як це було у 2017–2018 роках», — порівнює співзасновник «Бойових птахів». Крім того, розширення асортименту спричинене і зміною пріоритетів у постачанні, які держава й армія комунікують, змінюючи кількість коштів на закупівлю засобів того чи іншого призначення.

Як працюватимуть «Бойові птахи» за умови зменшення інтенсивності бойових дій? Замість масштабування компанія сфокусується на ефективності та диверсифікації. Ковальчук переконаний, що деякі види безпілотників закуповуватимуться і надалі. Крім того, виникне можливість працювати над довгостроковими високотехнологічними проєктами, які дозволять компанії зберігати персонал, випускаючи меншу кількість засобів.

Що ж стосується експорту військових технологій за кордон, то тут Ковальчук бачить доволі змішану перспективу. Він переконаний, що всі держави зацікавлені в локалізації виробництва безпілотників. Вони купують іноземну продукцію невеликими партіями, аби вивчити її та спробувати створити на цій основі власні вироби. Водночас невеликий ринок все ж є.

«Це невеликі країни на європейському континенті, у яких є потреба терміново закрити нішу безпілотників, проте немає власних виробників такого рівня спроможностей», — підсумовує Ковальчук.

НА ЗЕМЛІ: ВІД ПЛАНІВ ЕМІГРАЦІЙНИХ ДО ПЛАНІВ ЕКСПОРТНИХ

Експертиза СРСР у сфері радіоелектронної розвідки та радіоелектронної боротьби виникла з низки причин. По-перше, інвестиції в засоби радіоелектронного придушення були спричинені запуском західними країнами на початку Холодної війни так званих «голосів», тобто спрямованих на радянське населення радіостанцій. По-друге, радянські військові вивчали досвід застосування захід радіоелектронних засобів під час воєн на Близькому Сході та в Південно-Східній Азії. По-третє, ці засоби формувалися також як підготовка до майбутньої війни проти армій країн-членів НАТО, які мали лідерство у високотехнологічній і залежній від радіосигналів зброї. Тож Україна успадкувала низку підприємств у Донецьку, Харкові, Запоріжжі та Києві, які розробляли такі засоби. Найвідоміших серед них був завод «Топаз» у Донецьку, який створив станцію РЕР «Кольчуга».

У неспеціалізованому середовищі найбільше цей виріб асоціюється з «касетним скандалом» Леоніда Кучми. У 2002 році стало відомо, що у 2000 році між президентом країни і керівником «Укрспецекспорту» Валерієм Малєвим відбулася розмова про таємне постачання в Ірак чотирьох станцій «Кольчуга», яке президент начебто погодив. Це би порушило санкції ООН, запроваджені після вторгнення Іраку в Кувейт. Доказів того, що «Кольчуги» дійсно потрапили в Ірак, не існує.

Ця історія демонструє одну характерну рису радіоелектронного сектору до 2014 року — залежність від експорту. Після початку російсько-української війни ситуацію додатково ускладнило і те, що підприємства Донецька були окуповані.

«Саме там вироблялися засоби ультракороткохвильового діапазону, які найбільше потрібні на війні», — говорить Ярослав Калінін, директор компанії «Інфозахист».

На той час Калінін ще не працював в «Інфозахисті». До 2012 року він перебував у складі Служби зовнішньої розвідки України. Умови роботи були прийнятні, керівництво відзначало його здобутки, проте «на той час не було матеріальних засобів для реалізації тих ідей, які я мав».

■ Початок війни росії проти України у 2014 році

Тож після завершення контракту він полишив службу, заснував власну компанію і паралельно працював розробником в DataArt. У 2013 році, як і чимало інших технічних спеціалістів, думав про переїзд у США. «Компанія 3–4 рази подавала мене на візу для висококваліфікованих фахівців H1B, проте отримати не вдалося», — пригадує керівник «Інфозахисту».

До того ж у 2015 році Калінін відвідав передові позиції українського війська на Сході і вирішив, що хоче і далі будувати своє життя в Україні. Він все ще мріяв втілити проєкт, який не вдалося реалізувати у Службі зовнішньої розвідки. Із цією метою Калінін приєднався до «Інфозахисту».

На той час насиченість лінії фронту засобами РЕР була вкрай низька. «Радянські або вийшли з ладу, або не давали жодного результату», — пригадує Калінін і відзначає, що ефективним було лише імпортне обладнання. Тут «Інфозахист» побачив нішу — локалізація малого пеленгатора, подібного за своїм форм-фактором до станції PUHU турецької компанії Aselsan, яка також розвинулася внаслідок необхідності локалізувати виробництво військового обладнання через ембарго США на постачання зброї в Туреччину. Наприкінці 2016 року «Інфозахист» випустив за державним оборонним замовленням першу партію цих пеленгаторів, що отримала назву «Пластун».

Відтоді змінився не лише асортимент товарів «Інфозахисту», трансформувалися також і спілкування між державою, військом і виробниками.

«Суттєво збільшилася якість комунікації з Генеральними штабом, з Міністерством оборони, з окремими довольчими органами, як-от Головне управління розвідки чи Національна гвардія, — говорить Калінін, проте відразу уточнює, що має на увазі. — ***Якість — це відповідність очікуванням, отже вдалося скоротити цей інтервал між очікуваннями та результатами»,*** — пояснює він.

Інакше він дивиться на те, як після початку повномасштабного вторгнення відбуваються процедури випробування, кодифікації, допуску до експлуатації. Калінін, так само, як і Артем В'юнник, переконаний, що складність цих процесів необхідна для забезпечення якості. «Не завжди швидкість означає якість», — говорить Калінін і наводить приклад: якщо уважно не протестувати засіб на вібростійкість, то він розпадеться на частини вже під час застосування у військах. У результаті першими до закупівельного фінішу можуть приходити не ті виробники, які вклалися в якість, а ті, які фокусувалися на нижчій ціні та більшій швидкості.

■ Початок війни росії проти України у 2014 році

Співрозмовник редакції також обережно ставиться до експортного майбутнього української Defense Tech галузі, оскільки вже проходив цей шлях до 2022 року. «До повномасштабного вторгнення ми якраз таки виходили на фінішну пряму щодо постачання наших виробів низці іноземних країн», — пригадує він і відразу наголошує на трьох ключових складностях.

Передусім в інших країнах відмінні уявлення про те, якою буде наступна війна. «Уявлення замовника про поле бою складається на основі локальних особливостей, культури та багатьох інших факторів», — говорить Калінін. Ці фактори треба вивчати, щоб розуміти, якою може бути тактика застосування виробу.

Крім того, кожна країна має свій специфічний цикл бюджетування. Угода про закупівлю має бути підписана до конкретної дати, а це означає, що до цієї дати мають бути завершені усі випробування, інакше доведеться чекати рік до наступної можливості контрактування. «У кращому випадку ти розумієш, як цей цикл працює і можеш під нього підлаштуватися», — пояснює очільник «Інфозахисту».

Зрештою, умови випробування можуть цілком відрізнятися від українських. Калінін пригадує ситуацію, коли під час випробування в іншій країні виріб «Інфозахисту» виявився не призвичаєним до місцевих стандартів стійкості до температури. «За 60°C увесь наш герметик розплавився та витік», — пояснює він. Тому необхідно адаптовувати свій продукт.

Водночас це не означає, що Калінін підтримує заборону України на експорт. «Якщо ціль цієї політики полягає в запобіганні витоку інтелектуальної власності, то це не надто ефективний захід, — пояснює очільник «Інфозахисту» та обґрунтовує свою позицію так: — Іноземні клієнти готові платити величезні кошти за локалізацію виробництва, тому тримається все не на забороні, а на патріотизмі та високій мотивованості українських інженерів».

Зараз «Інфозахист» продовжує роботу з виходу на стабільні джерела замовлень, що існують на іноземних ринках, зокрема країн Рамштайнської коаліції. Також у планах — створити виробничі спроможності за кордоном.

«Це необхідно, щоб під час наступного вторгнення росії наше виробництво не було окупованим, а отже могло би повноцінно забезпечувати потреби українського війська», — підсумовує Калінін.

НА ЗЕМЛІ: ВІД ФУТУРИСТИЧНОЇ ІГРАШКИ ДО «ДАВАЙТЕ ЦЕ СЮДИ»

Радіоелектронна розвідка необхідна для ефективного планування операцій, як оборонних, так і наступальних. Натомість українські засоби РЕБ дають відповідь на інше запитання: як захищатися від радіокерованих повітряних загроз, які швидко множаться?

Станом на 2017 рік українське військо готувалося до взяття на озброєння щонайменше трьох засобів РЕБ українського виробництва: комплексу «Анклав» від «Укрспецтехніка», комплексу «Нота» від «Трител» та комплексу «Буковель-AD» від «Проксімус». Це були доволі габаритні засоби, які розроблялися для протидії безпілотникам на відстані 15–20 кілометрів.

Натомість влітку 2014 року засновник компанії Kvertus Андрій Знайченко побачив кардинально інший спосіб протидії БпЛА. Побачив у доволі нестандартному місці: на виставці споживчої електроніки в Китаї. Такі події часто мають доволі розважальний характер, тож не дивно, що представлений під час заходу засіб РЕБ направленої дії мав вигляд футуристичної іграшки. Знайченко побачив на власні очі, що ця «іграшка» була здатна садити дрони і почав цікавитись військовими перспективами застосування антидронових рушниць.

До початку повномасштабного вторгнення такі вироби починали надходити в українське військо: восени 2021 року литовські EDM4S-UA вже використовувалися на лінії фронту. Kvertus на той час також уже створив подібну рушницю ANTIDRON KVSG-6, проте в комунікаціях із державою та військом компанії доводилося «пробиватися через стіну» незацікавленості.

Проте після початку повномасштабного вторгнення ставлення змінилося на: «У вас щось є? Давайте це сюди! Чим вам допомогти?». Компанія, яка у 2024 році реалізувала своєї продукції на близько 2 млрд гривень, відзначає, що вагому роль у пришвидшенні цих змін відіграв кластер підтримки Defense Tech розробок Brave1.

Про це зазначають і в Генеральному штабі ЗСУ. За 11 років війни українська оборонна галузь здійснила технологічний прорив.

■ Початок війни росії проти України у 2014 році

«Якщо у 2014 році застосування підрозділом у зоні бойових дій тактичного БпЛА вважалося чимось унікальним та поодиноким, то з 2022 року Збройні сили завдають найбільшу кількість уражень по російських військових об'єктах саме за допомогою дронів. Йдеться про повноцінне оформлення БпЛА як окремого виду озброєння з відповідною класифікацією. Це і розвідувальні, і ударні, і транспортні та низка інших безпілотників», — кажуть у Генштабі.

Водночас, продовжують у Генштабі, автоматизовані комплекси керування вогнем допомогли максимально скоротити час від виявлення цілі до її ураження, а винайдені рішення в сфері радіоелектронної боротьби протидіють ворожим каналам зв'язку та наведення. Крім цього, з'явилися наземні роботизовані комплекси різних типів.

«Збройні сили отримали доступ до високоточного озброєння. Триває робота над низкою інноваційних проєктів у ракетному озброєнні», — розповідають у відомстві.

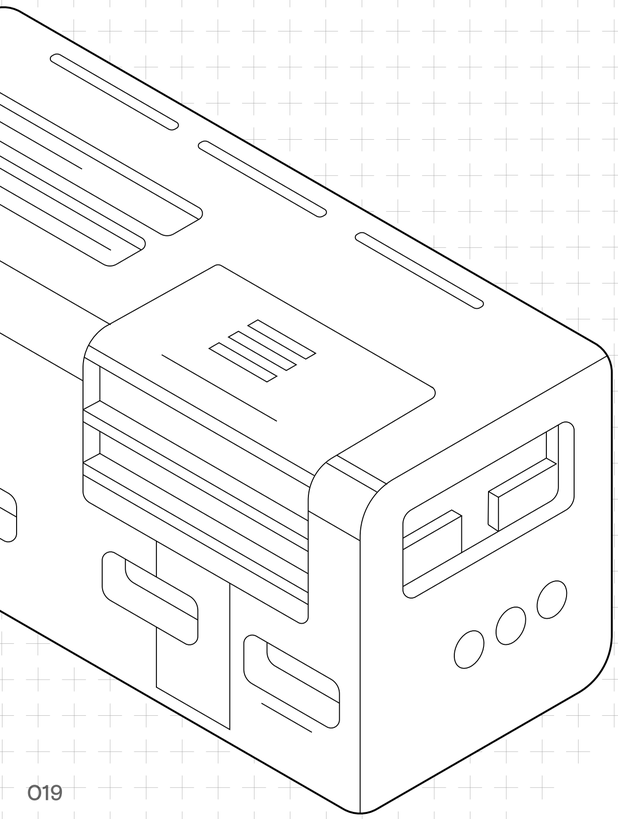
Змінилося ставлення і з боку іноземних ринків. Раніше необхідність засобів РЕБ ближньої дії був зрозумілий лише тим оборонним відомствам, які самостійно стикалися із загрозою безпілотників. На них дивилися як на «щось далеке, незвичайне і непотрібне». Натомість зараз інтерес до таких засобів з боку європейських закупівельників зростає. А великі оборонні компанії взагалі прагнуть локалізувати на своїх потужностях розробки Kvertus. Компанія сподівається скасування заборони на експорт, щоб самостійно постачати вироблену в Україні продукцію за кордон.

«Деякі з ваших запитань дещо передчасні», — так відповів представник одного із українських виробників безпілотників, із яким AIN спілкувався, готуючи цей огляд. Але він принаймні відповів. Чимало інших компаній, розробки яких працюють на фронті і за ним, не відповідають, адже свідомо уникають публічності. Так, наприклад, чинить «Укрджет» — компанія, яка займається безпілотниками щонайменше з 2017 року, увійшла в п'ятірку українських виробників БпЛА за найбільшим чистим прибутком у 2024 році, і вироби якої можна побачити в небі Татарстану.

Дійсно, викладене — лише окремі сторінки з історії українського Defense Tech. Ненаписаною залишається історія українських морських дронів через вищу секретність цих розробок. Окремого розділу потребуватимуть розробки у сфері програмного забезпечення. Публічна й аналітична робота лише починається.

ЗАГАЛЬНИЙ ОГЛЯД ЕКОСИСТЕМИ: СТАРТАПИ, АКСЕЛЕРАТОРИ, ДЕРЖАВНІ ІНСТИТУЦІЇ, ФОНДИ, ІНВЕСТОРИ, ЯКІ ПРЕДСТАВЛЕНІ НА РИНКУ, НАПРЯМИ РОБОТИ

КОМПАНІЇ



Усього в Україні 240 компаній, які розробляють свої продукти у сфері Defense Tech, підрахували Molfar. Серед них 5 державних. У період з 2014 до 2025 року заснували 222 компанію. Втім, найбільший сплеск — 73 нові компанії — зафіксували у 2023-му.

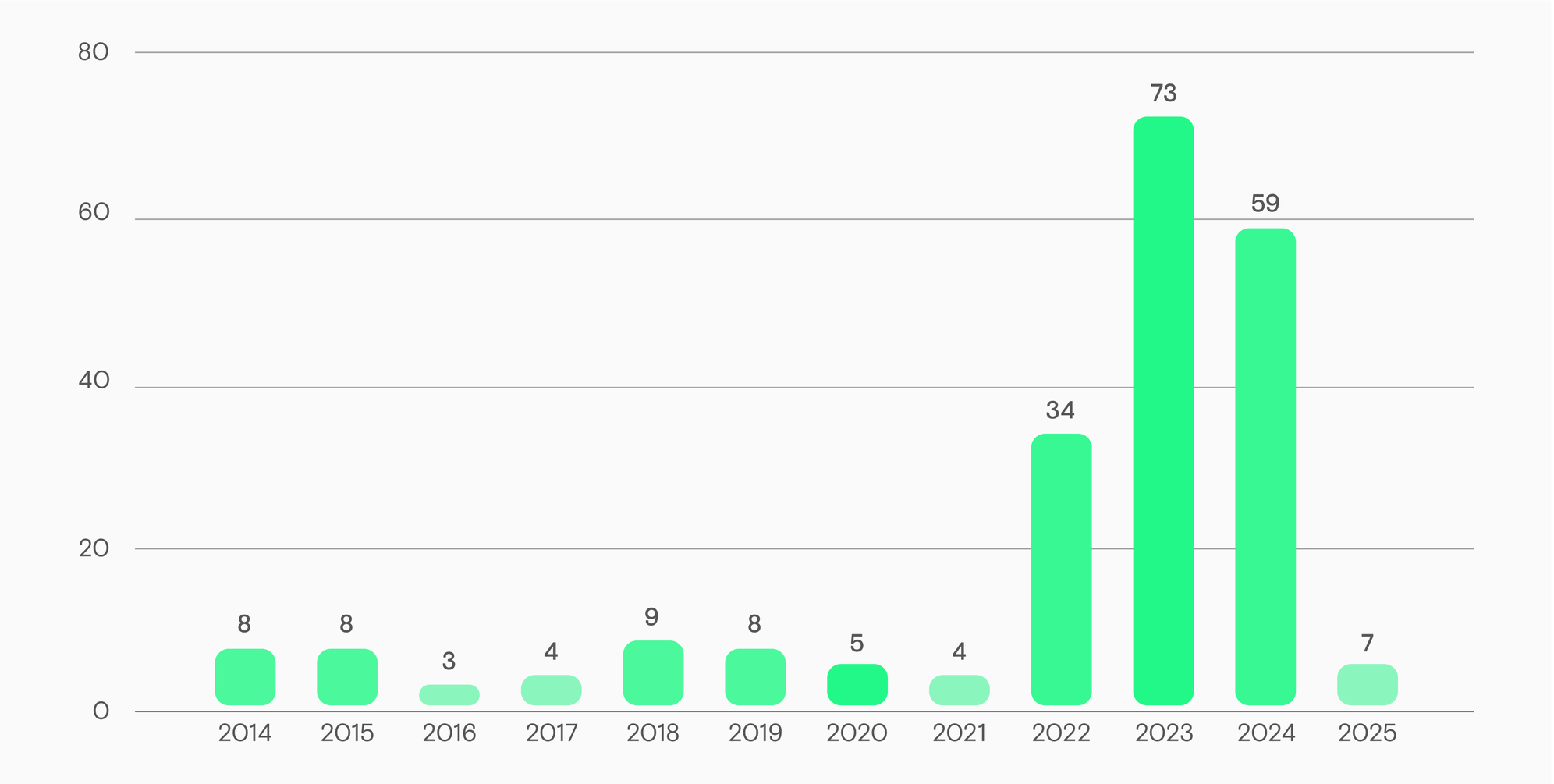
За даними Brave1, на платформі представлено 3600 розробок, сотні з яких вже кодифіковано за стандартами НАТО й застосовано на фронті.

ТАБЛИЦЯ З КОМПАНІЯМИ

*Список може бути неповним, а стартапи можуть бути розділені на кілька категорій одночасно.

Редакція вдячна за фактчекінг і консультування керівному партнеру Angel One Venture Fund Івану Петренку та співзасновнику й голові ГО «Аеророзвідка» Ярославу Гончару.

■ Загальний огляд екосистеми



У переліку подані приватні продуктові оборонні компанії, засновані у період 2022-2024;

Відібрані компанії, які засновані та/або мають штаб-квартиру в Україні. Офіси іноземних компаній не враховувалися.

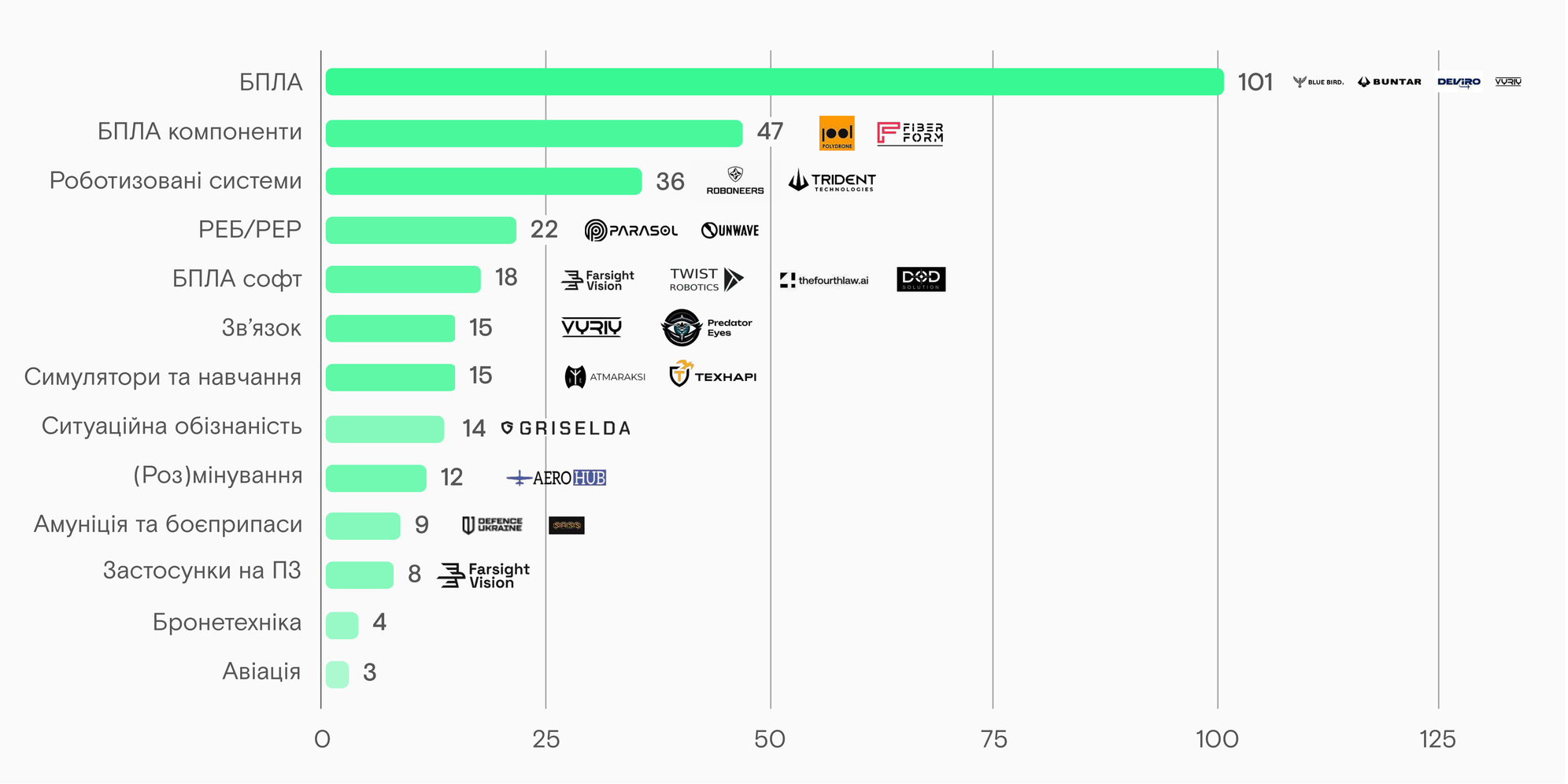
Пошук даних про інвестиції відбувався здебільшого по відкритих джерелах, додатково використовувалися Crunchbase та Pitchbook.

В переліку обрані компанії з TRL7

КОМПАНІЇ

За даними державного кластерадля розвитку оборонних технологій Brave1, на платформі представлені 3600 розробок, сотні з яких уже кодифіковано за стандартами НАТО й застосовано на фронті.

За підрахунками Molfar, найпопулярнішими серед українських Defense Tech компаній є 14 продуктів. У топі — робота з безпілотними літальними апаратами та їхніми компонентами, роботизованими системами, РЕБ/РЕР і софт для БПЛА. Деякі компанії розробляють більше як один продукт.

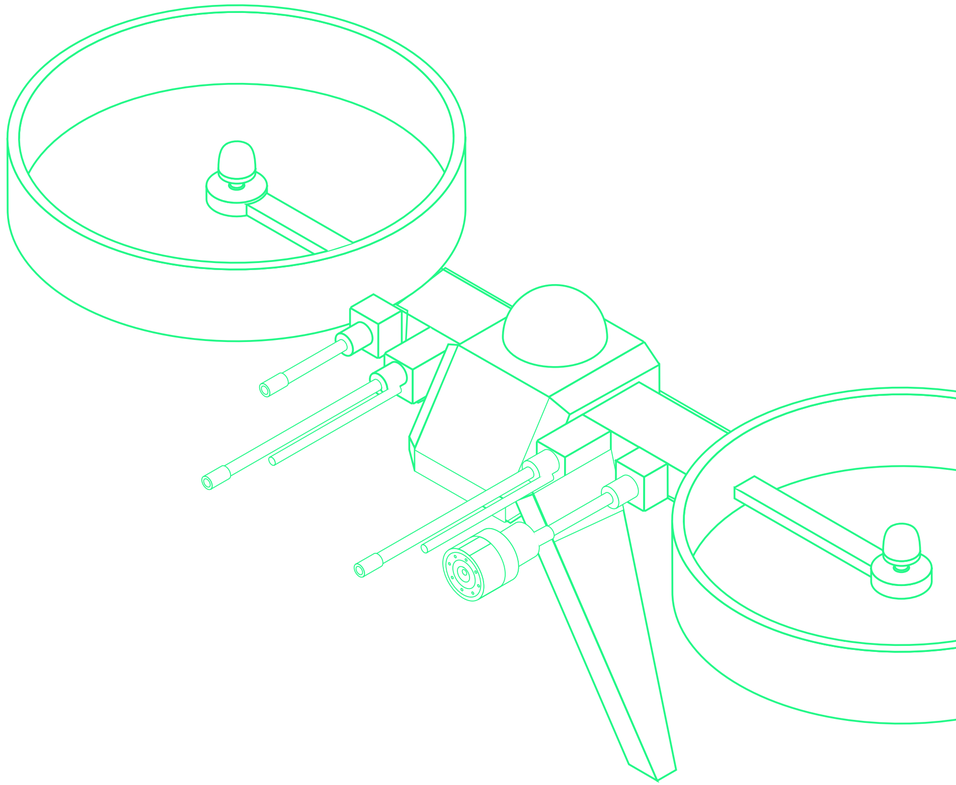


ФОНДИ \ ІНВЕСТОРИ \ ГРАНТОВІ ПРОГРАМИ \ АКСЕЛЕРАТОРИ

До переліку потрапили ті інвестори, які працюють з українськими продуктами. Джерела даних: Open VC, Crunchbase, PitchBook, офіційні сайти фондів, DataDriven.

Окрім українських та іноземних фондів підтримка українських компаній, що займаються розробкою дронів, здійснюється через наступні ініціативи:

- Коаліція дронів, очолювана Латвією та Великою Британією. У 2024 коаліція виділила Україні $1.87 млрд (€1.8 млрд), у 2025 планується направити Україні $2.86 млрд (€2.75 млрд).
- ZBROYARI: Manufacturing Freedom – у 2024 зібрали $1.5 млрд для української оборонної промисловості з внесками від ЄС, Данії, Канади, Нідерландів, Литви, Великої Британії, Норвегії, Ісландії та США. З цієї суми $559 млрд (€538 млрд) скалала "Даньська модель" – уряди Данії, Швеції, Ісландії та відсотки від російських заморожених активів фінансували українські оборонні підприємства.



ФОНДИ \ ІНВЕСТОРИ \ ГРАНТОВІ ПРОГРАМИ \ АКСЕЛЕРАТОРИ

Назва	Середній чек	HQ	Українські проєкти, в які інвестували
MITS Capital	$100 тис. -$200 тис.	Нью-Йорк, Київ	M-Fly, Tencore, Teletactica, NORDA Dynamics
Nezlamni Fund	$100тис. — $400 тис.	Київ	Himera, Ailand Systems, Buntar Aerospace, Mantis Analytics, Frontline
Double Tap Investments	$100 тис. — $300 тис.	Фінляндія	Griselda, The Fourth Law, Black Forest Systems, Hard Cat Drones
Green Flag Ventures	$150 тис. — $1.2 млн	Лос-Анджелес	Teletactica, Swarmer, Himera
Angel One	$50 тис. — $300 тис.	Львів	Swarmer, NORDA Dynamics, Frontline, Teletactica
Brave1	$12 тис. — $192 тис.	Київ	Frontline, Ratel, Swarmer, Mantis Analytics, Tencore, Kvertus, Kolossal, Vepryk, SkyLab UA, Ailand Systems
DarkStar	€500 тис. — €1 млн	Естонія	Deftak, Farsight Vision
D3.vc	$125 тис.	Київ	Zvook, Frontline, Swarmer, Ailand Systems, Buntar Aerospace, Drone Space Lab, Stridar
Presto Tech Horizons	€150 млн	Прага	Teletactica, NORDA Dynamics, Himera
United Angels Network	$100 тис. — $375 тис.	Львів	Teletactica, NORDA Dynamics, Himera
Startup Wise Guys	$50 тис. — $200 тис.	Таллінн	Frontline
Seeds of Bravery	до €60 тис.	Берлін	Mantis Analytics, BeesAgainstMines, Rcam, Airlogix, Temerland
Startup Competition від IT Arena	$10k тис. — $3 млн	Львів	Zvook, Himera
ZAS Ventures	$50 тис. — $200 тис.	Київ	Mantis Analytics
Radius Capital	$100 тис. — $1 млн	Сан-Франциско	Swarmer
42CAP	$500 тис. — $2 млн	Мюнхен	Osavul

Назва	Середній чек	HQ	Українські проєкти, в які інвестували
SMRK VC Fund	$0,5 тис. — $1,5 млн	Київ	Osavul
Ukrainian Startup Fund	$25 тис. — $50 тис.	Київ	Huless, IZIVIZ, DrillApps, AeroDrone
Freedom Fund VC		Берлін	M-FLY, Himera
Resist.ua		Київ	M-FLY
Slava Ventures		Менло-Парк (США)	Zvook
Kalyna Capital	$200 тис. — $2 млн	Лос-Анджелес, Київ, Сіетл	
Seven Capital	$25 тис. — $1 млн	Брюссель	невідомо
ZAKA VC	$100 тис. —$300 тис.	Прага, Кремнієва долина	немає даних
Innsaei Capital	$100 тис. — $2 млн	Лондон	невідомо
Defense Builder	$10 тис. — $40 тис.	Київ	Barvinok-5, Hard Cat Drones, Strug, Життя без мін, Coalas
Oppenheimer Acceleration	$125 тис.	Сан-Франциско	Anvarix Technologies, Aetos Space Labs, BabAI, RightSpot.AI, MARA
Хакатон «Наступ машин» від МО	$10 тис.	Київ	
IRON Lviv Tech Cluster		Львів	
Акселератор «Інноваційна Україна»		Київ	працюють з ініціативами навчальних закладів
Innovation Hub від TAF Drones	до $1 млн	Україна	
Vacuum		Україна	Airlogix, Temerland, Rcam, DrillApps

ДЕРЖАВНІ ІНСТИТУЦІЇ

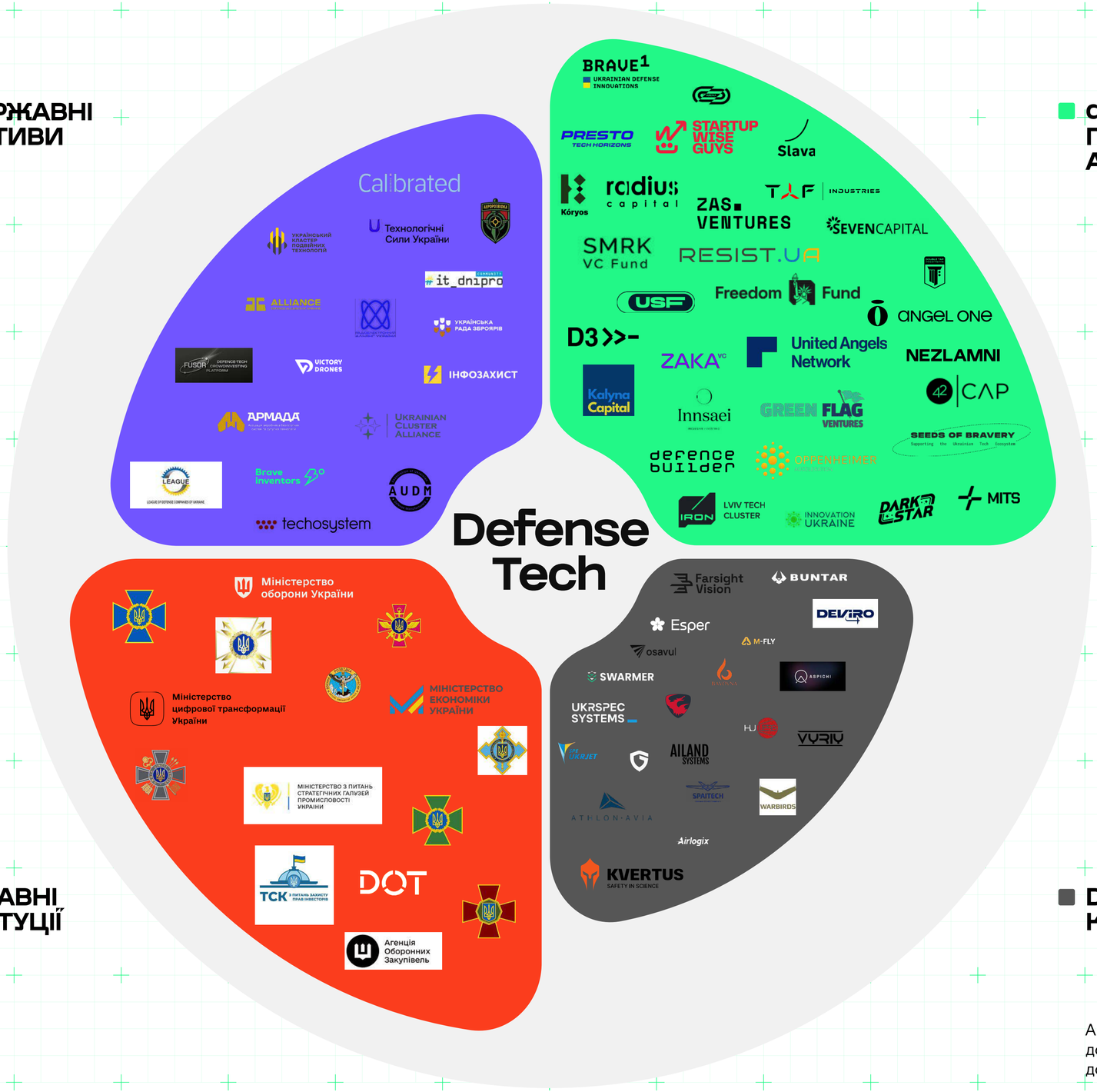
Інституція	Діяльність у сфері Defense Tech
Міністерство оборони	головний орган, що забезпечує реалізацію державної політики у сфері оборони.
Головне управління розвідки	воєнна розвідка.
Генеральний штаб Збройних сил	основне військове формування.
Міністерство цифрової трансформації	формування та реалізація державної політики у сфері цифровізації; Армія дронів; Brave1.
Міністерство економіки	працює над залученням інвестицій, економічною стратегією.
Державна служба спеціального зв'язку та захисту інформації	орган, що відповідає за захищений зв'язок, кібербезпеку та криптозахист.
Рада національної безпеки та оборони	координаційний орган з питань нацбезпеки.
Служба безпеки	спецслужба, яка виконує функції контррозвідки, боротьби з тероризмом, кіберзлочинністю.
Національна гвардія	військове формування з правоохоронними функціями.
Державна прикордонна служба	охорона державного кордону.
Служба зовнішньої розвідки	розвідувальна діяльність за межами України.
Тимчасова спецкомісія з питань захисту прав інвесторів	робота з інвесторами та покращення інвестиційної привабливості.
Агенція оборонних закупівель	державне підприємство Міністерства оборони України, створене для оптимізації та централізації процесу закупівель у сфері національної безпеки й оборони.
Державний оператор тилу	державна агенція, що постачає харчі, речі та пально-мастильні матеріали для потреб військових.

НЕДЕРЖАВНІ ІНІЦІАТИВИ

Інституція	Діяльність у сфері Defense Tech
Технологічні Сили України	об’єднання понад 80 приватних виробників озброєння та військової техніки, адвокують розв’язання проблем галузі для ефективного розвитку індустрії.
ГО «Аеророзвідка»	громадська організація, яка з 2014 року створює військові розробки: дрони, програмне забезпечення, система ситуаційної обізнаності «Дельта» та технологічні хаби.
Victory Drones	проєкт технологічної мілітаризації суспільства, який пропонує навчання для майбутніх військових на FPV-дронах і зі спеціалізованим програмним забезпеченням.
Calibrated	комунікаційна агенція, яка працює з комунікаціями для Defense Tech стартапів.
Український кластер подвійних технологій	об'єднання, яке зосереджене на розробці, впровадженні оборонних технологій.
IT Dnipro Community	спільнота IT-фахівців, які розробляють рішення для навчання пілотів FPV-дронів та зв'язківців, а також проєкти «Нічний водій», Skylark і Tactical CommLink Point.
Українська рада зброярів	об'єднання виробників озброєння та військової техніки, створюючи платформу для співпраці з державою, військом і міжнародними партнерами.
Оборонний альянс України	об’єднання промисловості, військових і держави.
Ліга оборонних підприємств України	об’єднання національних приватних виробників озброєння і військової техніки.
Асоціація «Радіоелектронний альянс України»	об’єднання виробників РЕБ/РЕР.
Асоціація «Армада»	об’єднання виробників безпілотних систем та супутніх технологій.
Український кластерний альянс	мультигалузева загальнонаціональна спілка підприємств, бізнес-об’єднань, кластерів і кластерних організацій України.

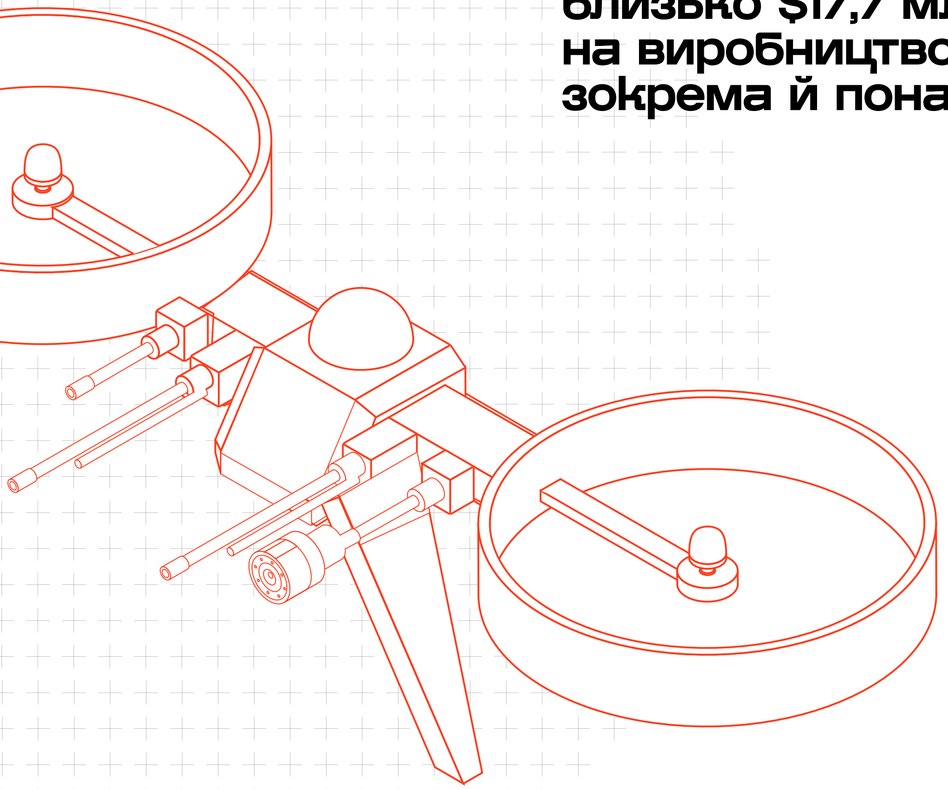
НЕДЕРЖАВНІ ІНІЦІАТИВИ

Інституція	Діяльність у сфері Defense Tech
«Інфозахист»	за 20 років став представником комерційного сектора оборонної галузі України, розробляє програмні та апаратні рішення для силових структур України.
Techosystem Defense Cluster	кластер, який допомагає розвивати оборонні технології в Україні.
Brave Inventors	неурядова платформа, яка об'єднує винахідників, інвесторів, бізнес і волонтерів навколо спільної ідеї — забезпечити ЗСУ інноваційним технічним обладнанням.
Асоціація виробників озброєння та військової техніки України	об'єднання приватних компаній і виробників озброєння, засноване за підтримки Ради волонтерів при Міністерстві оборони України.
Fusor	платформа crowd-інвестування, яка об'єднує українські Defense Tech стартапи з приватними інвесторами.
Defence Builder	акселераційна програма для українських оборонних стартапів.
MITS	інвестиційна група, що фокусується на залученні іноземного капіталу в український оборонний сектор. Має власний акселератор.
Defense Innovation Highway (DIH)	платформа для посилення оборонної кооперації між Україною та Нордичними країнами.



Автори матеріалу вдячні DataDriven за внесок до огляду Defense Tech екосистеми в їхньому дослідженні Ukrainian Defence tech market report

РЕЙТИНГ DEFENSE TECH КОМПАНІЙ, ЯКІ ЗА 10 РОКІВ ЗАЛУЧИЛИ НАЙБІЛЬШЕ ІНВЕСТИЦІЙ

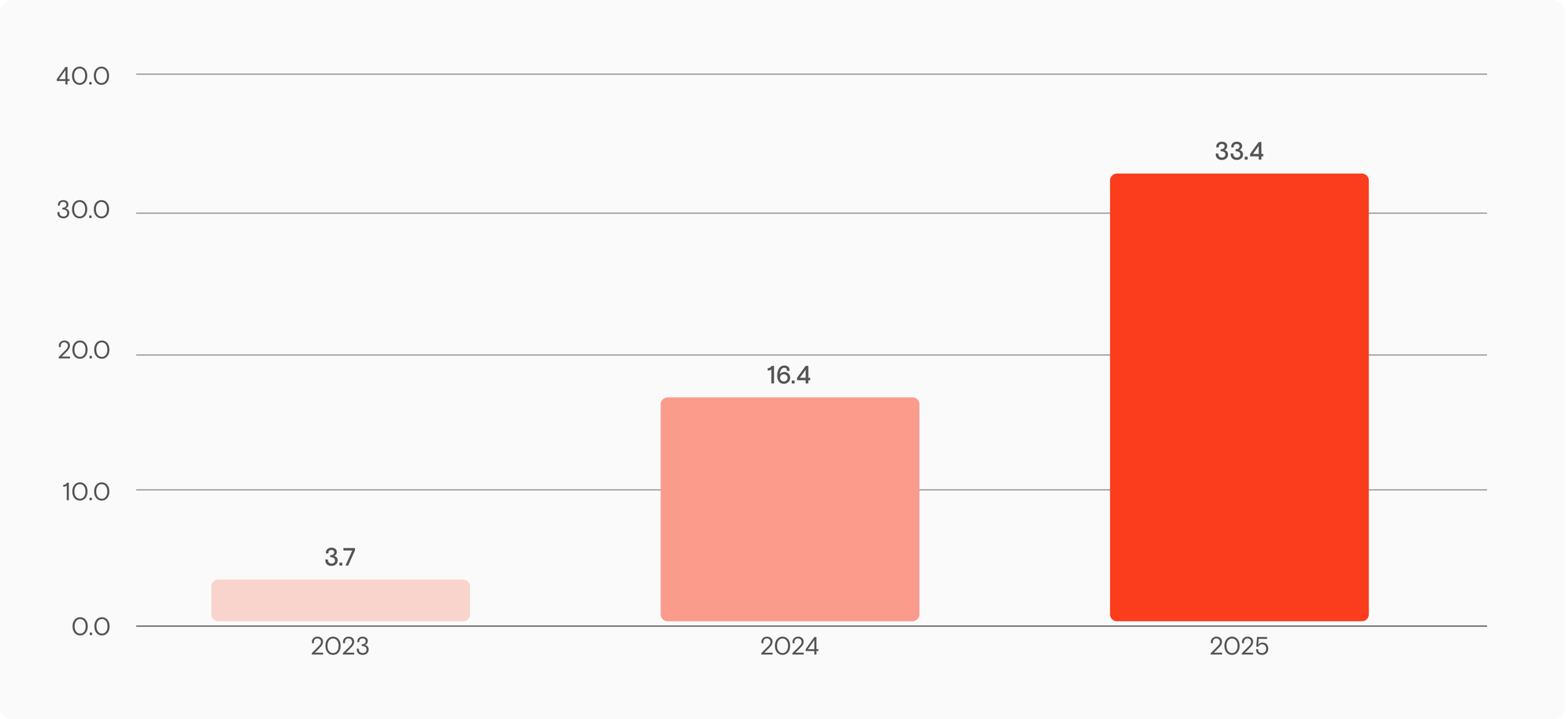


За даними EY, у 2025 році на потреби оборони та безпеки з держбюджету України планують витратити 26,3% ВВП або понад $53 млрд. З цієї суми близько $17,7 млрд спеціально виділено на виробництво та закупівлю зброї, зокрема й понад $1 млрд на БПЛА.

Було знайдено інформацію про інвестиції в 58 компаній з 240, з них відомі суми в 35 компаній. За даними дослідження, у 2022 сума інвестицій невідома, у 2023 компанії зібрали $3.7 млн, у 2024 - $16.4 млн. За даними EY, загалом у 2023 році українські стартапи зібрали $5 млн інвестицій, у 2024 ця сума зросла до $40 млн. А протягом 2025 року лише державний кластер Brave1 планує залучити $100 млн, при цьому коштів з держбюджету у цій сумі — майже три чверті — $71,6 млн.

За даними Molfar, на початок вересня 2025 відомо про $33.4 млн інвестицій сумарно від державних і приватних інвесторів.

■ Рейтинг Defense Tech компаній

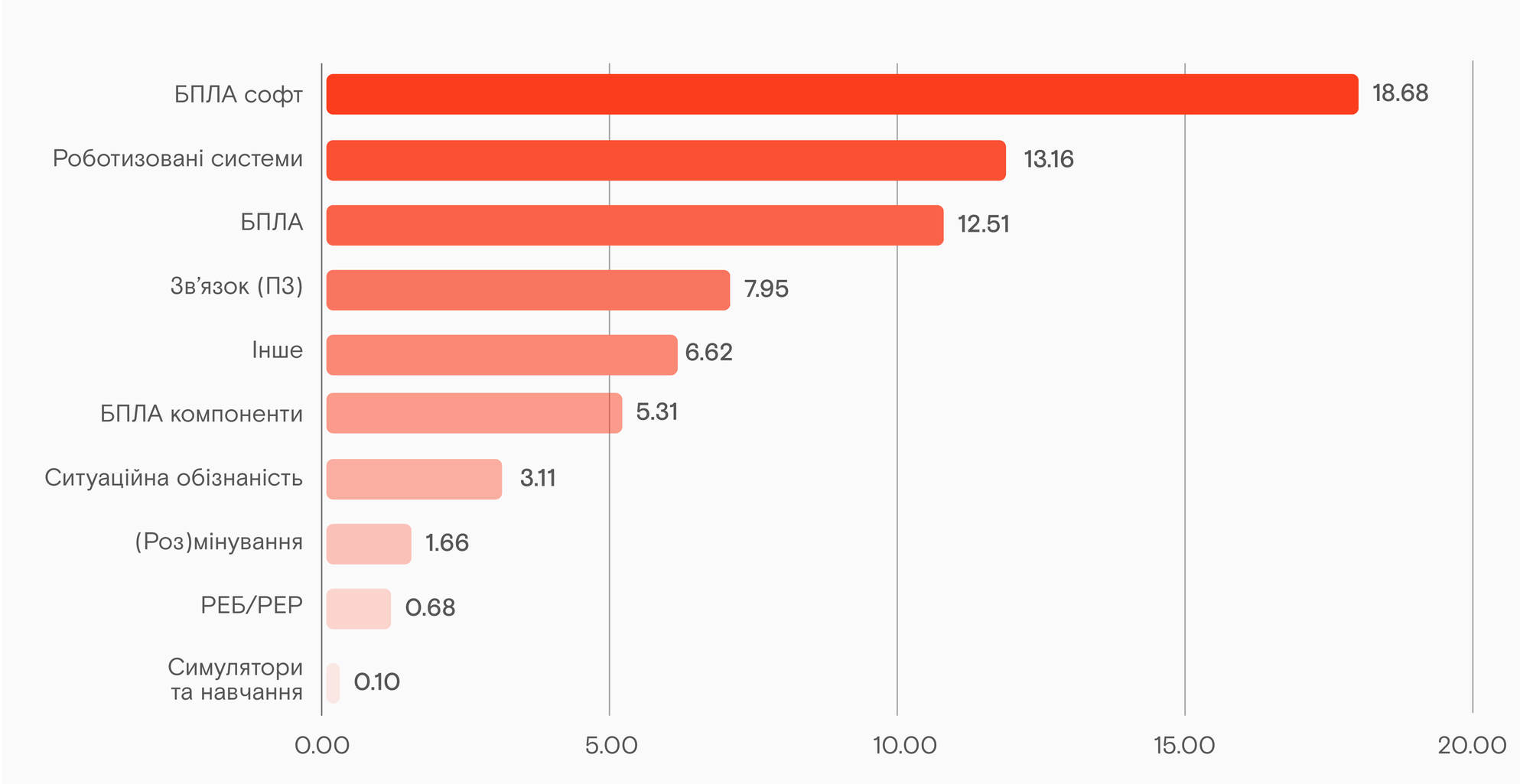


Українські Defense Tech компанії, які залучили найбільше інвестицій з 2014-го по середину вересня 2025-го року

Компанія	Сума інвестицій, $ млн
Swarmer	$17,8 млн
Ark Robotics	$8.7 млн
Trypillian	$5 млн
Osavul	$4 млн
Buntar Aerospace	$4 млн
Tencore LLC	$3.7 млн
Teletactica	$2.5 млн
Himera	$2.15 млн
M-Fly	$1.3 млн
Huless	$1.3 млн

— Дані: Crunchbase, Pitchbook

Інвестиції за напрямами, 2022-2025, млн доларів



— Дані: Crunchbase
— До Defense Tech проєктів редакція також додає компанії, які працюють для ветеранів і ветеранок, зокрема в галузі протезування.

За даними EY, середній розмір Seed раунду у Defense Tech секторі зріс з $500 тисяч у 2023-му до середнього діапазону від $1 млн до $3 млн у 2024-му.

Серед напрямків найбільші інвестиції за 3 роки сумарно отримали:
- БПЛА софт - $18.68 млн;
- роботизовані системи - $13.16 млн;
- БПЛА - $12.51 млн.

Топ українських фондів за інвестиціями в компанії екосистеми (в портфоліо фондів може бути більше компаній).

Назва	Тип	Капітал, $, млн	Типовий розмір інвестицій, $, тис.	Відома кількість інвестицій	Стартапи
Brave1	Gov	71.6	12-192	27	Frontline, Ratel, Swarmer, Mantis Analytics, Tencore, Kvertus, Kolossal, Vepryk, SkyLab UA, Ailand Systems
D3 Venture Capital	Private	19.0	125	8	Zvook, Frontline, Swarmer, Ailand Systems, Buntar Aerospace, Drone Space Lab, Stridar
Defence Builder	Private	–	10-40	5	Barvinok-5, Hard Cat Drones, Strug, Життя без мін, Coalas
Nezlamni Fund	Private	2.0	100-400	5	Buntar Aerospace, Himera, Frontline, Ailand Systems, Mantis Analytics
MITS Capital	Private	50.0	100-200	4	M-Fly, Tencore, Teletactica, NORDA Dynamics
United Angels Network	Private	–	150-375	3	Teletactica, NORDA Dynamics, Himera
Ukrainian Startup Fund	Gov	8.7	25-50	2	Drill, Huless

— Дані, які аналітична платформа YouControl подала кількома значеннями (наприклад, 3 100 000 — 3 200 000), ми округлили до більшого числа. Такі клітинки відмічені *

BUNTAR AEROSPACE

Засновники:

Богдан Сас
Катерина Безсудна
Іван Каунов

Дата заснування:

2023

Загальна сума відомих інвестицій:

$4 млн.

Основне джерело доходу — інвестиції. Працюють над тим, щоб вийти на самоокупність у 2025 році.

Про компанію і розробку:

Buntar Aerospace розробляє комплексні рішення для навігації та управління БпЛА. Команда працює над розробкою таких продуктів:

- **Buntar Copilot:** програмне забезпечення для планування та виконання розвідувальних місій, що генерує динамічні плани польотів, враховуючи всі тактико-технічні деталі: ситуаційну обізнаність, прогноз погоди, карту висот, карти сигналів та інші джерела. На 90% автоматизує роботу оператора БпЛА з планування та управління місіями, а також сумісний з іншими БпЛА.
- **Buntar One:** розвідувальний БпЛА тактичного рівня з додатковою камерою та модулем візуальної навігації на основі ШІ.

Основні події компанії:

- Український стартап Buntar Aerospace визнаний стартапом 2024 року за версією Innovation Development Fund Award.
- Buntar Aerospace отримав нагороду «Найбільш перспективний проєкт» у категорії «Оборонні технології» від DOU у 2024 році.
- Buntar Aerospace обрали найкращим Tech for Good стартапом 2024 року за версією Tech Ecosystem Awards.
- Співзасновники Uklon Віталій Дятленко, Сергій Смусь, Вікторія Дубровська та Дмитро Дубровський проінвестували $200 000 у межах seed-раунду у 2024 році.
- Компанія завершила програму SRI Deep Tech Security Accelerator у Кремнієвій долині.

Як ви оцінюєте свій потенціал до зростання в найближчі роки та після завершення війни?

Ми впевнені, що зможемо стати вагомим гравцем в українському ОПК. Наш підхід до команди — це, мабуть, головна причина. У нас талановиті інженери, пілоти, конструктори. Багато хто пішов з великих компаній, щоб приєднатися до нас, бо бачить сенс і драйв у тому, що ми робимо. Ми створюємо не просто продукт, а нову культуру виробництва військових технологій. І ця культура відрізняється від радянського спадку, який досі присутній у деяких підприємствах галузі.

Чим технології Buntar Aerospace можуть бути корисні в цивільному користуванні?

Зараз фокус — це винятково оборонка. Світ став жорсткішим, і виживає той, хто може себе захистити. Але технологічно — так, наші рішення можуть використовуватись у цивільному секторі. Наприклад, складні автономні місії, вимоги до навичок оператора, підвищена надійність — усе це затребувано і в рятувальних операціях, і в аграріїв, і в енергетиці.

Наразі ми не хочемо розпорошуватись. Є війна — ми працюємо на перемогу. Пізніше будемо думати, як адаптувати ці технології для мирного життя.

BUNTAR

Які події чи зміни останніх років мали найбільший вплив на розвиток компанії?

Складно виділити щось одне: у нас події як в бойовому зведенні — щотижня новий виклик. Але як маркер — запуск БпЛА Buntar-3. У нього ми зібрали все найкраще, що зробили до того. Після його появи команда відчула, що ми дійсно готові до великої гри.

Як компанія адаптується до змін на глобальному ринку?

Через диверсифікацію. Ми не ставимо все на одну карту. Є діалог з партнерами та постачальниками в Європі, США, на Близькому Сході. З кожним будуємо окрему логіку взаємодії — комерційно, технологічно, юридично. Це вимагає більше зусиль, але це гарантія стійкості. Бо глобальний ринок зараз нестабільний, і мати план Б — обов'язково.

BUNTAR

Які стратегічні рішення найбільше сприяли зростанню бізнесу?

Фокус. Це було найболючіше рішення — сказати «ні» кільком крутим напрямам, які, можливо, дали б швидкий прибуток, але забрали б фокус. Ми залишили тільки ті продукти, в які самі віримо на 200%. Buntar-3, Skyhopper, програмне забезпечення Buntar Copilot — і все, що допомагає їм працювати як система. Решту — віддали в партнерство або поставили на паузу.

Чи є в компанії особливий підхід до управління та корпоративної культури?

Ми будуємо компанію, де кожен має голос. У нас немає «начальників» у класичному сенсі — є відповідальні. Ми не боїмось помилок, але не прощаємо байдужості. Людина або «наша», або ні. І це визначається не резюме, а тим, як вона діє під тиском. Усі, хто залишився після першого нашого року, — це перевірені бійці. І вони роблять дійсно велику справу.

Що відрізняє вас від конкурентів?

BUNTAR

Ми можемо дозволити собі розкіш — не бігти за кожною гривнею. У нас є резерв, який дозволяє будувати продукт системно. І ми можемо обирати, з ким працювати. Це створює інший підхід: ми не намагаємося всім продати все. Ми шукаємо партнерів, які розуміють цінність і готові працювати на результат. Це і є наш шлях — не масовість за будь-яку ціну, а якість, яка витримає найжорсткіше бойове застосування.

HIMERA

Засновники:

Міша Рудомінський
Олексій Олійник

Дата заснування:

2022

Загальна сума відомих інвестицій:

$2.15 млн

Про компанію і розробку:

HIMERA – розробник і виробник систем зв'язку для Сил оборони. Продукція HIMERA вже присутня у всіх типах підрозділів Сил оборони України та має застосування в Повітряних Силах та Силах спеціальних операцій США.

Серед продуктів компанії:

- Портативна радіостанція G1 PRO – 48+ годин автономної роботи
- Автономний ретранслятор B1 – одразу готовий до використання
- Ретранслятор R1 з можливістю інтернет-ретрансляції – бездротова конфігурація всієї мережі

HIMERA

Засновники:

Міша Рудомінський
Олексій Олійник

Дата заснування:

2022

Загальна сума відомих інвестицій:

$2.15 млн

Основні події компанії:

- 3 лютого 2025 року команда має офіційного партнера в США та Канаді з правом просування на окремих ринках НАТО і союзників — компанію Quantropi Inc., експерта в галузі квантово-безпечних технологій.
- Український розробник систем зв'язку з високим рівнем захисту Himera залучив інвестиції у seed-раунді від фонду Nezlamni. Розмір інвестицій не розголошується, але відомо, що він відповідає типовому чеку фонду — від $100 000 до $400 000.
- Himera Radios залучила $525 000 на нарощування виробництва для Сил оборони України у 2024 році.
- Проєкт посів перше місце в конкурсі стартапів IT Arena 2023 і отримав $10 000.
- У квітні 2024 Himera підписала дистриб'юторську угоду з американською оборонною технологічною компанією Reticulate Micro.
- Український стартап залучив інвестиції від фонду Green Flag Ventures у 2024 році.
- Залучили $150k від United Angels Network, щоб стимулювати експансію в Україні та за кордоном. Це друга інвестиція від United Angels Network, завдяки чому загальна сума підтримки стартапу склала $375k.
- Компанія стала переможцем премії DOU в номінації «Найперспективніший проєкт в military-tech галузі» у 2024 році.
- HIMERA у 2024-му стала одним з переможців хакатону «Наступ Машин» від Міністерства оборони України.
- Стартап переміг в Ukrainian Startup Awards 2023 Lift99 Kyiv Hub у категорії Defense & Security у 2024.
- У 2023 році HIMERA отримала премію USF Startup Awards 2023 у номінації Best Dual-Use Startup.

Як ви оцінюєте свій потенціал до зростання в найближчі роки та після завершення війни?

Маємо на меті стати основною комунікаційною системою Сил оборони України.
Також потенційний ринок охоплює країни-члени НАТО, ЄС. Плануємо диверсифікувати свою діяльність у суміжних секторах, включаючи правоохоронні органи, служби з надзвичайних ситуацій і приватну безпеку, відкриваючи додаткові можливості для зростання.

Чим технології HIMERA можуть бути корисні в цивільному користуванні?

Ми запустили систему, яка створює свою захищену мережу та підтримує mesh-технологію — вона найдовше серед конкурентів працює автономно й навіть у складних умовах. Такий зв'язок можуть використовувати служби швидкого реагування, охоронці чи рятувальники — для безперебійної передачі голосу й даних у місцях катастроф, наприклад, під час завалів або операцій у важкодоступній місцевості.

HIMERA

Як компанія адаптується до змін на глобальному ринку?

Робимо все можливе, аби бути готовими до будь-яких змін. Наприклад, по кожному з компонентів, які використовуємо, маємо мінімум два постачальники, щоб мінімізувати затримки, та збільшуємо кількість оборотних коштів, які вкладаємо в резерви.

Які стратегічні рішення найбільше сприяли зростанню бізнесу?

Ми сфокусувались на тому, щоб якісно робити меншу кількість продуктів.

Що відрізняє вас від конкурентів?

Наші конкуренти поділяються на дві категорії: застарілі тактичні системи зв'язку та цивільні портативні радіостанції. Застарілі тактичні системи потужні і дорогі, використовують військові сертифіковані мікросхеми з обмеженими виробничими можливостями. На відміну від них, цивільні ручні радіостанції відносно дешевші, пропонують базовий голосовий зв'язок і обмежені можливості шифрування. Тож ми поставили собі задачу: зробити тактичну радіостанцію, а потім і систему зв'язку, яка, з одного боку, важка для виявлення, перехоплення і придушення, містить систему передачі даних, працює у складних умовах, механічно захищена, а з другого — доступна для масового виробництва.

AILAND SYSTEMS

Засновники:

Дмитро Тітов
Георгій Шакула

Дата заснування:

2020

Загальна сума відомих інвестицій:

$425 000

Основне джерело доходу — інвестиції. Працюють над тим, щоб вийти на самоокупність у 2025 році.

Про компанію і розробку:

Ailand Systems — компанія, що працює та створює рішення для землеробів, а з початку повномасштабної війни почала розробляти проєкти для розмінування. Серед розробок компанії — безпілотний літальний міношукач ST1 та інноваційне рішення, що дозволяє відловлювати комах і жуків.

До повномасштабної війни Ailand Systems працювала на ринку 10 років як сервісна IT-компанія, основною експертизою якої був комп'ютерний зір, 3D-графіка, віртуальна і доповнена реальність. З часом компанія спробувала себе в дронобудуванні та сфокусувалася на аграрному секторі — виготовляла ШІ-квадрокоптер RT1 Debugger, який ловив шкідників на полях без використання пестицидів.

«Усі технології, з якими ми раніше працювали, безпосередньо потрібні в навігації, плануванні маршрутів, детекції об'єктів. Тому робототехніка стала логічним розвитком для нас. Ми створили прототип дрона для контролю шкідників на агрополях — це контроль, детекція і їхнє знешкодження механічним способом. Взимку 2022 року якраз домовилися з фермерами про запуск пілотного проєкту, але почалось повномасштабне вторгнення, і проблеми фермерів змінилися — їх більше хвилюють міни, ніж шкідники», — розповідає CEO Ailand Systems Дмитро Тітов.

Тож Ailand Systems адаптували дрони — тепер їх використовують для пошуку мін на полях. Так з'явився проєкт ST1 — дрон для детекції вибухонебезпечних об'єктів.

Основні події компанії:

- Фонд «Незламні» оголосив про $200 000 інвестицій в компанію у 2024 році.
- У 2023 році стартап отримав $125 000 від фонду D3.
- Ailand Systems отримали фінансову підтримку в розмірі $100 000 від Google у 2024 році.

Яке джерело доходу є основним для вашої компанії?

Надання консультативних сервісів не тему розмінування та продаж дронів.

Як ви оцінюєте свій потенціал до зростання в найближчі роки та після завершення війни?

Потенціал буде прямо пропорційним до суми залучених інвестицій. Усі проєкти, пов’язані з дронами, мають значний потенціал до росту. Але зростуть тільки ті, кому вдасться вийти на західні ринки шляхом залучення значних інвестицій. У нашому випадку закінчення війни буде тільки сприяти зростанню, бо розмінування стане головним пріоритетом, яким, на даний момент, є зброя та засоби ураження.

Чим ваші технології можуть бути корисні в цивільному користуванні?

Розмінування буває військовим і гуманітарним. Тобто в нашому проєкті вже є цивільна складова. Крім того, плануємо налагодити виробництво дронів для сільського господарства. Насправді, наша компанія розпочиналась саме з дронів сільськогосподарського призначення, які ми адаптували під розмінування після початку повномасштабного вторгнення.

Чи планується залучення нових інвестицій?

Так, прямо зараз перебуваємо в процесі фандрейзингу на seed раунді. Додаткові кошти потрібні для масштабування виробництва та випуску нових продуктів.

Чим ваші технології можуть бути корисні в цивільному користуванні?

Початок повномасштабного вторгнення змусив нас адаптувати наші дрони під розмінування. Далі все йшло більше менш прогнозовано: розробка, гранти, інвестиції, покращення розробки — і так по колу.

Які стратегічні рішення найбільше сприяли зростанню бізнесу?

Виділити ресурси на пошук грантів і міжнародних донорів. Ринок розмінування дуже складний із комерційного погляду. Тут багато залежить від допомоги донорів.

Чи є в компанії особливий підхід до управління та корпоративної культури?

Ми наслідуємо найкращі практики IT-компаній: гнучкий підхід до процесу розробки (Agile), демократичне ухвалення рішень, щоденні наради для синхронізації. У цілому умови роботи є демократичними й адаптованими під потреби інженерів: наприклад у деяких інженерів є свій власний графік роботи, а в декого можливість працювати дистанційно.

Що відрізняє вас від конкурентів?

Якщо говорити про виробників дронів для розмінування, то нас відрізняє наявність дрона власного виробництва, українського. Усі конкуренти використовують китайські дрони, на які навішують додаткові сенсори.

Якщо говорити про виробників дронів загалом, то нас відрізняє повна автономність: від початку і до кінця обстеження дрон працює в повністю автономному режимі, що включає побудову траєкторії, підбір висоти, обліт перешкод і повернення на базу при низькому заряді батарей.

Крім цього, ми розробляємо повну екосистему для виконання операцій із дронами, до якої належать:

- БПЛА;
- Базова станція для забезпечення зв’язку та точного позиціонування;
- Зарядна станція для заряджання батарей;
- «Розумні» батареї з точною оцінкою рівня заряду;

Усі ці продукти будуть корисні не тільки в розмінуванні, але й в дронах аграрного виробництва.

BAVOVNA AI

Засновники:

Максим Прасолов

Дата заснування:

2022

Загальна сума відомих інвестицій:

$2,7 млн

Основне джерело доходу — інвестиції. Працюють над тим, щоб вийти на самоокупність у 2025 році.

Про компанію і розробку:

Bavovna AI — українсько-американська DeepTech компанія, яка розробляє альтернативну навігацію та автономію для безпілотних систем у GPS-denied та EW-загрозливих умовах. Компанія створює рішення, здатні працювати там, де звичайна супутникова навігація та візуальні сенсори безсилі — над морем, у тумані, над пустелями та в умовах радіоелектронної боротьби.

Флагманський продукт UAV AirTower, створений у партнерстві з американською компанією Aurelia Aerospace, оснащений модулем Bavovna H-INS — гібридною інерціальною навігаційною системою з точністю до 99,98%, яка не потребує GPS, карт чи камер. Bavovna працює у форматі dual-use, забезпечуючи рішення як для оборонного сектору, так і для цивільних індустрій: логістики, безпеки, інфраструктури та енергетики.

Основні події компанії:

- Bavovna AI став першим українським стартапом, який потрапив до американської військової програми Air Force Labs Masschallenge (програма працює із Defense Tech проєктами, працює при американському Міністерстві оборони та фінансується урядом США).
- Український стартап Bavovna AI оголосив про закриття late-seed раунду фінансування на суму $1,7 млн.
- Bavovna AI виграв спеціальну нагороду «Найкраще інноваційне рішення для БПЛА» на конкурсі EDGE Challenge в Абу-Дабі.

Яке джерело доходу є основним для вашої компанії?

Основним джерелом доходу є продаж навігаційних модулів H-INS та UAV-рішень типу AirTower. Додатково компанія отримує прибуток від програмного забезпечення, інтеграційних проєктів і консалтингу в оборонній та автономній індустріях.

Як ви оцінюєте свій потенціал до зростання в найближчі роки та після завершення війни?

Глобальний тренд на переозброєння створює величезне вікно можливостей: країни оновлюють арсенали, фокусуючись на автономних системах нового покоління. Цей процес триватиме щонайменше 10 років. Bavovna вже інтегрується в ці процеси — ми створюємо системи, які працюють без GPS і готові до майбутніх конфліктів. Після війни технології знайдуть широке застосування в цивільному секторі — агро, логістика, інфраструктура, безпека.

Чим ваші технології можуть бути корисні в цивільному користуванні?

Технології Bavovna можуть використовуватись для інфраструктурного моніторингу, георозвідки, надзвичайних ситуацій і доставки в складних умовах. Окремо ми бачимо перспективу у створенні електронних кордонів. Уже сьогодні тисячі кілометрів українського кордону не мають стабільного GPS-покриття — і це лише питання часу, коли країни масово почнуть використовувати системи постійного контролю повітряного простору. Ми вже працюємо над цим.

Чи планується залучення нових інвестицій?

Після закриття seed-раунду на $2,7 млн у 2024 році, Bavovna отримала активну зацікавленість від венчурних і приватних фондів із США, ЄС і країн Близького Сходу. Наступний раунд планується для масштабування виробництва та сертифікації на нових ринках.

Які події чи зміни останніх років мали найбільший вплив на розвиток компанії? Як компанія адаптується до змін на глобальному ринку?

Найбільший поштовх розвитку дали бойові умови — потреба в GPS-незалежній навігації. Також — глобальний запит на NDAA-сумісні технології, що дозволив увійти на ринок США. Ми адаптувались через партнерства, локалізацію виробництва та відповідність міжнародним стандартам.

Які стратегічні рішення найбільше сприяли зростанню бізнесу?

- партнерство з Aurelia Aerospace для виводу AirTower на ринок;
- власний R&D-центр в Україні;
- фокус на західні ринки та участь у пілотних програмах Міністерства оборони США, Міністерства національної безпеки США та НАТО.

Чим ваші технології можуть бути корисні в цивільному користуванні?

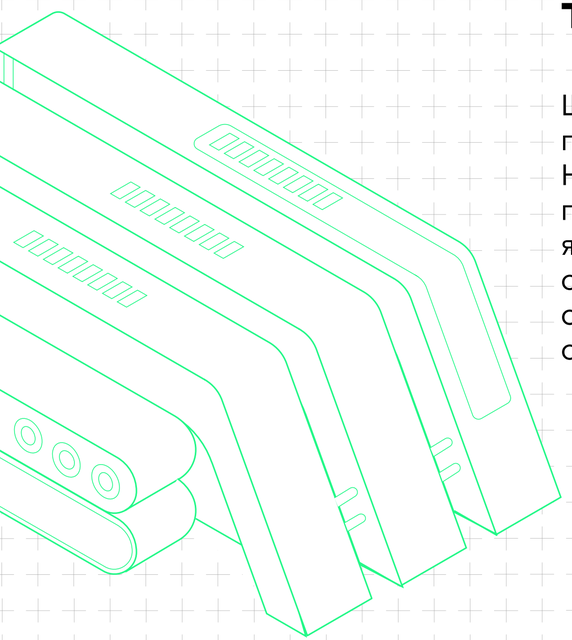
30% нашої команди — військові з бойовим досвідом з різних країн і фахівці з розвідувального співтовариства. Це забезпечує глибоке розуміння реального бою та створює культуру рішучості, мобільності та швидкого ухвалення рішень. Ми працюємо за принципом field-driven R&D — те, що не працює в полі, ми не впроваджуємо.

Що відрізняє вас від конкурентів?

Ми базуємо рішення на тисячах годин польотних логів і досвіді інтеграції з різними платформами. Наша навігація може працювати в морі, тумані, пустелях — там, де інші системи втрачають орієнтацію. Наш головний конкурент — це GPS. Ми прагнемо досягти точності GNSS, залишаючись автономними навіть у найагресивніших середовищах.

ВІД ЗНЕЗБРОЄННЯ ДО СТАНДАРТІВ НАТО. ЯК УКРАЇНА ЦИФРОВІЗУВАЛА ВІЙСЬКОВІ ПОСЛУГИ ТА ПРОЦЕСИ

До російського вторгнення у 2014-му українська армія не була готова. Крім людських ресурсів, бракувало і зброї, щоб вибити російські війська зі Сходу та Півдня.



Ще до розвалу СРСР держава затвердила принцип без'ядерності, вже за часів Незалежності, у 1992-му — ратифікувала Договір про звичайні збройні сили в Європі (ДЗЗСЄ), який обмежував кількість військової техніки та озброєння. Україна позбувалася обороноздатності: літаки, ракетно-артилерійське озброєння експортували або просто списували.

Рідшали і лави ЗСУ, чисельність яких за каденції екпрезидента-втікача Віктора Януковича досягла антирекорду. На кінець 2013-го, напередодні російського вторгнення, у Збройних силах було 165,5 тисяч людей, з них — до 120,9 тисячі військовослужбовців.

Тоді, вочевидь, не йшлося про цифровізацію документів і процесів — насамперед треба було відновити боєздатність армії.

Але вже зараз, на четвертий рік повномасштабної війни з рф, українці оновлюють облікові дані в застосунку «Резерв+», військові подають рапорт на відпустку онлайн в «Армія+», а всі розвіддані доступні в системі DELTA, яку порівнюють з американським Palantir. Диджитал-розробки змінили хід російсько-української війни — велику роль у цьому процесі зіграла робота Міністерства оборони України.

«До повномасштабного вторгнення українці вже звикли до цифрової держави: електронні документи, онлайн-запис до лікаря, швидкі фінансові сервіси, — говорить Олег Берестовий, тодішній керівник IT-департаменту Міноборони. — Повномасштабне вторгнення зробило критично важливими швидкість рішень, реальні дані та зручні інструменти для військових — тож, безумовно, цифровізація оборони пришвидшилась».

МАПА З РОЗВІДДАНИМИ В РЕАЛЬНОМУ ЧАСІ. DELTA

«Україна з меншими витратами створила те, на що Пентагон витратив десятиліття та мільярди доларів», — так у The Wall Street Journal описують систему ситуаційної обізнаності DELTA.

У WSJ відзначають повільність і забюрократизованість західної військової системи для впровадження подібних інноваційних рішень. Перевага України — підхід «знизу-вгору»: військові технології створюють окремі підрозділи чи навіть невійськові експерти, потім розробки впроваджують на загальнодержавному рівні, зазначають у виданні.

Систему DELTA, якою зараз користуються всі рівні Сил оборони, дійсно започаткували люди, частина з яких на той час не була напряму причетна до війська.

Розробляти проєкт, який змінить хід війни, почали у волонтерському об'єднанні «Аеророзвідка». Воно з'явилося в червні 2014-го: тоді прокуратуру анексованого Криму релокували до Києва, частину Луганщини і Донеччини включно з обласними центрами окупували російські війська, за Краматорськ і Слов'янськ точилися бої. До підписання Мінського протоколу, який де-юре мав заморозити війну, залишалося три місяці.

Серед співзасновників «Аеророзвідки» — Натан Хазін, колишній очільник Єврейської сотні Самооборони Майдану, який у квітні 2014-го долучився до ЗСУ. З початку 2014-го, коли росія вже окупувала Крим, він шукав шляхи посилити технічне озброєння армії.

Протягом пів року війни з рф стало зрозуміло, що бракує розвідувальних даних: розуміння, де росіяни розташовують військову техніку, звідки завдають ударів по українських позиціях. Рішенням стали дрони.

«Ми з побратимами знайшли у друзів квадрокоптер Phantom і перепрограмували йому, так би мовити, «мозок», щоб він міг летіти вище і щоб ми бачили, що діється в «зеленці» і по той бік лінії розмежування», — розповідав Хазін. Пізніше в ГО зрозуміли, що легше збирати власні пристрої замість модернування вже наявних.

Взимку 2015-го, коли тривали бої за Донецький аеропорт, учасники «Аеророзвідки» також налагоджували відеоспостереження: встановлювали стаціонарні камери на лінії зіткнення. Цей проєкт отримав назву «Східна брама». Саме команда «Аеророзвідки» першою привезла дрони і стаціонарні камери на поле бою, згадує підполковниця і розробниця DELTA Єлизавета Бойко.

Крім налагодження відеоспостереження, була потреба у швидкому зборі та аналізі даних, якими користувалися 6 Збройні сили для швидшого і більш точного ураження сил ворога.

«Спершу спостерігачі під камерами передавали інформацію по рації. Потім, за запитом 93-ї бригади, ми вивели відео з 5–8 камер на монітори в командному пункті. Це стало справжнім проривом: до того в штабах не було ані екранів, ані комп'ютерів, здатних працювати з відео»,

— розповідає голова ГО «Аеророзвідка» Ярослав Гончар.

Можливості системи оцінили командири, і тоді начальник Генштабу ухвалив рішення створити військову частину, яка розгорне та утримуватиме систему відеоспостереження вздовж усієї лінії фронту, а також розробить систему ситуаційної обізнаності.

Так ГО переросла в окремий підрозділ ЗСУ — А2724, — куди увійшли більшість учасників «Аеророзвідки». У підрозділі було дві команди: одна працювала безпосередньо з дронами, інша — розробляла систему ситуаційної обізнаності DELTA.

DELTA — це диджитал-мапа з багатьох шарів, яка оновлюється в режимі реального часу.

До системи вносять дані про розташування, склад і напрям руху ворожих військ. Ці дані надходять з різних джерел — від авіарозвідки, з супутників, а також через чатботи «єВорог» і Stop Russian War, інтегровані в систему.

Працювати з системою можна з будь-якого пристрою: від смартфона до платшета чи ноутбука.

Функціональність DELTA:

- понад 150 000 паралельних переглядів відеотрансляцій з безпілотників в пунктах управління та на передовій;
- найповніші дані щодо ураженнь ворога;
- можливість ухвалювати рішення завдяки якісним розвідданим з поля бою;
- підтримка в ефективному плануванні місій екіпажів БпЛА в режимі реального часу.
- система щодня підтримує ураження понад 2000 ворожих цілей, за рік — понад пів мільйона.

Перший реліз системи, яку розробляли відповідно до стандартів НАТО, відбувся у квітні 2016-го. Влітку того ж року її випробовували в тодішній зоні АТО — в Часовому Яру, що в Донецькій області.

«Функціонал [DELTA — ред.] мав би продемонструвати військовим, що можна обмінюватися в реальному часі між різними підрозділами, координувати дії та формувати ситуаційну обізнаність», — розповідає Марат Утюшев, один зі співзасновників «Аеророзвідки», колишній очільник Центру інновацій і розвитку оборонних технологій. Цю інституцію як підрозділ Міністерства оборони створили на основі A2724.

З моменту створення DELTA мала недоліки: наприклад, через відсутність шарів дані в системі зливалися в суцільний масив, в якому було складно розібратися. Тож першого потужного впровадження не вийшло, каже Утюшев. Та розробники системи зробили висновки, і до кінця 2017-го – початку 2018-го представили наступну, покращену версію Defense-продукту.

Ще кілька років DELTA залишалася неофіційною допоміжною системою для військових, та за великої війни з росією вона стала геймченджером.

ОБОРОНА КИЄВА ТА ЗНИЩЕННЯ КРЕЙСЕРА «МОСКВА». РОБОТА DELTA ПІД ЧАС ПОВНОМАСШТАБНОГО ВТОРГНЕННЯ. ЛЕГАЛІЗАЦІЯ СИСТЕМИ НА РІВНІ ДЕРЖАВИ

Падіння Києва мало статися «за кілька днів» — такими були мрії та плани рф, яка у 2022-му почала повномасштабну війну. Невтішні прогнози лунали й від західних експертів.

Росія впритул наближалася до української столиці. За чотири дні після вторгнення, 28 лютого, супутник Maxar Technologies зафіксував 64-кілометрову колону російських танків і бронетехніки, яка рухалася з території білорусі в бік Києва.

Взяти Київ військам рф не вдалося ні за «кілька днів», ні за кілька років. Перепоною до оточення української столиці на початку 2022-го для армії рф стали не лише власні логістичні проблеми. Справа в тому, що росія, як і Захід, недооцінила підготовку України до повномасштабного вторгнення. Так, система DELTA, яку вже неодноразово випробовували в бойових умовах, зіграла свою роль у захисті столиці. Так само нею користувалися і під час інших великих військових операцій. Одна з них — знищення ракетний крейсер «Москва»: 14 квітня 2022 року український ракетний комплекс «Нептун» вразив флагман Чорноморського флоту рф.

Система допомогла потопити ще десятки російських кораблів, знищити сотні одиниць важкої військової техніки та тисяч одиниць піхоти рф. Її використовували при деокупації Херсона та звільненні острова Зміїний.

У 2023-му DELTA успішно протестували на щорічних навчаннях НАТО CWIX зі взаємосумісності національних бойових та інформаційних систем із системами і протоколами НАТО.

Українську розробку випробували з 15 системами з 10 країн, включно з трьома системами, розробленими безпосередньо НАТО. Усі тести на взаємосумісність були позитивними.

З серпня 2025-го DELTA офіційно впроваджена на всіх рівнях Сил оборони України. Також, згідно з постановою Кабміну від 2023-го, комплекс може розміщуватися на хмарних ресурсах та/або в центрах обробки даних, що розташовані на території держав — членів НАТО.

«Це перша система в історії країни, яку легалізували за декларативним принципом, фактично за стандартами НАТО: ми пройшли всі security-контролі, незалежний аудит», — розповідає для AIN заступниця міністра оборони з питань цифрового розвитку у 2023–2025 роках Катерина Черногоренко. За потреби Україна через цю систему може обмінюватись даними з партнерами в режимі реального часу.

За словами Черногоренко, сам факт легалізації системи не був самоціллю: насамперед Міноборони мало дати кожному військовому доступ до DELTA та можливість її використовувати.

Легалізації системи передували зміни «нормативки». «Ми ухвалили два закони, зробили окремо постанову Кабміну, підготували необхідну документацію та підписали у Головнокомандувача технічне завдання на DELTA, — розповідає Черногоренко. — Систему, яка жила “партизанським” життям, ми перетворили на легальну, юридично визнану, з реалізованими підходами до безпеки».

ТРІАДА ДЛЯ ПОВНОГО ЦИКЛУ УРАЖЕННЯ ВОРОЖИХ ЦІЛЕЙ. DELTA, AVENGERS І «ВЕЖА»

«Основний тренд сучасної війни — так званий kill chain, або ланцюжок ураження цілі: можливість дуже швидко отримувати розвідувальні дані, підтверджувати їх і так само швидко здійснювати високоточні ураження — у глибині від двох до 30 кілометрів», — розповідає Катерина Черногоренко.

Цю величезну перевагу на полі бою дала DELTA — «цифрова зброя» для українських військових. Водночас бракувало ШІ-системи, яка зможе обробляти величезні масиви зображень і відео.

Над лінією бойового зіткнення висять тисячі безпілотників, які ведуть стрими нон-стоп. Всі ці дані потрібно обробляти, і в експертів це займає тисячі годин, пояснює колишня заступниця голови МО. Щоб пришвидшити цю роботу і зробити її більш якісною, в межах DELTA розробили систему Avengers. За допомогою нейронної мережі розпізнавання вона детектує ворожі об'єкти та класифікує їх за 2,2 секунди з дуже високою точністю.

До системи DELTA також інтегрували модуль «Вежа», який обробляє потік відеоданих у реальному часі з розвідувальних БпЛА. Завдяки цій тріаді — системі ситуаційної обізнаності, «Вежа» і Avengers — українські військові можуть завершити повний цикл ураження цілі за сім хвилин.

ОНОВЛЕННЯ ОБЛІКОВИХ ДАНИХ ОНЛАЙН. ЗАСТОСУНОК РЕЗЕРВ+

Через розв'язану росією війну український уряд запровадив часткову мобілізацію: за два роки — 2014-й і 2015-й — було шість хвиль.

Після третьої хвилі тодішній міністр оборони Степан Полторак зазначив, що військове керівництво припускалося помилок, через які виникали проблеми у ЗСУ, зокрема із забезпеченням військових і їхньою підготовкою до зими. Проблемою залишалися бюрократичні процедури, казав Полторак: «У міністерства було дуже багато дублюючих функцій і нормативної бази, яка не давала швидко ухвалювати рішення».

До повномасштабного вторгнення усі процедури, пов'язані з військовим обліком, були доступні лише офлайн. У зв'язку з цим було чимало неочевидних, на перший погляд, проблем. Наприклад, військовозобов'язані українці, які переїхали з окупованих територій, мали б реєструватися заново за новим місцем проживання. Процес, який мав би бути налагодженим де-юре, де-факто не завжди працював.

У 2014-му, після вторгнення рф на Схід України, мешканець Донецька Петро [ім'я змінено на прохання чоловіка. — ред.] переїхав до Києва. Влаштовуючись на нову роботу, він, за умовою працедавця, мав надати військово-облікові документи — приписне або військовий квиток. Ці документи залишилися в окупованому Донецьку, куди не було можливості повернутися.

«Я телефонував на якусь гарячу лінію, мені сказали, що я приписаний у Маріуполі, і треба туди їхати і розбиратись», — розповідає Петро. Врешті за браком часу він працевлаштувався без військових документів.

Через подібні юридичні нюанси реєстр військовозобов'язаних потребував оновлення, бо чимало українців не оновлювали дані і не ставали на облік. У 2022-му проблема стала критичною.

З повномасштабним вторгненням рф в Україну уряд запровадив загальну мобілізацію. Перші кілька тижнів черги до військкоматів були величезними — і ситуація не змінилася радикально протягом наступних місяців. Тисячі чоловіків мали годинами чекати на можливість оновити військово-облікові дані або знятися з обліку. Це впливало і на загальний процес мобілізації, і на стан економіки: замість можливості долучитися до армії чи працювати в тилу військовозобов'язані витрачали робочий час на черги.

Тоді ключовою задачею Міністерства оборони було налагодити мобілізаційні процеси: зробити так, щоб дані можна було оновити швидко і зручно, як і стати на облік. Найбільш оптимальним варіантом була цифровізація процесів.

Досвід у запуску диджитал-сервісів у Міністерстві оборони мала Катерина Черногоренко. Раніше, протягом роботи в Мінцифри вона успішно реалізувала COVID-сертифікат. Попри скепсис, з яким вона стикнулася, — адже тоді було чимало сумнівів щодо «Дії» та електронних документів загалом — розробка себе виправдала. Кількість користувачів застосунку «Дія» після запуску е-сертифікату зросла з шести до 16 млн.

У вересні 2023-го, в перший місяць на посаді заступниці міністра оборони Черногоренко мала першочергову задачу — розробити зручні е-сервіси для військовозобов'язаних і військовослужбовців. У військовій сфері, де до цього не було культури цифровізації та передумов до таких швидких змін, ця задача була з «зірочкою».

Терміни на запуск застосунку для військовозобов'язаних, який ініціювала Черногоренко, були вкрай стислі. Також новий проєкт, крім полегшення процедури взяття на облік, мав вирішувати також і проблему корупції.

«Більшість послуг, які можна отримати онлайн, нівелюють корупційні ризики», — говорить в коментарі для AIN виконавчий директор BRDO Олексій Дорогань. Він пояснює, що такі послуги, як-от відстрочки через Резерв+, взагалі не передбачають залучення людини, адже оформлюються в автоматичному режимі через взаємодію між державними реєстрами. Відповідно, кожна така відстрочка вже отримується без будь-яких корупційних механізмів, додає Дорогань.

«Мав бути величезний антикорупційний ефект, тому що корупція приносить у державні процеси неефективність, дає сигнал суспільству, що можна не виконувати законодавчі обов'язки», — каже Черногоренко.

Крім неї, над диджитал-продуктом для військовозобов'язаних працював Артем Романюков, голова Директорату цифрової трансформації Міноборони. Цей Директорат відповідає за цифрову трансформацію, інноваційні технології, автоматизацію, інформатизацію в сфері оборони.

Романюков, який має воєнний та IT-бекграунд, з початку своєї каденції в міністерстві окреслив задачу максимум — цифрова армія замість паперової. Так само роботу Директорату запланували структурувати як ефективну IT-компанію, каже він, порівнюючи її з чимось на кшталт департаменту стратегічного планування та юридичним департаментом — два в одному.

«Україна давно в топі цифровізації серед країн світу, але сфера оборони весь цей час була ніби забута і лежала на тому ж рівні, що її лишили у 1980-х. Резерв+ став першим масовим IT-продуктом від Міноборони за понад 30 років цифрової прокрастинації», — каже в коментарі для AIN Романюков.

Щоб реалізувати перший настільки масштабний для Міноборони цифровий продукт, команда мала всього півтора місяця. Застосунок Резерв+ зарелізили в першу ніч набуття чинності закону про мобілізацію — 18 травня 2024 року.

Згідно із законом, громадяни України, які перебувають на військовому обліку, зобов'язані впродовж 60-ти днів уточнити облікові дані (номер телефону, адресу електронної пошти та адресу проживання) до 16 липня включно. У Міноборони планували дати можливість вибору — оновити дані офлайн (у ТЦК чи у ЦНАПах) або онлайн у застосунку.

Як працює Резерв+? Принцип роботи застосунку простий: він дає швидкий доступ людям за їхніми даними в реєстрі «Оберіг».

- Резерв+ — мобільний застосунок, в якому можна уточнювати облікові дані, отримувати відстрочку від мобілізації та її пролонгування.
- Також у застосунку зберігається електронний військово-обліковий документ.
- Користувачі авторизуються через BankID, вказують телефон, адресу проживання та електронну пошту (за бажання).
- За вчасного оновлення даних застосунок показуватиме відповідну позначку.
- У разі невчасного оновлення штраф також можна сплатити онлайн.

У першу добу релізу застосунок не витримував навантаження: через велику кількість охочих оновити облікові дані було багато повідомлень про збої.

Та, за словами Черногоренко, важливою була готовність користувачів почекати, доки Резерв+ відновить коректну роботу: ***«Для мене теж було показово, що люди готові були пробачати такі речі. Ми чесно сказали: не очікували, що українці будуть настільки відповідальними, що в першу ніч релізу, о першій ночі оновлюватимуть свої дані».***

Реалізуючи застосунок, міністерство зобов'язалося нести відповідальність і за його перемоги, і за його падіння, каже вона. Тож комунікація була відкритою і прозорою: не боялися визнати проблеми чи помилки, якщо такі були, паралельно нормалізовували дані в реєстрах, а також працювали над новою функціональністю.

У червні 2024-го в Резерв+ додали електронний військово-обліковий документ. До розробки Постанови КМУ 559, яка, зокрема, прирівняла цей е-документ до паперового, була залучена команда BRDO.

«Електронний документ має таку ж юридичну силу», — пояснює Черногоренко, додаючи: на етапі запровадження стикалися з певним скепсисом від посадових осіб, які могли просили надати паперовий документ. Міноборони відстежувало такі кейси, нагадуючи: е-документ такий само легальний, як і паперовий.

Також у 2024-му завдяки Резерв+ оформлення відстрочки стало простішим: люди з інвалідністю, студенти, аспіранти та докторанти отримали можливість робити це онлайн. На початку 2025-го в застосунок додали опцію електронного направлення на ВЛК, а також автоматичне продовження відстрочок від мобілізації. У липні 2025-го в новій версії застосунку стала доступною можливість сплатити штраф за несвоєчасне уточнення даних.

«Я вважаю, що ми маємо в таких речах, як цифровізація сфери військовозобов'язаних, наслідувати ціннісний принцип. Тому що, якщо держава продовжує бути незручною, незрозумілою, непрозорою, то це поганий вектор», — каже Черногоренко.

За її словами, щоб проводити такі складні проєкти — як з боку розробки, так і з боку законодавчого регулювання — команда має повністю розуміти всі нюанси. Також Черногоренко згадує й іншу суперсилу — здатність думати постійно про свою роботу.

МОЖЛИВІСТЬ ПОДАТИ РАПОРТ ОНЛАЙН І ПЕРСОНАЛІЗОВАНА СИСТЕМА БОНУСІВ. ЗАСТОСУНОК АРМІЯ+

Крім роботи з військовозобов'язаними, Міноборони має другий важливий вектор — покращення послуг для тих, хто захищає країну від сусідньої держави-терориста.

«Довгий час в армії залишався консервативний підхід щодо цифрових документів для військових, це пояснювали міркуваннями безпеки», — розповідає Катерина Черногоренко.

Втім, за її словами, був великий запит на масовий диджитал-продукт для військових. Тож Міністерство почало розробляти застосунок, концепцію якого захистили в міністра оборони та затвердили з президентом.

Тож міністерство почало розробляти застосунок, концепцію якого захистили в міністра оборони та затвердили з президентом. Загалом, крім Міноборони, до розробки долучився Центр масштабування технологічних рішень ГШ. Партнерами виступили Cossack labs, Brdo, Strimco, Splilka, Fedoriv, ISD Group.

«Наші захисники займатимуться службою, а не паперами», — з цими словами 8 червня 2024-го Міноборони представило Армія+.

- Армія+ — застосунок, який є онлайн-посередником у спілкуванні між військовими та командиром.
- У застосунку можна подати рапорт на відпустку, звільнення від виконання службових обов'язків за станом здоров'я, виплату за підписання першого контракту, відпустку після звільнення із полону, фінансову компенсацію, заяву на переведення до іншої бригади тощо. Останньою опцією скористалися 45 000 військових.
- Близько 900 000 військовослужбовців активно користуються Армія+. З них 600 000 використовують застосунок майже щодня.

Як і Резерв+, проєкт реалізували в стислі терміни: за місяць, включно зі змінами нормативно-правових актів — постановою Кабміну, каже Черногоренко.

Опір диджитал-нововведенням на перших етапах був: зокрема, через нерозуміння, як працюватиме застосунок.

«Там вийшла нова програма від Зеленського, називається Армія+. Велике прохання – не заходьте туди, не реєструйтеся, як подавали рапорти паперові, так і будемо. Від цього робота легше не стане», — цей аудіозапис військовослужбовця, який намагається заборонити підлеглим встановлювати застосунок, «завірусився» в соцмережах.

Дисциплінарних стягнень для автора висловлювання не було: натомість в Міноборони вийшли з комунікацією для діловодів у ЗСУ, говорить Черногоренко в коментарі для AIN. Їм більш детально пояснили принципи роботи Армія+, розповіли, як він нормативно регулюється. До розробки законопроєкту № 10062, який передбачав створення застосунку Армія+, також долучалася команда BRDO.

Після пояснень щодо роботи Армія+, каже Черногоренко, кількість реєстрацій в застосунку значно збільшилася.

Через більш ніж рік після запуску сервісів рівень довіри суспільства до них зростає. ***«Все більше людей пересвідчуються, що ці застосунки передусім призначені для швидкого та ефективного надання послуг військовим та військозобов'язаним, а не як інструмент примусу та контролю. Все більше людей використовують Резерв+ для отримання відстрочки, направлення на ВЛК, або для дистанційної швидкої сплати штрафу за адміністративне правопорушення»,*** — коментує Олексій Дорогань, BRDO.

Функціональність. Насамперед в Армія+ хотіли додати рапорти. «Ми провели глибинні інтерв'ю у 63 000 наших військовослужбовців, репрезентативно заміряли, який є запит у армії, і зрозуміли, що рапорти варто впроваджувати першими», — каже Черногоренко.

Команда BRDO була задіяна в підготовці експериментальної постанови, яка запровадила механізм подачі та погодження рапортів на переведення між частинами через Армія+.

Найбільший запит стосувався рапортів, бо на паперову роботу командири часто витрачають більшу частину свого часу, а погодження можуть займати місяці, пояснює Олег Берестовий.

«Ми реалізували електронні рапорти, тепер їх можна подати за кілька хвилин, погодити — за кілька днів. Це дало визначний результат: з серпня 2024 року в системі опрацьовано понад 850 тисяч електронних рапортів», — додає він.

Однією з ключових опцій стало подання рапорту на переведення в іншу військову частину.

- «Рапорти на переведення — це найкраще нововведення цього застосунку, — говорить у коментарі для AIN військовослужбовець Єгор Мороз. До цього, за його словами, звичайному солдату чи навіть молодшому офіцеру потрібно було подавати рапорт командиру взводу, роти чи батальону, самому збирати ці підписи або ж передавати цю задачу командиру. — Тож, як правило, переведення не проводилося, і це було величезним простором для корупції. Ба більше, ці рапорти, доходячи до стройової, могли просто загубитися, і підписи треба було збирати знову».

  Ще однією проблемою переведень офлайн Мороз називає можливість відмови: випадки, коли кадровий центр отримує цей запит, відправляє його до командира військової частини, і той коментує перевод як «недоцільний», не є рідкісними. «Я мав вісім відмов на перевод, з дев'ятої спроби зміг це зробити, — каже військовослужбовець. — Тож ця можливість подавати рапорт онлайн — величезне спрощення життя».

- З плюсів застосунку — зручність написання стандартних рапортів, каже капітан ЗСУ [попросив не називати його імені. — ред.]: «Просто і зрозуміло, що треба вписати, які дані потрібно вказати. Не треба мати папір, ручку. Не треба фізично його носити від метрів до десятків кілометрів».
  Також, за його словами, з переваг є відсутність людського фактору в заповненні форми рапортів: «Написані від руки часто бувають каліграфічно складні, або концептуально не ясно, що людина хоче. Діловоду банально зручніше зручніше слідкувати за статусом поданих рапортів через систему електронного документообігу, а не перебирати купу паперів».
  Зі складностей капітан ЗСУ називає необхідність старших начальників користуватися власним мобільним телефоном для використання застосунку. «На більшості військових об'єктів формально заборонена наявність мобільних телефонів, не кажучи про їх активне використання зі сторонніми програмами авторизації, — пояснює він. — Використання власного телефона в робочих цілях передбачає його перевірку фахівцем кібербезпеки і видалення великої кількості потенційно небезпечних застосунків, абсолютно потрібних і нормальних у повсякденному, не військовому житті. Це власне майно і передбачено винятков зобов'язання мати застосунок і ним користуватися без жодних натяків на амортизацію чи компенсацію».

- «Я вважаю, що проєкт має перспективу для розвитку, але наразі він фактично не дає військовослужбовцям нових можливостей, окрім зменшення бюрократії, пов'язаної з переведенням чи іншими процедурами, — каже Юрій «Мілан» Гаврилишин, начальник рекрутингу 1-го корпусу НГУ «Азов». — Плюс хотілося б бачити у застосунку можливість переведення між ЗСУ та НГУ, а також запровадження спрощеної процедури переведення без погодження командира й інших системних процесів, які могли б реалізовуватися через Армія+. Я б також запропонував додати фактичні опитування щодо актуальної проблематики СЗЧ — зокрема про причини, через які військовослужбовці йдуть у СЗЧ. Крім того, опитування на різні теми, як-от: чи скористалися б ви можливістю один раз на рік здійснити переведення без погодження командира? Це дозволило б зрозуміти, наскільки подібний інструмент був би корисним. Завдяки таким опитуванням ми могли б отримувати реальні кількісні й якісні дані про існуючі проблеми та шляхи їхнього вирішення».

Крім функціональності для робочих процесів, у Міністерстві оборони запланували інтегрувати в застосунок інші корисні сервіси для військових — зокрема певні бенефіти. Так в Армія+ з'явилася програма «Плюси». До розробки функціоналу знижок та безоплатних сервісів від соціально відповідальних бізнесів для військовослужбовців долучалася команда BRDO.

Серед пропозицій у «Плюсах» — квитки зі спецрезерву в «Укрзалізниці». «Це важлива опція для військових: щоб вони могли викупити квитки, плануючи поїздку додому або повертаючись на службу, — каже Черногоренко. — Тому Міноборони з Укрзалізницею швидко зробили проєкт, який давав можливість через Армія+ отримувати доступ до цього пріоритету».

Військовослужбовець Єгор Мороз каже, що опція придбати пріоритетні квитки — одна з найбільш популярних серед його побратимів, особливо в період відпусток, коли квитки не вдається вчасно купити через «перекупів»: «Це порятунок для тих, хто їде далеко, припустимо, з Донбасу на Захід».

Серед інших бонусів:

- Знижки на пальне від АЗК «Укрнафта», WOG, ОККО.
- Знижки на відправлення посилок від «Нової пошти» — раз на місяць за ціною до 30 кг за 1 гривню.
- Мережа кінотеатрів Multiplex — два промокоди на місяць, завдяки кожному з них можна купити квиток в кіно за 60 гривень.
- «Армія+ користуюсь за необхідністю, зазвичай це 3–5 разів на місяць, — військовослужбовець ЗСУ [просив не називати імені. — ред.]. — Використовую можливість отримувати знижки на пальне через застосунок. Рапорти через Армія+ в рази спрощують роботу і це значно економить час на їх підписання. Але повністю папери застосунок не замінив: не на всі потреби є зразки».
- «Ставлюся до Армія+ позитивно, але рапортами користувався тільки в тестовому режимі. Багато вищих посадовців не вміють ними користуватися, тому паперовий рапорт досі база. Але бонусами [програма “Плюси”. — ред.] користуюся регулярно, — каже військовослужбовець ЗСУ Тимофій. — Проходив опитування щодо того, щоб додати в Армія+ можливість замовляти речове забезпечення та/або отримувати гроші на руки. Рапорт на оздоровчі (13-та зарплата) в мене через Армія+. І це дуже на руку, бо його [рапорт. — ред.] писали, коли я був у відпустці, а кожен день затримки — затримка виплати. А так я зробив це в декілька тапів, дистанційно, за хвилину-дві».
- «Використовую в основному “Плюси” на заправці [для отримання знижок на пальне. — ред.] і рапорт на відпустку одного разу писав. В цьому плані, звісно, простіше [порівняно з паперовими рапортами. — ред.]: пара натискань — і рапорт готовий», — військовослужбовець ЗСУ (попросив не називати імені).
- «Найзручніше [в застосунку Армія+. — ред.] — це “Плюси”, використовував відправлення “Новою поштою” за 1 грн, також популярне бронювання квитків на потяг для військових», — військовослужбовець ЗСУ Богдан.
- «З рапортів зазвичай використовую лише рапорти на відпустку, але, наскільки я знаю, потім все одно роблять паперову копію з цього рапорту, — Артемій, військовослужбовець ЗСУ. — Часто користуюся “Плюсами”: купую квитки на потяг день в день, отримую знижки на заправках і в кінотеатрах, що дуже економно».

З 2024-го до застосунку почали інтегрувати навчальні курси, які також зберігатимуться в ньому. Серед модулів — базова кібербезпека на війні, основи БпЛА, уроки виживання у складних польових умовах, курс з DELTA, курс з проведення закупівель тощо.

Зараз у застосунку дванадцять освітніх курсів, які 90 000 військових уже їх проходять, а 36 000 — завершили хоча б один курс повністю.

«Саме за запитом військових ми запустили в Армія+ відеокурс “Основи БпЛА”, і він швидко став найпопулярнішим: його обирають майже вдвічі частіше серед усіх доступних у застосунку», — коментує Олег Берестовий.

Онлайн-навчання стане в пригоді особливо тим, хто проходить БЗВП, каже Єгор Мороз: ***«Моїм побратимам, які були не в темі БпЛА, наземних роботизованих комплексів, курс в Армія+ допоміг освоїти ази. У планах самого військовослужбовця — пройти курси з англійської та навчання з дронів».***

Обмежень за часом проходження курсів немає, також їх можна скачати на телефон і проходити офлайн. Це зручно, пояснює Єгор, адже військові часто перебувають в місцях, де взагалі немає доступу до інтернету.

Один з популярних курсів у застосунку — «Побут в польових умовах». Його авторка — Олена Риж, бойова медикиня та інструкторка з такмеду в штурмовому підрозділі.

Ініціатива створення такого курсу, за словами Олени, належала команді Армія+.

«Курс буде корисним радше новачкам або тим, хто з небойового підрозділу переходить у бойовий», — пояснює Риж, додаючи: для досвідчених бійців у модулі можуть бути хіба точкові новинки.

До Резерв+ і Армія+ Міністерство оборони не мало експертизи щодо реалізації подібних великих і складних проєктів, розповідає Черногоренко: ***«Була проведена велика робота з Генштабом, бригадами, безпосередньо користувачами».*** Завдяки таким проєктам Україна стає трендсеттером в оборонній сфері для інших країн, каже вона. Наприклад, Німеччина планує запустити власний аналог Резерв+.

Запуск цих проєктів змінив буквально все в галузі, каже Артем Романюков: ***«В один момент Міноборони з цифрового динозавра перетворилося на спроможну IT-команду, яку так і стали сприймати».***

За його словами, тепер нормативні зміни, які супроводжують запуск будь-якої нової цифрової ініціативи, стали даватися легше: ***«Спротив був і буде завжди, адже все нове завжди лякає. Але ми вже навчилися розмовляти з нашими партнерами зі Збройних сил, Генштабу і трансформуватися разом».***

«Ми прагнемо, щоб для військових “Армія+” став корисним застосунком на кожен день — зручним інструментом, який покриває всі основні потреби, пов’язані з кар’єрою, здоров’ям, виплатами, навчанням, швидким зворотним зв’язком тощо, — окреслює він цілі застосунку. — ***Це має бути сервіс, з яким військовий взаємодіє регулярно, і який справді полегшує життя під час служби».***

Наступний крок — запровадити в застосунок функцію «Відгук», яка дасть можливість військовим напряму повідомляти виробників про проблеми з технікою та пропонувати апгрейди. За словами Берестового, така опція дозволить швидше вдосконалювати обладнання й дасть українській армії додаткову технологічну перевагу.

Також Міністерство оборони поглиблює співпрацю з Генеральним штабом ЗСУ. У межах цієї співпраці впровадять єдину IT-вертикаль для системного розвитку цифрових рішень. Це працюватиме таким чином: у кожному підрозділі з’являться цифрові офіцери та команди, які передаватимуть фідбек і допомагатимуть поширювати і покращувати системи, пояснює Берестовий.

ЦИФРОВІ ПРОДУКТИ МІНІСТЕРСТВА ОБОРОНИ: РЕЗУЛЬТАТИ

Застосунок	Коли запустили	Користувачі	Послуги
Резерв+	18 травня 2024 року	понад 4,5 млн	• е-документ для військового обліку — згенерували понад 4,5 млн користувачів; • можливість виправляти помилки у персональних даних; • онлайн-рекрутинг із вакансіями у війську: понад 10 000 позицій і понад 135 тисяч заявок; • електронні направлення на ВЛК без візитів до ТЦК — понад 200 000 згенеровано; • п'ять типів відстрочок онлайн — кожну третю відстрочку оформлюють у застосунку; • дев'ять видів штрафів за порушення правил військового обліку.
Армія+	8 серпня 2024 року	понад 800 тисяч	• доступні 42 типи рапортів, користувачі подали понад 850 000; • понад 47 000 військових змогли перевестися в інші підрозділи; • 13 навчальних відеокурсів, понад 120 000 військових проходять навчання, 52 000 — завершили хоча б один курс; • 18 опитувань для військових, зібрано понад 400 000 відповідей; • програма «Плюси» (знижки на пальне, доставку через НП, придбання техніки на Rozetka тощо): скористалися понад 4,2 млн разів, заощадили понад 334 млн грн на пальному та доставці, придбали понад 89 000 залізничних квитків зі спецрезерву, 61 000 разів поділились «Плюсами» з рідними.

МАСШТАБНА ЦИФРОВІЗАЦІЯ. ЄДИНИЙ ДЕРЖАВНИЙ РЕЄСТР ВІЙСЬКОВОСЛУЖБОВЦІВ

У 2025-му Верховна Рада України ухвалила оновлений законопроєкт щодо створення Єдиного державного реєстру військовослужбовців (ЄДРВС).

Завдяки реєстру військовослужбовці матимуть швидкий, зручний і прозорий доступ до державних послуг. Також ЄДРВС має підвищити ефективність управлінських рішень у Генштабі та Міноборони.

Працювати з реєстром розпочали ще у 2024-му, цей проєкт був дуже складний саме в нормативному регулюванні, розповідає Артем Романюков: «Реєстр потребував змін до законів, які ми змогли провести, на жаль, не з першого разу. Тому довелося добряче попрацювати вже навіть над легалізацією цих змін».

Попереду — технічна розробка, яка триває: над нею працює архітектурна, технічна, нормативна команда. Головна особливість — в чутливості інформації та технічних трюках, щоб максимально убезпечити дані, які не мають потрапити до ворога.

Важливо підкреслити, що ЄДРВС — не «срібна куля», пояснює Романюков: «Не треба думати, що після його запуску одразу відбудеться магія і згорять всі журнали обліку журналів обліку. Ми, звісно, від них позбудемося, але в результаті впровадження цілого комплексу систем, серед яких і реєстр, і декілька систем обліку, які будуть пов'язані в гарну архітектурну конструкцію, яка вивільнить справжній потенціал цифровізації у сфері оборони».

На питання, за який період можливо цифровізувати більшість процесів у Міноборони, Романюков відповідає — можливо, це десятки років. Водночас зміни, над якими працюють у міністерстві, відчуватимуться щокварталу.

«У нас стояла і стоїть задача робити речі за межами можливого, — каже він. — ***Власне, українці це роблять постійно з лютого 2022-го на полі бою. А ми намагаємося робити в цифровій сфері».***

За його словами, в Директораті, як і в Міноборони загалом, над рішеннями працюють дуже й дуже багато. «Особисто я приїжджаю в офіс о 7 ранку, а виходжу не раніше за 21:00, — зізнається Романюков, додаючи: якби не необхідність спати, працював би і більше. — Я вірю в те, що ми робимо, і хочу встигнути якомога більше».

На сьогоднішній день досягти повної автоматизації щодо всіх послуг поки не вдалося, каже Олексій Дорогань, BRDO:
«Досі залишаються відстрочки, які складно оцифрувати, адже потрібна для них інформація ніде не оцифрована, однак робота в цьому напрямку ведеться. Амбітна ціль – максимально виключити людський фактор з процесів ухвалення рішень та перевести всі функції в онлайн», — пояснює він.

КІБЕРБЕЗПЕКА. ЯК ЗАХИЩАЮТЬ ДАНІ В РЕЗЕРВ+ ТА АРМІЯ+

Війна з росією триває і в кіберпросторі, тому кібербезпеці в Міністерстві оборони приділяють максимальну увагу, каже Олег Берестовий.

Ворог регулярно запускає інформаційні атаки, поширює клони застосунків, підроблені фішингові сайти, неправдиву інформацію про нібито «злами», розповідає він. У Міноборони на такі дії рф реагують оперативно: ліквідують підробки, перевіряють системи, а також пояснюють користувачам і партнерам, як саме побудована архітектура захисту.

Також в Міністерстві оперативно публікують спростування російських фейків, наприклад, про нібито незаконний збір даних українців через Резерв+. Насправді застосунок не відстежує геолокацію користувачів і не має доступу до GPS, працюючи лише з інформацією, якою користувачі діляться через BankID, та з даними з реєстру «Оберіг».

«Обидва застосунки, Армія+ та Резерв+, пройшли всі необхідні перевірки й отримали атестати відповідності комплексної системи захисту інформації (КСЗІ)», — каже Берестовий. Персональні дані на серверній частині не зберігаються: вся інформація передається лише в зашифрованому вигляді, а серверні потужності розгорнуті в захищеній хмарній інфраструктурі в Україні, яка має сертифікати безпеки відповідно до законодавства.

«Це означає, що навіть у разі спроби атаки дані користувачів залишаються захищеними», — пояснює він.

Доступ до Єдиного державного реєстру призовників, військовозобов'язаних та резервістів, із якого підтягує інформацію Резерв+, мають лише визначені законом суб'єкти: Міністерство оборони, Генеральний штаб ЗСУ, СБУ, Служба зовнішньої розвідки, ТЦК та СП, говорить Берестовий. Облікові дані можуть змінювати винятково уповноважені працівники районних ТЦК та СП. Також кожну зміну підтверджують особистим електронним ключем оператора.

Про безпеку застосунків дбає Центр реагування на кіберінциденти при Міністерстві оборони. Фахівці центру працюють 24 на 7: захищають IT-інфраструктуру Сил оборони України, моніторять ситуацію, попереджають будь-які кіберзагрози, прогнозують атаки та формують стратегії кіберзахисту.

DUAL USE, АБО ЯК ТРАНСФОРМУЮТЬСЯ ЗАСТОСУНКИ ПІСЛЯ ПОВНОМАСШТАБНОГО ВТОРГНЕННЯ

Армія+ і Резерв+ були б потрібні і без повномасштабної війни, говорить Олег Берестовий. За його словами, держава все одно мала б цифровізувати кадрові й тилові процеси — особові справи, довідки, рапорти, навчання, оформлення відпусток і виплат для військових, сервісну взаємодію з громадянами, управління мобілізацією тощо: різниця була б лише у швидкості та пріоритетах релізів.

Сервіси будуть у пригоді і після завершення війни, говорить Олексій Дорогань, BRDO. За його словами, в довгостроковій перспективі екосистема Резерв+ та Армія + перетвориться на середовище «Цифровий ТЦК», що буде надавати послуги військовозобов'язаним, військовослужбовцям та членам їхніх родин швидко, зручно та без участі людей.
«Це буде актуально, адже велика кількість послуг для військовослужбовців мають соціальний характер і спрямовані не тільки на військовозобовязаних, але і на військовослужбовців та членів їх сімей», — пояснює він.

ДИДЖИТАЛІЗАЦІЯ, ЯКА ЗМІНИЛА ВІДНОСИНИ УКРАЇНИ З НАТО. ЯК ІНШІ КРАЇНИ ОРІЄНТУЮТЬСЯ НА УКРАЇНСЬКІ РОЗРОБКИ

У травні 2025-го Україна та НАТО підписали ліцензійну угоду на використання некомерційного програмного забезпечення — Системного інтерфейсу Центру управління й оповіщення (CRC System Interface, CSI). Це перша такого масштабу угода з Альянсом, каже Черногоренко, додаючи: фактично Україна відкрила шлях до спільних операцій українських Повітряних сил і країн НАТО.

За словами Черногоренко, такі проєкти доводять: інтеграція в НАТО можлива ще до офіційного членства, ба більше, успішні домовленості закладають фундамент для можливого входження в Альянс.

За словами екзаступниці міністра оборони, українці за роки повномасштабної війни довели свою професійність на полі бою, швидко опанувавши передану зброю та технології, і західні країни це відзначають.

«Водночас можу констатувати, що ми привнесли неймовірну експертизу в НАТО як альянс, де народжуються найкращі військові доктрини та практики», — каже Черногоренко. З цим погоджується Романюков, констатуючи: український досвід активно переймають в інших країнах.

Наприклад, проєкт «Армія дронів» і масштабні операції на території ворога, як-от «Павутина», вплинули на підхід до оборони у Сполучених Штатах. У червні 2025-го президент США Дональд Трамп підписав укази щодо посилення можливостей США у сфері безпілотників.

Так само Європейський Союз запускає великий процес із переозброєння армії, переосмислює підходи до воєнного навчання, додає Черногоренко, додаючи: Україна задає високі Defense-стандарти для партнерів.

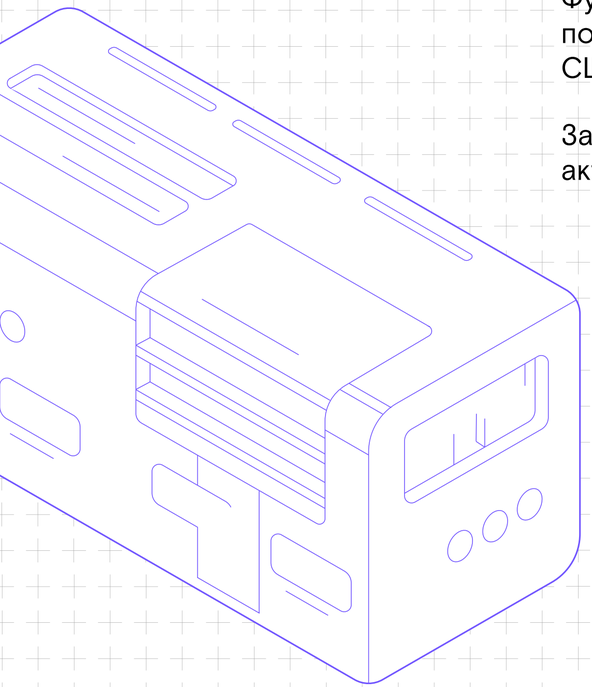
Інші країни також втілюють у мобільних застосунках окремі послуги для військових і військовозобов'язаних, розповідає Олег Берестовий. Як приклад наводить Ізраїль, який має застосунок з новинами і медіаконтентом Армії оборони, доступний і для військових, і для широкого загалу.

Також, говорить він, Пентагон створив My Military OneSource для військових та їхніх родин — з довідниками, інформацією про пільги, службою психологічної й побутової підтримки. Міністерство оборони Південної Кореї Міноборони спільно з приватною IT-компанією запустили для військових та їхніх родин застосунок The Camp: в ньому користувачі мають доступ до актуальної інформації про службу, новин армії, онлайн-магазину, можуть надсилати захисникам і захисницям листи підтримки.

«Проте наразі немає жодної платформи, навіть приблизно схожої на Армія+ та Резерв+ за викликами й масштабами», — каже Берестовий. Саме тому, за його словами, все більше країн активно цікавляться українськими розробками.

Особливо за досягненнями української Defense-галузі слідкують країни Європи, оскільки перед ними зараз стоїть багато викликів, пов'язаних із обороною та потенційною військовою агресією. ***«Основні напрями, де вони бачать застосування цифрових рішень, — це рекрутинг і мобілізація — і нам дійсно є що запропонувати»,*** — підсумовує він.

ПОРІВНЯННЯ УКРАЇНСЬКОГО DEFENSE TECH З ІНОЗЕМНИМ: ЯКІСТЬ, ВИПРОБУВАННЯ, ІНВЕСТИЦІЇ, ДЕРЖАВНІ ТА ПРИВАТНІ ЗАКУПІВЛІ РОЗРОБОК



«Чи зберігає досі концепція “Заходу” сенс у першому десятилітті XXI сторіччя?»,

— запитував американський політолог Френсіс Фукуяма у 2002 році, коли чимало європейських політиків критикували близькосхідну політику США.

За ери Трампа це питання все ще залишається актуальним — остаточної відповіді наразі немає.

Екосистеми США та ЄС є вкрай відмінними. «Це два різних світи, серйозно», — говорить у коментарі AIN Tic Клінкхамер, аналітик венчурного фонду з Нідерландів Keen Venture Partners.

■ Порівняння українського Defense Tech з іноземним

ЄВРОПА І США: КАПІТАЛ

Саме це демонструють дані щодо насичення цих екосистем капіталом:

Рік	Проінвестовано в Defense Tech стартапи в Європі, млн доларів	Проінвестовано в Defense Tech стартапи в США, млн доларів
2019	37	700
2020	52,9	2700
2021	141,6	2900
2022	49,7	4500
2023	302,2	2200
2024	625,9	2500
2019–2024	1209,3	15500

Джерело: Crunchbase

■ Порівняння українського Defense Tech з іноземним

Тобто за останні п’ять років у європейські стартапи було проінвестовано у 12 разів менше ніж ті, що базуються в США. Станом на 2024 рік Міжнародний валютний фонд оцінює валовий внутрішній продукт ЄС у $29 трильйонів, а ВВП США — у $29,1 трильйона. Які ключові фактори призводять до того, що в економіках схожого розміру настільки відмінна інвестиційна динаміка щодо Defense Tech ніші?

Протягом останніх 30 років європейські державні та приватні гравці загалом мало інвестували в оборону. Аналітичний центра Agenda Austria підрахував, що у 2023 році видатки західноєвропейських членів НАТО були на приблизно тому ж рівні, що і в 1990 році. Натомість фінансування освіти було на 75% більшим, а інші соціальні видатки збільшилися у понад два рази.

Оборонні бюджеті США, згідно з розрахунками Стокгольмського інституту дослідження проблем миру, щороку, починаючи з 2004-го, перевищують рівень 1990 року.

«Внаслідок цього європейська оборонна промисловість пережила щонайменше два десятиліття зменшення державних замовлень, а американська промисловість це менше відчула на собі», — говорить у коментарі AIN Маттіас Лена, Director of Business Development & Government Relations у німецькому скейлапі Quantum Systems. Проте це далеко не єдина проблема європейської Defense Tech екосистеми.

Лена називає інший фактор який уповільнює розвиток: «Європейський оборонний ринок фрагментований, адже в кожної країни свої «локальні чемпіони», тобто найбільші оборонні підприємства. Кожна держава хоче створити такі умови, які виведуть ці підприємства на найвищий рівень, зокрема спрямовуючи державні оборонні видатки саме таким компаніям, а не іноземним виробникам».

■ Порівняння українського Defense Tech з іноземним

Іншими словами, євроінтеграційні процеси, які тривають понад 70 років, майже не вплинули на цю галузь. «Головна різниця між США і ЄС полягає саме у фрагментованості європейського ринку», — погоджується Тіс Клінкхамер, аналітик з Keen Venture Partners.

Ця нідерландська венчурна компанія наразі збирає 125 мільйонів євро для фонду, який буде присвячено суто інноваціям у сфері безпеки та оборони. У такий спосіб Keen Venture Partners хочуть вплинути на іншу ключову відмінність: меншу концентрацію європейського приватного капіталу. Це стосується не лише інвестицій у Defense Tech стартапи.

«У США загалом приватні інвестори є більш активними в усіх сферах», — пояснює Лена з Quantum Systems. Водночас він зауважує, що Європа не є гомогенною: у Великій Британії приватні інвестори активніше вкладають Defense Tech галузь, натомість «як у Німеччині, так і у Франції ринки капіталу є доволі консервативними». Навіть коли окремі фонди-«жайворонки» розглядають інвестиції в оборонний стартап, то стикаються з багатьма обмеженнями на нормативному рівні. «Проте це зараз змінюється», — каже Director of Business Development німецького скейлапу.

Зміни на регуляторному рівні відбуваються паралельно з трансформаціями уявлень приватного капіталу про доцільність інвестицій у Defense Tech. Німецька венчурна компанія Project A підрахувала, що за останній рік кількість зацікавлених у європейському Resilience Tech та Defense Tech виросла втричі.

Рік	2024	2025
Кількість венчурних компаній, зацікавлених в європейському Resilience Tech та Defense Tech	44	127

Джерело: Project A

■ Порівняння українського Defense Tech з іноземним

Проте це не означає, що всі ці 127 компаній вже проінвестували в європейські стартапи. У коментарі AIN німецький венчур пояснив, що у свій перелік вони також включали компанії, які «активні в екосистемі, наприклад, беручи участь у релеватних подіях» і підтримують Resilience Tech та Defense Tech стартапи, хоч досі в них і не вклалися.

Цю ж тенденцію підтверджує в коментарі AIN співзасновник венчурної компанії «Sunfish Partners» Маркус Еркен: так, дійсно, про оборонні технології частіше говорять у середовищі європейського венчурного капіталу. Його компанія три роки регулярно бере участь у заходах, що стосуються аеронавтики та оборони, і вже має відповідні стартапи у своєму портфоліо. Попри це Еркен відзначає, що не варто поспішати з висновками щодо того, наскільки збільшаться обсяги інвестицій в європейські оборонні стартапи: «Наразі це все ще не до кінця зрозуміло».

Іншими словами, найбільша проблема полягає навіть не у відсутності інтересу, а у тому, що він не сягає фондів із найбільшим капіталом. «Все ще складно отримати більше фінансування, необхідне для пізніх етапів у розвитку стартапу», — говорить Янік Майєр, Investment Associate у Project A.

Цю тезу поділяє аналітик Keen Venture Partners Тіс Клінкхамер: «Дві третини капіталу, які європейські Defense Tech стартапи залучають на пізніх етапах, мають американське походження». Така ситуація може мати негативні стратегічні наслідки. Клінкхамер розповідає, що досить часто засновники європейських стартапів отримують пропозиції щодо інвестицій за умови переїзду в США.

■ Порівняння українського Defense Tech з іноземним

ЄВРОПА І США: ЛЮДИ

Такий відтік людей і стартапів може поглибити вже наявну тенденцію на європейському ринку щодо дефіциту талантів, необхідних для розвитку європейських Defense Tech стартапів. Часто молоді європейці з високоспеціалізованою освітою надають перевагу роботі на американських технологічних гігантів.

Візьмемо, наприклад, француза Поля Муст'єра. У 2017 році він завершив здобуття магістерського ступеня з прикладної математики в École des Mines de Paris. Стажувався в Університеті Каліфорнії, проте академічна дослідницька робота йому не сподобалася: «Усе відбувалося занадто повільно», — розповідає він AIN.

Тоді Муст'єрє приєднався до американського Palantir, одного із найбільших Defense Tech стартапів світу. Palantir працює з великою кількістю американських державних організацій, проте вісім наступних років роботи у Palantir Мустер'є здебільшого стикався з європейськими клієнтами, від Airbus до служб охорони здоров'я. Так чи інакше, більшість акціонерів компанії становлять резиденти США. Крім того, кілька колишніх працівників Palantir приєдналися до адміністрації американського президента Дональда Трампа.

Мустер'є помітив, що після президентських виборів у США у 2024 році компанія почала змінюватися. Йому подобалося, що раніше Palantir розповідала працівникам про те, над якими державними проєктами вони працюють. Згодом таких комунікацій «почало ставати менше, аж поки вони геть не зупинилися», — говорить він.

Крім того, Мустер'є почав бачити більше колонок і виступів на телебаченні керівництва компанії, зі змістом яких він не погоджувався. «Мені байдуже, які в них політичні погляди, вони мають право на них, проте мені не байдуже, коли вони це роблять від імені компанії», — розповів інженер у коментарі AIN. Тоді він почав шукати іншу роботу і в квітні 2025 року приєднався до французького стартапу Comand AI, який використовує штучний інтелект для пришвидшення ухвалення рішень на полі бою.

■ Порівняння українського Defense Tech з іноземним

Нова адміністрація в США не вплинула на роботу Palantir в Україні, заявив віцепрезидент Palantir у Великій Британії та Європі Луїс Моузлі. Ця співпраця включає як військових клієнтів, так і цивільних. Comand AI співпрацює з українською геоінформаційною платформою Griselda. Мустер'є знав про роботу Comand AI в Україні, і це було «позитивним фактором» для нього під час ухвалення рішення про наступне місце роботи.

Чи підштовхне політика США інших інженерів з ЄС приєднуватися до європейських, а не американських стартапів? Чи історія Мустер'є лишиться доволі унікальною? Час покаже, проте 13 країн-членів ЄС закликали Європейську комісію до того, аби запросити в Європу «блискучих талантів з-за кордону, які можуть страждати від втручання в дослідження та невмотивованих і жорстоких скорочень фінансування».

Натомість Еркен з Sunfish Partners закликає не забувати, що, попри всі розбіжності з ЄС, навряд чи вдасться знайти кращого за США партнера, тому слід прагнути реалістичних компромісів. До того ж перехоплення талановитих кадрів з американської екосистеми є далеко не єдиним джерелом для поповнення рядів європейського Defense Tech. Також є потенціал до зростання завдяки збільшенню інтересу до оборонних стартапів з боку європейської молоді.

«Мені видається, що молодші люди завжди більш зацікавлені в технологічних інноваціях», — каже Маттіас Лена, Director of Business Development & Government Relations у Quantum Systems. Він бере до рук смартфон і питає: «Коли востаннє були по-справжньому проривні інновації у сфері смартфонів?». І тут же відповідає: «Років 10 тому». Натомість саме у сфері оборонних технологій зараз відбувається найбільший розвиток, підсумовує Лена.

■ Порівняння українського Defense Tech з іноземним

ЄВРОПА І США: СУСПІЛЬСТВА

Згідно з дослідженням Центру військової історії та соціальних наук ЗС Німеччини, станом на літо 2024 року більша половина німців віком від 16 до 29 років вважала відновлення строкової служби занадто великим обмеженням їхньої свободи. Зрештою, у США ситуація подібна: частка людей, яка заявляє в опитуваннях про своє бажання обороняти країну, зменшується останні 30 років; молодші люди менш схильні обирати цей варіант.

Проте це ще не означає, що молоді люди у заможних країнах не мають жодного бажання робити свій внесок в протистояння загрозам. Восени 2024 року 80% опитаних соціологічним агентством Forsa німців такої ж вікової групи були готові особисто докладатися до незбройних форм підтримки безпеки суспільства. Робота в європейському Defense Tech можете стати альтернативою для тих молодих європейців, які розуміють загрози Європі, проте не готові долучатися до оборони в іншій спосіб.

Зрештою, уявлення можуть змінюватися, і подекуди ці процеси в Європі лиш починаються. Наприклад, коли Мустер'є оголосив своїй родині, що переходить у Comand AI, його молодший брат зреагував критично, мовляв, «якщо це співпраця з державою, то це погано за визначенням, байдуже, про що там конкретно ідеться». А коли Клінкхамер звернув увагу засновника одного європейського стартапу на те, що його продукт може бути корисним не лише для цивільних клієнтів, то отримав доволі неочікувану відповідь: «Він сказав, що йому страшно заходити в оборонний ринок». Клінкхамер переконаний, що цей острах спричинений недостатньою поінформованістю щодо різноманітних регуляторних норм.

■ Порівняння українського Defense Tech з іноземним

Не лише він відчуває дефіцит інформації. «Якщо у США Defense Tech має майже власний медійний сегмент, то в Європі, а особливо в німецькомовній її частині, ця тема недостатньо висвітлена», — сказав у коментарі AIN докторант університету Збройних Сил ФРН Йонас Зінгер.

Тому він створив власний подкаст, у якому обговорює оборонні інновації як з військовослужбовцями чи дослідниками, так із засновниками стартапів та інвесторами. Проте слухають його не лише люди, які вже долучені до екосистеми. «Кілька студентів та засновників стартапів на ранніх стадіях писали, що подкаст надихнув їх придивитися до оборонних інновацій», — розповідає Йонас.

Інтерес до його подкасту зріс після Мюнхенської безпекової конференції у лютому 2025 року. Те саме сталося і з розсилкою European Resilience Newsletter, яку випускає Project A. Згідно з підрахунками SimilarWeb, кількість переглядів Resilience Media, створеного для висвітлення європейського Defense Tech, потроїлася у березні, порівняно з лютим.

■ Порівняння українського Defense Tech з іноземним

ІНОЗЕМНИЙ DEFENSE TECH В УКРАЇНІ

Достатньо завітати на одну з багатьох подій, що присвячені оборонним інноваціям та відбуваються в Києві, аби побачити скільки іноземних компаній шукають клієнтів.

«Зараз Європа неймовірно багато вчиться в України, зокрема у сферах суспільної стійкості, цифровізації, обороноздатності», — говорить Маттіас Лена з Quantum Systems. Часто більшу частину учасників становлять європейці, оскільки за відсутності авіаційного сполучення будь-яка подорож зі США в Україну займає доволі багато часу. Тож йому здається, що «тут у країн-членів ЄС є стратегічна перевага».

Цією перевагою користуються. Наприклад, група підприємців, інженерів та інвесторів Darkstar Coalition регулярно проводить буткемпи в Україні, метою яких є познайомити європейські стартапи з українськими реаліями. Так, під час останнього заходу стартапи з Естонії, Польщі, Німеччини та Канади мали змогу протестувати свої вироби на українському полігоні, поспілкуватися з українськими військовослужбовцями, які впроваджують інновації у своїх підрозділах, та познайомити з потенційними українськими стартапами-партнерами. Коаліція також проводить хакатони, під час яких європейські інженери шукають рішення для українських проблем.

Рагнар Саас, естонський підприємець і засновник Darkstar Camp, у розмові з AIN зазначає, що Україна має найбільшу екосистему оборонних стартапів у світі, понад 2000 компаній — тоді як усі скандинавські країни сукупно мають менше ніж 200.

«Найбільша проблема наразі — це конкуренція на українському ринку. Наприклад, у сфері дронів чи ШІ для військових продуктів багато, компанії мають схожі ідеї. Крім того, вони повинні адаптуватися до ринку НАТО. У майбутньому, навіть після війни, їм потрібно працювати з багатьма країнами, щоб уникнути залежності від однієї. Але Україна точно має потенціал стати ключовим гравцем на ринку технологій для боротьби з FPV-дронами, які стають найбільш викликом для глобальної безпеки», — впевнений він.

Але Darkstar — не єдиний гравець Defense Tech екосистеми Європи, який організовує подібні заходи. На таких подіях спеціалізується European Defense Tech Hub. Ініціатива розповіла AIN, що за 2024 рік їй вдалося залучити понад 400 учасників до своїх заходів. Вони розв'язували проблеми з реального світу, сформульовані на основі досвіду України та НАТО, такі як виявлення безпілотників або навігація без застосування супутників. European Defense Tech Hub уже провів свій перший хакатон у Львові навесні поточного року і планує організувати ще й у Києві восени 2025.

Далеко не всі європейські ранні стартапи чи більш зрілі компанії, які побувають в Україні на виставці, форумі чи хакатоні, дійдуть до своїх перших замовлень. Проте це можливо, і Quantum Systems тому приклад. Німецька компанія працює в Україні з 2022 року, локалізувала виробництво, постачає своїх безпілотники за замовленням Міністерства оборони України, а її дочірня українська компанія задекларувала у 2024 році 92 млн гривень доходу.

Які складові були необхідними для такого результату? ***«Сміливість, гнучкість та, до певної міри, інтуїція»,*** — відповідає Маттіас Лена, Director ead of Business Development & Government Relations компанії.

Водночас ці компоненти мають бути частиною більшої стратегії, спрямованої на локалізацію. «Необхідні українські партнери, які розуміють, як розвивається ситуація в Україні», — каже він.

Це звучить не надто привабливо, оскільки передбачає значні інвестиції. Крім того, іноземні стартапи, які розпочнуть роботу в Україні, стикнуться з іншим фокусом роботи.

«Якщо їдеш на хакатон і спілкуєшся з українськими фаундерами, все, що чуєш від них протягом двох днів: технології, технології, технології», — пояснює Тіс Клінкхамер, аналітик венчурного фонду з Нідерландів Keen Venture Partners. Натомість коли він спілкується з європейськими компаніями, то частіше чує про «дохід, продажі та стратегію».

Поєднати обидва полюси вкрай важливо.

З одного боку, є велика кількість українських стартапів, яким не вдається залучити капітал для масштабування своїх інноваційних ідей. Безумовно, на це впливають також і державні політики, проте частково причина й в іншому — ці стартапи насамперед сфокусовані на ефективності тут і зараз, тож часто сил на довгострокове планування не вистачає.

А з другого боку — є також й іноземні компанії, яким не вдається технологічно продемонструвати результати на фронті в Україні, хоч у них чимало клієнтів в інших країнах. Як це можливо? Будь-який інноваційний продукт розробляється на основі певного уявлення про майбутню війну та умови, у яких вона ведеться. Наприклад, окремі версії керованого американського артилерійського снаряда M982 Excalibur розроблявся для війни, у якій супротивник не здатний ефективно вести радіоелектронну боротьбу та встановлювати перешкоду для сигналів GPS. Вочевидь саме ці версії Україна й отримала, тож коли росіяни почали впливати на передачу сигналів глобальної системи позиціонування, ефективність M982 впала з 70% до 6%. Іншими словами, сюрприз, спричинений застосуванням цього снаряду, був недостатнім, аби дезорганізувати супротивника.

■ Порівняння українського Defense Tech з іноземним

Уявлення про майбутню війну — це основа діяльності будь-якої служби, яка відповідає у запровадженні інновації в армії мирного часу. Наприклад, у США вона називається Підрозділ оборонних інновацій. Метою підрозділу є не лише пришвидшити опанування військом цивільних технологій, а й бути драйвером змін щодо того, «як ми будемо битися за кожного уявного сценарію», пише перший очільник цього підрозділу Радж Шах.

На операційному рівні служба займається тим, що допомагає приватним компаніям без попередніх державних замовлень дійти до першої закупівлі. Те, які саме технології підрозділ прагне отримати, багато говорить про їхнє уявлення щодо майбутньої війни. Наприклад, станом на квітень 2025 року підрозділ збирав пропозиції щодо розробки підводної роботизованої платформи.

Дещо подібні технології розвиваються компаніями з України. Кожна країна має власну стратегічну культуру та національні інтереси, а отже, уявлення інших держав про майбутню війну відрізнятимуться від українських.

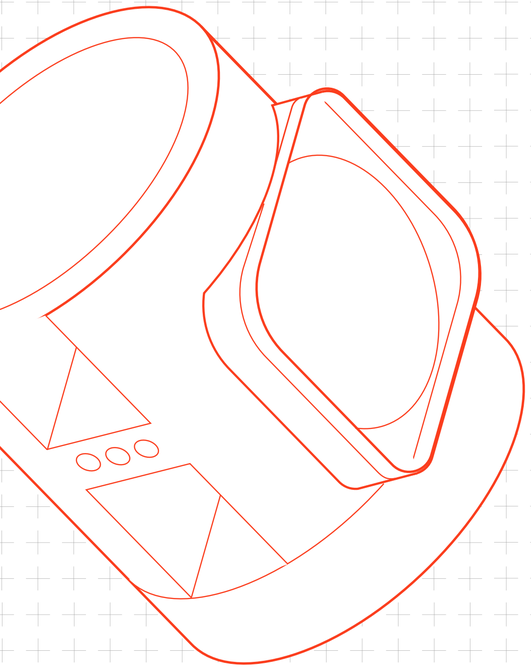
Проте Маттіас Лена з Quantum Systems переконаний, що досвід України все одно є життєво важливим: ***«Інновації у сфері БпЛА зараз відбуваються саме в Україні, тому якщо іноземна компанія хоче претендувати на лідерство в цій галузі, їй необхідно працювати в Україні. Байдуже, наскільки складні в Україні умови. Ви або адаптуєтесь або не стверджуєте, що ви лідер».***

Наприкінці розмови він говорить фразу, яку досить часто можна почути на оборонно-інноваційних подіях в Україні, але у багатьох гравців іноземних Defense Tech екосистем: ***«Якщо ви не працюєте в Україні — вас не існує».***

РЕАЛІЇ ТА ПОТОЧНІ ПРОБЛЕМИ СФЕРИ: 2014–2022 РОКИ, З 2022 РОКУ

Ця частина огляду була опублікована на сайті AIN в лютому 2025 року у матеріалі «Зростати всупереч: головні виклики українського Defense Tech у 2025 році».

AIN опитав 11 українських Defense Tech стартапів, поспілкувався з інвесторами та галузевим об'єднанням — Технологічними силами України.



Ранжувати виклики за важливістю неможливо, оскільки в роботі розробників кожна складова взаємопов'язана з іншою. Водночас їх можна розподілити на кластери:

- ті, що стосуються факторів виробництва;
- ті, що стосуються розвитку;
- ті, що стосуються SaaS-стартапів.

Кожен виклик супроводжується пропозицією щодо його подолання. Ці пропозиції не можуть бути вичерпними з огляду на комплексність викликів.

1. ФАКТОРИ ВИРОБНИЦТВА

До факторів виробництва можна зарахувати людський капітал, матеріали та фінансовий капітал.

1.1 Людський капітал

Виклик: складний процес здобуття статусу критично важливого підприємства, який не дозволяє швидко бронювати працівників.

З цим викликом українські оборонні розробники стикалися ще в попередні роки. Проте в першому місяці 2025 року ця проблема знову потрапила в новинні заголовки: 27 січня стартап «Око Камера», що розробляє тепловізійні камери для безпілотних систем, повідомив, що їхнього керівника виробництва утримують в Печерському ТЦК. Компанія повідомила, що має статус критично важливого підприємства, виконує державне оборонне замовлення, тож має право на бронювання своїх працівників. Натомість центр комплектування заявив, що це не відповідає дійсності.

Міністерство цифрової трансформації України надало AIN наказ, яким підприємству надано статус критично важливого. «Око Камера» в коментарі підтвердила, що зрештою працівник отримав військово-обліковий документ і бронювання.

Причина конфлікту полягала в тому, що співробітник Defense Tech стартапу не перебував на обліку. У такій ситуації єдиний варіант розв'язання ситуації під час постановки на облік — це офіційний лист до ТЦК від компанії з роз'ясненням. У січні 2024 року CEO «Око Камера» Денис Ніколаєнко скерував такого листа в Печерський ТЦК. Або ж міг би спрацювати інший сценарій.

«Коли людина приходить стати на облік, може отримати повістку, пройти ВЛК і в той же день поїхати в навчальний центр», — каже Ніколаєнко. Додає: у такому випадку дії ТЦК є законними, оскільки без перебування на обліку немає підстав для відстрочки.

Військово-обліковий статус окремих працівників — не єдине джерело труднощів для стартапів. Часті зміни нормативно-правових актів, що регулюють бронювання, суттєво ускладнювали цей процес для стартапів.

«Поки ми підготували документи, змінилися критерії», — розповідає в коментарі AIN COO виробник детекторів дронів Kara Dag Technologies Андрій Побережнюк.

Подібна історія відбулася і з виробником дронів-міношукачів Ailand Systems: спершу компанія намагалася забронювати працівників, подаючи паперові оригінали документів, проте згодом уряд запровадив електронне бронювання, чим компанія також скористалася.

Наявність документів про бронювання не завжди впливає на дії та рішення ТЦК.

Засновник Ailand Systems Дмитро Тітов у коментарі AIN розповідає, що ключового інженера компанії мобілізували, а інші розробники провели тижні в чергах, намагаючись довести свій статус забронюваних.

«Працівники ТЦК сміялись нам в обличчя і говорили, що документи про бронювання — це "туалетний папір"», — пригадує він.

Одного з розробників Kara Dag Technologies також мобілізували, що призупинило новий проєкт компанії.

Попри це Тітов вважає, що бронювання — це «велика розкіш», за яку він вдячний. Він відзначає прагнення регуляторів покращити цей процес. Побережнюк з Kara Dag Technologies також зберігає оптимізм: навіть якщо значну частину працівників мобілізують, компанія сповільниться, але не зникне.

Крім того, деякі компанії стикалися з меншими викликами під час бронювання: «Ми не маємо потенційної загрози мобілізації провідних співробітників, інженерної та виробничої команди», — каже Міша Рудомінський, співзасновник виробника систем зв'язку HIMERA. Завдяки співпраці з Міністерством з питань стратегічної промисловості та Міністерством оборони стартапу вдалося забронювати команду.

Денис Ніколаєнко з «Око Камера» також вважає, що попри труднощі «вже є прогрес у системі бронювання», особливо порівняно з 2022 роком.

Гостро для проблема стоїть і для Buntar Aerospace — один із співзасновників проєкту Богдан Сас вважає, що виклик досі не стовідсотково вирішений для Defense Tech стартапів: «Ми втратили кількох важливих людей через абсолютно абсурдні ситуації, коли навіть статус критичної інфраструктури не врятував. У нас зараз є юристи, які ведуть дві справи по співробітниках. Але навіть якщо виграємо — людину вже мобілізовано, вона вже тричі була на ротаціях. Тобто це боротьба не за минуле, а за зміну системи в майбутньому».

Водночас, за його словами, покращилася ситуація з можливістю виїзду представників стартапів за кордон — спілкування з інвесторами, представлення продукту, відвідування галузевих подій. «Це важливо: укладати угоди, домовлятися про поставки, бути на виставках. Ми не раз це робили, і щоразу це давало результат. Але ми підходимо до цього з повною відповідальністю — ніхто після відрядження не залишився за кордоном, всі повернулись. Це питання довіри».

Досі частка бронювання складає від 50% усіх військовозобов'язаних, що працюють у штаті компанії. Євген Третяк, співзасновник Frontline Robotics каже: «Defense Tech компанії зібрали унікальних в своїх галузях спеціалістів, і втрата навіть одного співробітника може поставити на паузу розробку перспективної оборонної технології, що може в рази збільшити потенціал Сил оборони України».

Водночас співзасновник Frontline Robotics відзначає, що 2024 рік став проривним для полегшення цього процесу завдяки механізму бронювання через «Дію».

Проте це не єдине нововведення, запроваджене Кабінетом Міністрів стосовно бронювання. 1 грудня 2024 року набула чинності оновлена постанова Кабміну: якщо раніше міністр оборони міг окремим рішенням дозволити забронювати понад 50% військовозобов'язаних лише в управліннях Національної поліції та ДСНС, тепер ця процедура поширюється і на критично важливі підприємства.

Проте є нюанс: окреме рішення міністра оборони не може застосовуватися щодо підприємств, заброньованих Міністерством з питань стратегічних галузей промисловості. А таких у галузі Defense Tech досить багато, пояснює співзасновниця ігрового симулятору з домедичної допомоги та тактичної медицини LifesaverSIM Олеся Дячишин.

Водночас частина галузі також може бути заброньована і Міністерством оборони. Для цього, згідно з постановою, необхідно мати укладений договір із Міністерством оборони щодо постачання оборонних товарів чи послуг. Проте за таких обставин може виникнути замкнуте коло: компанія не має права на 100% бронювання, оскільки не має договору з міністерством, а укласти договір про постачання такого товару вона не може, оскільки він все ще перебуває в розробці, а завершити його розробку компанія не може, бо є виклик створити стабільну команду високоспеціалізованих інженерів.

Завдяки змінам постає принаймні теоретична можливість здійснити те, про що голова Defense Tech кластера Brave1 Наталія Кушнерська говорила ще у 2023 році: бронювати не 50%, а 100% «фахівців, залучених до пріоритетних для Сил безпеки і оборони проєктів».

Проте навіть виконання вже наявних вимог не завжди призводить до надання статусу критичності. Наприклад, постанова Кабінету Міністрів дозволяє Міністерству оборони визнавати критично важливими ті організації, що «що здійснюють підготовку, перепідготовку та підвищення кваліфікації військовослужбовців з домедичної допомоги в інтересах сил безпеки та оборони України за програмами, затвердженими Генеральним штабом Збройних сил або Міноборони».

LifesaverSIM має понад 90 000 зареєстрованих користувачів і, за оцінкою розробників, половина з них — чинні військовослужбовці. Згідно з рішенням Міноборони та розпорядженням Генштабу, проєкт успішно пройшов закрите тестування симулятора у військових закладах вищої освіти та навчальних центрах ЗСУ, отримавши висновок про необхідність впровадження. Підтримати впровадження симулятора також пообіцяв командувач Медичних сил ЗСУ Анатолій Казмірчук. Застосунок посів перше місце в конкурсі Міністерства оборони серед навчальних симуляторів. Проте цього виявилося недостатньо, аби Міністерство оборони відповіло на запити LifesaverSIM щодо отримання критичності.

Крім того, стартап звернувся і до Міністерства з питань стратегічних галузей промисловості. Спершу у серпні 2024 року, потім ще раз у жовтні. У грудні від міністерства надійшла відповідь, що LifesaverSIM не надає послуг «з розроблення, виготовлення, ремонту, модернізації та утилізації озброєння, військової і спеціальної техніки, боєприпасів».

«Ми детально вивчили нормативну базу, і з'ясували, що для розробників винятково програмних продуктів для Сил оборони, як у нашому випадку, процедур бронювання не існує», — стверджує співзасновниця стартапу Олеся Дячишин.

За її словами, якщо не надати проблемі розголосу і не вирішувати її системно, критичних фахівців будуть мобілізовувати, команди розпадатимуться, а перспективні інноваційні розробки буде втрачено.

«Профільні міністерства повинні терміново внести зміни до своїх наказів і постанов для забезпечення критичності та бронювання фахівців інноваційних оборонних стартапів, а розвитком Defense Tech має займатися державна інституція з достатніми повноваженнями і громадянським контролем», — підсумовує вона.

Подолання: створення простої та стабільної системи бронювання, яка дозволить працівникам Defense Tech стартапів виконувати оборонне замовлення.

Міністерство цифрової трансформації України надало AIN наказ, яким підприємству надано статус критично важливого. «Око Камера» в коментарі підтвердила, що зрештою працівник отримав військово-обліковий документ і бронювання.

Виклик: недостатньо кандидатів для заповнення вакантних посад.

Згідно з опитуваннями Інституту економічних досліджень і політичних консультацій, наприкінці 2024 року вперше за весь час повномасштабного вторгнення саме нестача людського капіталу стала головною перешкодою для бізнесу. Для Defense Tech підприємств цей виклик поглиблюється тим, що потрібними є доволі рідкісні спеціалісти.

«Це питання «на вчора»», — каже CEO «Око Камера» Денис Ніколаєнко й відзначає, що чим більше зростає команда, тим гостріше відчутна нестача саме кваліфікованих кадрів.

Проте і це ще не все: про Defense Tech говорити треба так, аби не наражати підприємства на зайві загрози з боку ворога. Результат? «Про нас не знають», — говорить Олеся Дячишин, співзасновниця мобільного застосунку-симулятора надання домедичної допомоги LifesaverSIM.

У 2024 році вона долучилася до двох ярмарків вакансій. До стенда LifesaverSIM підходили студенти. «А що таке Defense Tech? А що це за симулятор? Цікаво, розкажіть більше», — пригадує Дячишин їхні реакції. Вона відзначає, що студенти цілком можуть виконувати різні завдання в межах її стартапу. Kara Dag Technologies також залучає студентів, каже Побережнюк.

Засновник Defense Tech стартапів у сфері БпЛА The Fourth Law і Odd Systems Ярослав Ажнюк може довго перелічувати виклики та ніші, які потребують розвитку в межах українського Defense Tech: від обчислювальної гідрогазодинаміки, необхідної для розвитку ще більш просунутих крилатих ракет, до нових методів семантичної сегментації, які б дозволили автономну навігацію для дронів чи ракет над морем, попри нестабільність текстури поверхні води під ними.

Для подолання викликів такої складності потрібні люди з досить унікальним досвідом, пояснює Ажнюк. І йдеться не лише про спеціалізовані інженерні знання.

У TFL та Odd Systems є конкурентна перевага стосовно найму: засновник компаній є досить відомим з огляду на свою попередню підприємницьку діяльність. Це збільшує ймовірність того, що вакансії побачать майбутні працівники. Багато інших гравців такої переваги не мають. Навпаки — усі вимушені зайвий раз публічно не наголошувати на своїх розробках, аби не привертати до команди та рішень зайвої уваги росіян.

Крім того, загальна ситуація на ринку праці, ймовірно, залишатиметься досить напруженою і у 2025 році. Згідно з обрахунками Центру економічної стратегії, майже увесь 2024 рік активність шукачів роботи була нижчою за 2022 і 2023 роки. Навіть за умов зменшення інтенсивності бойових дій ситуація на ринку праці не обов'язково покращиться. Старший економіст Центру економічної стратегії Володимир Ланда припускає, що за таких обставин вперше в сучасній історії Україна відчуватиме гостріший дефіцит людського капіталу, ніж фінансового.

Подолання: спрямування комунікації про Defense Tech стартапи на нові аудиторії із врахуванням безпекових аспектів та обмеженості видатків на HR.

1.2 Матеріали

Виклик: загострення протистояння між США та КНР може призвести до розриву ланцюжків постачання товарів, через що hardware стартапи відчуватимуть дефіцит компонентів.

Заголовки на кшталт «Китай заборонив експорт...» регулярно можна побачити в стрічці новин. Очевидно, що українське суспільство відчуває свою залежність не лише від підтримки західних партнерів, а й від бажання КНР далі заробляти на війні.

Наразі важко спрогнозувати, як зміна політичного і військового керівництва США вплине на позицію Китаю в міжнародній торгівлі. Навіть дружні до України держави можуть запровадити експортні обмеження у випадку суттєвого загострення глобального протистояння і термінової необхідності виробництва зброї для власних потреб — так, як це було з медичними товарами під час пандемії.

У будь-якому випадку опитані стартапи очікують нестабільності: «Ситуація значною мірою залежатиме від кон'юнктури зовнішньої політики та потенційних воєнних конфліктів у світі», — каже COO Kara Dag Technologies Побережнюк.

Нестабільності сприяє не лише фактор непрогнозованості експортної політики інших країн. Співзасновник HIMERA Міша Рудомінський пояснює так: «У 2024 році пропозиція на ринку електронних компонентів скоротилася, оскільки, не отримавши достатніх прибутків, виробники почали зменшувати свої потужності». Його компанія прогнозує, що у 2025 році ця тенденція призведе до збільшення термінів очікування, відповідно, і до збільшення термінів виготовлення та постачання на фронт.

Подолання: диверсифікація постачання та локалізація виробництва із врахуванням кінцевої собівартості.

HIMERA, як і більшість опитаних AIN стартапів, розробила стратегію мінімізації таких ризиків. Наприклад, компанія має щонайменше двох постачальників кожного компонента чи прагнуть укладати прямі договори з виробником. Тим часом «Око Камера» активно працює над локалізацією виробництва компонентів.

Держава також може сприяти подоланню цього виклику: «Потрібно більше уваги приділяти стимулюванню українського виробництва», — вважає Побережнюк з Kara Dag Technologies.

«Крім того, державі слід відповісти на запитання, чи готова вона платити більше за вироби без китайських компонентів», — каже в коментарі AIN Катерина Михалко, виконавча директорка Технологічних сил України.

Інакше можуть виникнути ситуації, коли гравці з локалізованими компонентами програватимуть у вартості тим проєктам, що надалі будуть використовувати деталі з КНР.
Наприкінці 2024 року уряд затвердив розроблений Міністерством з питань стратегічних галузей промисловостей порядок формування переліку «Зброя Перемоги», у який входитимуть товари зі ступенем локалізації понад 50%. Конкретний механізм функціонування цього переліку буде визначений в окремій постанові уряду.

Міністерство розповіло AIN, що наразі триває робота над цією постановою: її вже розглянув профільний Урядовий комітет, тож після низки правок її подадуть на розгляд уряду. Однак про зміст постанови вже можна говорити.

«При розгляді однієї номенклатури товарів оборонного призначення перевага має надаватися тим пропозиціям, які включені до переліку», — повідомило міністерство у коментарі AIN.

Тобто державний закупівельник має враховувати локалізованість продукції, обираючи між двома пропозиціями з подібними характеристиками. Це своєю чергою має створити додаткову економічну мотивацію для виробників щодо збільшення ступеня локалізації своїх виробів.

1.3 Фінансовий капітал

Виклик: неможливість постачати оборонні технології за кордон через державну заборону, спричинену міркуваннями щодо наслідків такого рішення

В українських Defense Tech стартапів доволі обмежені джерела виторгу. Насамперед це державне оборонне замовлення, яке залишається доволі непрогнозованим. Залучених у такі способи коштів не вистачає, щоб застосувати всі потужності підприємств.

Спершу в бюджеті 2024 року для Державної служби спеціального зв'язку та захисту інформації на закупівлі безпілотників було передбачено 43,3 млрд грн, у квітні уряд додав до цієї суми ще 15,5 млрд грн. Паралельно закупівлі здійснювала також Агенція оборонних закупівель (АОЗ) Міноборони: на безпілотники пішло понад 114 млрд грн. Також дрони купували українські спецслужби, проте на суттєво менші суми.

Попри це, згідно з підрахунками ТСУ, більшість членів якого виробляють якраз таки безпілотники, у 2024 році майже дві третини спроможностей виробників не були завантажені державними замовленнями.

«Могло бути виготовлено додатково 1,6 млн FPV та понад 80 тисяч безпілотників інших видів», — розповіла Катерина Михалко під час презентації Лічильника зброї, якої немає від ТСУ 6 лютого, на якій побував журналіст AIN.

У бюджеті 2025 року для Держслужби спецзв'язку та захисту інформації на безпілотні комплекси призначено близько 47 млрд грн. Водночас якщо у 2024 році Міністерство оборони планувало витратити на «розвиток, закупівлю, модернізацію та ремонт озброєння, військової техніки, засобів та обладнання» 265 млрд грн, то на 2025 рік заплановано 488 млрд грн. Чи призведе це зростання до завантаженості українських виробників?

Станом на кінець 2024 року більшість членів ТСУ не перебували в перемовинах з державними замовниками. Натомість початок 2025 року ознаменувався кризою в Агенції оборонних закупівель, що «також змушує нас очікувати затримок в укладанні контрактів», каже Михалко.

Тож цей виклик має подвійне походження: з одного боку, бюджет України обмежений; з другого, стартапи не завжди можуть покладатися на стабільність замовлень.
Крім того, нестача капіталу має стратегічні наслідки — відсутня здатність реінвестувати в R&D.

«За останні три роки ми імплементували в систему оборони більшість доступних простих або середньої складності рішень», — каже CEO «Око Камера» Ніколаєнко і відзначає: щоб рухатися далі, потрібно більше ресурсів. Супротивник тим часом на місці не стоїть і має порівняно більше можливостей для такого розвитку.

Якби українські виробники могли продавати свої вироби іншим країнам, це б дозволило диверсифікувати джерела доходу. Крім того, це б зробило українським ринок Defense Tech більш привабливим для інвесторів, повідомили в коментарі AIN інвестиційні фонди Dare to Defend Democracy (D3) та Presto Tech Horizons.

Немає конкретного документа, який забороняє експорт, проте після початку повномасштабного вторгнення регулятори відмовляють виробникам у дозволах на продаж військової техніки. За відсутності такого нормативного акта є ймовірність, що в окремих випадках експортувати вдавалося.

«Можливо, випускають окремі комплектуючі, але прогнозованого доступу до міжнародних ринків не існує», — каже Катерина Михалко.

Попри те що восени 2024 року розмови про скасування заборони активізувалися, досі цього рішення ухвалено не було.

«Це суспільно важка тема», — пояснює виконавча директорка ТСУ. Продавати зброю, від якої залежить сама Україна? Кому? Країнам НАТО, які з високою ймовірністю в короткостроковій перспективі її не застосують? Ідеальний рецепт для інформаційних операцій супротивника. А тепер додайте до цього загальну чутливість українського суспільства до різноманітних теорій змов про експорт: як не вивезення чорнозему вагонами, так продаж електроенергії в Румунію під час відключень. Тож є підстави вважати, що ворог зможе використати зміни в галузі експорту оборонних виробів для своїх цілей.

Крім того, такі інформаційні заходи можуть бути спрямовані не лише на українське суспільство, а й на політиків Європи, які мобілізовуватимуть виборців вже не лише під прапором «українська пшениця шкодить нашим фермерам», а й «українська зброя заважає нашим заводам».

«Різні органи державної влади регулярно звертаються до ТСУ із запитами щодо можливих механізмів експорту, що будуть працюючими для виробників. Ми знаємо, що зараз різними стейкхолдерами, з боку держави, напрацьовуються різні форми. Позиція ТСУ незмінна: дозволити експорт до країн-членів НАТО та держав, які уклали з Україною безпекові угоди з 2022 року, якщо обсяг державних замовлень менший за 100%, або в підприємств є надлишкові виробничі потужності» — зазначають Технологічні Сили України.

До чого може надалі призвести заборона експорту розробок?

Негативних наслідків цього чимало. В першу чергу, кажуть в ТСУ, — це вимушена релокація виробників. Заборона експорту спонукає виробників до вимушеної релокації за кордон у пошуках ринків збуту: 63% компаній-виробників, опитаних Технологічними силами, називають закритий експорт ключовою причиною релокації за кордон. Щобільше для 71% виробників мотивацією продовжувати розвивати підприємництво в Україні є знову таки — відкриття експорту ОВТ.

Серед інших не менш негативних наслідків, які поглиблює заборона експорту, – це скорочення спроможностей виробників, які не бачать можливостей для масштабування та розвитку технологій й розробок, а також банкрутство компаній.

Подолання: прийняття моделі контрольованого експорту партнерам України та відповідна комунікаційна кампанія.

Проте не змінювати поточну ситуацію суто з таких міркувань — означає залишатися під рефлексивним контролем супротивника, тобто продовжувати завдавати собі шкоди й думати, що в такий спосіб уникаєш ще більшої біди. Компромісним підходом до експорту може бути модель, за якої регулятор враховує реальну спроможність конкретного гравця щодо вироблення товару й розуміє здатність держави щодо контрактування цього товару.

Якщо між цими величинами прірва, то Україна не втрачатиме в обороноздатності, адже без іноземних грошей цей товар все одно не буде вироблений. Контрольованість експорту полягатиме також і в тому, що українські вироби продаватимуться лише в країни, варті довіри, а не компаніям, зареєстрованим позавчора на Кайманських островах.

Що ж стосується інформаційної компоненти виклику, то Михалко не втрачає оптимізму: «Люди розумні і мають зрозуміти, що контрольований експорт підсилить нас. Для цього суспільству необхідно надати інформацію про ситуацію в галузі. Але найважливіше навіть не це — державі потрібна сміливість, аби взяти відповідальність за таке рішення», — каже виконавча директорка ТСУ.

4 лютого відбулося засідання Ради національної безпеки та оборони, на якому обговорювали шляхи зменшення торговельного дефіциту України. РНБО вирішило сприяти збільшенню спроможностей оборонно-промислового комплексу, а також уточнити критерії, які уможливлюють бронювання працівників оборонних підприємств. Чи розглядала Рада потенціал експорту виробів цих підприємств? AIN надіслав запит Офісу Президента, однак на момент публікації відповіді не отримав. Як тільки її нададуть, редакція одразу її оприлюднить.

2. РОЗВИТОК

Фактори виробництва забезпечують роботу Defense Tech у теперішньому. Проте майбутнє стартапів визначатиме їхня здатність подолати виклики щодо продажів за кордоном і залучення іноземних інвестицій.

2.1 Продажі за кордон

Виклик: перенести успішний досвід оборонних закупівель з українського контексту в іноземний, але залишитися українською компанією.

Опитані стартапи погоджуються: хоч зараз вони майже повністю сфокусовані на фронті, проте робота на іноземних ринках буде вкрай важливою в майбутньому. Наприклад, СМО Frontline Robotics Микита Рожков у коментарі AIN каже: «Ми прагнемо побудувати довгостроково стабільну компанію та розуміємо, що це неможливо в ізоляції, тому звертаємо увагу на запити країн-партнерів і можливості розвитку на міжнародному ринку».

Проте зміни експортної політики недостатньо. Якщо уявити, що розпочнеться контрольований експорт, то українські стартапи потраплять у цілком новий для себе контекст європейських ринків. Як зауважує партнер інвестиційного фонду D3 Антон Верховодов, країни ЄС очікуватимуть від українських гравців локалізацію виробництва чи залучення локальних партнерів у продажі за оборонними контрактами.

Водночас локалізація виробництва за кордоном означатиме, що модель контрольованого експорту зазнала поразки: потужності в Україні далі простоюють, амортизація стає невигідною, тому зрештою підприємства скорочують потужності.

Наприкінці 2024 року Технологічні Сили України робили опитування щодо державних контрактів, згідно з яким лише 19% виробників мали контракти з державою, які забезпечували їм роботу у першому кварталі 2025 року. Наразі контрактування продовжується згідно з потребами Сил Оборони, зазначають в ТСУ. Міноборони спрямувало третину оборонного бюджету на технологічну зброю.

«Проте, галузь все ще фіксує відсутність довгострокових, стабільних та своєчасно укладених контрактів для українських виробників ОВТ (озброєння та військової техніки). Для виробників також залишається актуальним питання дієвого механізму визначення потреби, а також зв'язку про затребувані зразки на полі бою або їхню модернізацію. Це необхідно для чітких, передбачуваних умов забезпечення армії українською технікою», — кажуть в ТСУ.

Подолання: співпраця українського стартапу з іноземною компанією-інтегратором, що має контракти та відносини з Міністерством оборони своєї країни.

Співпраця з інтегратором може відбуватися за такою моделлю:

- Український стартап виробляє в Україні компоненти, у розробці яких має високу експертизу.
- Український стартап постачає ці компоненти компанії в країни ЄС.
- Компанія інтегрує ці компоненти у свої вироби.
- Міністерство цієї країни, члена ЄС, закуповує вироби.

Потенційно цей алгоритм можна розширити, коли виріб з однієї країни ЄС закуповують інші члени союзу. Попри співпрацю між країнами ЄС в оборонній галузі, наразі вони здебільшого віддають перевагу власним виробам.

Водночас наприкінці січня на річній конференції Європейської оборонної агенції її очільниця Кая Каллас і комісар ЄС з питань оборони Андрюс Кубілюс закликали рухатися саме до спільного для всіх країн ЄС ринку оборонних товарів.

Чим ця модель є корисною для українського стартапу? Крім очевидного — заробітку на продажу компонентів — український стартап не витрачає ресурси на вивчення нормативної бази оборонних закупівель в іншій країні. У інтегратора вже є досвід співпраці з Міністерством оборони своєї країни та активні контракти.

До того ж інтегратор зацікавлений допомогти своєму партнеру модифікувати продукт так, аби той відповідав стандартам цієї країни.

Публічно про випадки застосування такої моделі не відомо — за відсутності прогнозованого експорту інтегратор ризикує не виконати контракт. Якби не це, вироби «Око Камера» вже б використовувалися в іноземних безпілотних комплексах, каже CEO стартапу Денис Ніколаєнко і додає, що регулярно отримує такі запити від гравців, що виробляють дрони за кордоном і постачають їх на українських ринок.

Співзасновник стартапу Максим Прасолов у коментарі AIN пояснює: ***«Шлях співпраці з інтеграторами дійсно призведе до оборонних закупівель швидше. У цих компаній зараз «шопінг»: вони йдуть за покупками і цікавляться українськими стартапами».***

Паралельно з цим його компанія продовжує прямувати до безпосередньої співпраці з Департаментом оборони США, проте цей шлях займе багато років і потребуватиме великих інвестицій.

2.2 Інвестиції

Виклик: недостатньо уваги до українських стартапів з боку іноземних інвесторів.

Катерина Михалко підтверджує, що інтерес до українських технологій зберігається на високому рівні, до ТСУ часто приходять запити з-за кордону щодо інвестицій. «***Але просто взяти й продати технологію за кордон Україні не вигідно»,*** — каже вона.

Дмитро Тітов з Ailand Systems також наголошує на тому, що іноземні інвестори прагнуть перевести компанії в іноземні юрисдикції, аби зменшити воєнні та корупційні ризики. Проте в результаті, пояснює Тітов, «це призведе до того, що коли закінчиться війна, виявиться що більшість наших технологій більше не належить країні та збільшують інші ВВП».

Але іноземні інвестори також програють від такої практики, вважає CEO «Око Камера» Ніколаєнко: ***«Структурування інвестиційної угоди через закордонні холдинги на ранніх етапах розвитку компанії відриває засновників від розробки продукту, який потрібен на фронті, і розвитку компанії, адже цей процес займає місяці».*** Іншими словами, хочете якісніший продукт та більш сталу команду — інвестуйте в українську юрисдикцію.

І це ще не все. Навіть коли в компанії є одночасно юридичні особи в Україні та за кордоном, як у Farsight Vision, інвестори все одно ставляться до стартапу обережно.
Farsight Vision розробляє платформу, яка швидко перетворює відеозаписи з дронів у 3D-моделі місцевості, що допомагає в плануванні бою. Компанія зареєстрована в Естонії на додачу до української ТОВ.

Співзасновниця підприємства Вікторія Яремчук розповідає, що стикалася з щирим здивуванням іноземних інвесторів, коли оцінювала свою компанію «на рівні з європейськими чи, не дай Боже, американськими стартапами, мовляв, ви ж з України, у вас там війна, [як ви можете створювати конкурентні розробки?]».

«Подібні за напрямком компанії зі Скандинавії чи Німеччини отримують оцінку у два чи три рази більшу просто тому, що розвиваються в цих країнах», — продовжує Яремчук. Її це вражає, адже саме застосування технології на полі бою в Україні наразі вважається показником якості.

Подолання: убезпечення людського капіталу, збільшення факторів виробництва та посилення комунікації.

«Приходить інвестор і дивиться, що велика кількість потужностей компанії простоює, що єдиний замовник — це держава без достатнього закупівельного бюджету, що міжнародні ринки закриті, тож досвіду за кордоном немає, — каже виконавча директорка ТСУ. — ***І що інвестору з цим робити?»***

Матей Луговий, інвестор венчурного фонду Presto Tech Horizons, підтверджує, що досвід роботи на іноземних ринках є важливим фактором в ухваленні рішень про інвестицію в український стартап.

Він пояснює у коментарі AIN, що наявність контрактів за кордоном допомагає інвесторам підтвердити гіпотези про існування глобального потенційного ринку для конкретної розробки, оскільки «навіть якщо щось ефективно працює в Україні та вирішує характерні Україні проблеми, необов'язково є гарним кандидатом для венчурної інвестиції».
Його колега з Presto Tech Horizons Мартін Ле підтверджує: «Інвестори сподіваються на скасування заборони на експорт».

Тому подолати цей виклик неможливо, не подолавши попередні. Проте навіть якщо ситуація з факторами виробництва зміниться, це ще не означатиме, що іноземні інвестиції потечуть в Україну рікою.

Антон Верховодом з D3 Venture Capital Firm наголошує: «Інформації про українські інновації за кордоном досі недостатньо. Нам потрібно не просто найкраща інформаційна кампанія про оборонні технології в Україні — це має бути ледь не пропаганда для ключових осіб в інвестиційних колах НАТО». Тому, додає він, засновникам стартапів треба і далі працювати над своїми навичками пітчингу.

Луговий з Presto Tech Horizons погоджується: ***«Самопрезентація — це найслабша ланка у стартапів не лише з України, а й загалом зі Східної Європи».***

Як зробити співпрацю між українськими Defense Tech стартапами та іноземними партнерами більш тісною? Ярослав Ажнюк пропонує концепцію «оборонної долини», яка може стати ключовим елементом нової національної стратегії. Її мета — зробити Україну незамінною для Північноатлантичного альянсу у сфері Defense Tech так само, як Тайвань є незамінним у галузі мікрочипів.

Її передумова — вже наявна в Україні концентрація талантів і досвіду. А механізм реалізації — стратегічні комунікації та позиціювання країни на президентському рівні, скасування заборони на оборонний експорт, створення вільної економічної зони та інші кроки до поліпшення інвестиційного клімату.

Дебора Фейрлемб з Green Flag Ventures також вважає, що трансформації мають бути комплексними, і не лише в Україні. Вона звертає увагу на те, що стартапам легше завоювати довіру американських інвесторів, якщо отримати закупівельний контракт від Міністерства оборони США. А підписання такого контракту — це досить повільний процес, який може затягнутися на більш як пів року, що для українських стартапів досить довгий строк.

Американські урядовці не змінюватимуть свої процедури через людей, про існування яких вони вчора і не знали. Проте необхідність діяти швидше очевидна не лише українцям.
У березні 2024 року спеціально створена Сенатом США Комісія з реформи планування, програмування, бюджетування та виконання оборонних видатків представила свої рекомендації. Вони здебільшого стосуються внутрішніх процедур Пентагону, як-от збору даних, внутрішніх комунікацій і ухвалення рішень, а також трансферу погоджених Конгресом видатків з однієї бюджетної лінії до іншої. Ці реформи були необхідні, адже наявні процедури «не забезпечували гнучкості, необхідної для впровадження інновацій досягнень з адекватною швидкістю».

У грудні 2024 року Палата представників США підтримала закон «Про асигнування на національну оборону на 2025 бюджетний рік», який зобов'язує міністра оборони створити окрему робочу групу для виконання цих рекомендацій. Чи це допоможе українському Defense Tech? Складно сказати, адже досі контракти часто отримували ті компанії, які краще лобіюють свої інтереси, «а не ті, які мають потрібні рішення», казав Голова Об'єднаного комітету начальників штабів США Чарльз Браун.

На ринку з'явився ще один гравець, що працюватиме в цьому напрямку. Ще в березні 2024 року Високий представник ЄС із зовнішньої політики оголосив про плани відкрити в межах Представництва ЄС в Україні підрозділ, що «стане містком між стартами та інноваторами у ЄС й промисловістю України та Збройними силами». Восени 2024 року це сталося: у Києві відкрився Офіс оборонних інновацій ЄС. Він прагне зробити пошук бізнес-партнерів у країнах-членах союзу більш доступним і систематичним для українських стартапів.

Розбудова цих мереж стосується не лише приватного капіталу, а й фінансування ЄС. Такі можливості вже існують, а у 2025 році їх може побільшати. Навесні 2024 року Європейська комісія запропонувала створити Європейську програму оборонної промисловості, серед цілей якої — розбудова співпраці між оборонною промисловістю ЄС та України. Початково комісія запропонувала витрати на програму 1,5 млрд євро, проте в жовтні Європейська палата аудиторів дійшла висновку, що цих коштів може бути недостатньо для досягнення заявлених цілей.

Наприкінці листопаду після довгих перемовин країнам-членам вдалося досягнути компромісу щодо критеріїв, які дозволятимуть участь підприємств у програмі. У разі песимістичного сценарію повноцінно програма почне працювати у вересні 2025 року, повідомив AIN європейський посадовець, який побажав залишитися анонімним.

3. ПРОБЛЕМИ SAAS СТАРТАПІВ

Коли говоримо про Defense Tech, здебільшого уявляємо рої автономних дронів, що запускаються з безпілотника-матки, або роботів, які самостійно розміновують деокуповані території. Людині легше уявити щось матеріальне.

Проте чимало українських стартапів мають SaaS продукти, які здатні вплинути на перебіг війни. Вони також стикаються зі специфічними проблемами та не отримують достатньо уваги.

3.1 Аналог кодифікації

Виклик: відсутність процедури кодифікації для програмних застосунків.

Щоб Збройні сили могли застосовувати, а держава закуповувати певне озброєння, воно має спершу пройти кодифікацію. Кодифікація застосовується до озброєння, військової та спеціальної техніки (ОВСТ). Програмне ж забезпечення не є ані озброєнням, ані технікою. Для кодифікації виробник подає в Міноборони низку документів. Серед них — проєкт технічних умов. У проєкті слід вказати, наприклад, довжину та ширину виробу або джерело живлення. Якою є ширина програмного коду? Як він живиться?

Після цього Міноборони перевіряє документацію. Яким чином вони перевірять, що програмне забезпечення не містить «слідів фарби на нефарбованих поверхнях», а також переконаються, що програмний код відповідає чинним стандартам «у частині впливу кліматичних чинників зовнішнього середовища»?

Простішими словами, проєкт технічних умов неможливо застосувати до суто програмних рішень. Візьмемо, наприклад, платформу Farsight Vision, яка працює за підпискою. Цьому стартапу дещо пощастило: крім платформи, команда також пропонує фізичній пристрій, необхідний для перетворення відео у 3D-моделі. Цей пристрій команда і подала на кодифікацію.

А от мобільний застосунок-симулятор з надання домедичної допомоги LifesaverSIM користувач запускає на власному телефоні, тому hardware-компонентів продукт не має. Цим він відрізняється від, наприклад, системи ситуаційної обізнаності «Кропива», яка часто постачається у військо передвстановленою на планшети.

4 лютого набули чинності зміни, внесені урядом напередодні у постанову, що регулює прийняття нового ОВСТ на озброєння. Оновлена постанова є більш чутливою до ПЗ: наприклад, «продукція оборонного призначення» перетворилася на «товари оборонного призначення».

Якщо раніше складовою частиною зразка ОВСТ визнавався «виріб, призначений для виконання [його] певних технічних функцій», то тепер у це визначення також включені й «комп'ютерні програми».

Отже, повноцінно підхід не трансформувався: ПЗ розглядається не як самодостатній продукт, а лише як компонента hardware рішення, тож такі застосунки як LifesaverSIM і далі лишаються за межами нормативної бази

Подолання: передача ліцензії на ПЗ замість кодифікації та посилення комунікації.

Співзасновниця LifesaverSIM Олеся Дячишин співпрацює з правниками Міністерства оборони, аби визначити шлях, який має пройти застосунок замість кодифікації. Ймовірно, це буде здійснюватися через передачу ліцензії. На цю роботу витрачається багато сил, оскільки відсутня політична ініціатива щодо створення стандартизованого механізму для таких стартапів.

«Потрібен комунікаційний майданчик між державою та стартапами, який би об'єднував багато стейкхолдерів: Мінцифри, Мінстратегпром, Міноборони, Генеральний штаб ЗСУ, можливо, також Державну службу спеціального зв'язку та захисту інформації», — каже Дячишин.

3.2 Загальна філософія щодо SaaS

Виклик: відсутність уявлення програмного забезпечення як самодостатнього продукту.

Протягом усієї історії людства війни велися фізичними предметами. Від списа до гіперзвукової ракети, саме матеріальний вимір зброї завжди був у фокусі військових. Безумовно, FPV-дрони стали проривною технологією саме завдяки тому, що корисне навантаження безпілотника здатне завдавати матеріальної шкоди ворогу. Проте програмне забезпечення відіграє все більшу роль у веденні війни.

Водночас під час попередніх інтеграцій ПЗ у Збройні сили це здійснювалося або на волонтерській основі («Кропива»), або через трансформацію волонтерської команди в штатний підрозділ ЗСУ (DELTA). Через це таким стартапам, як Farsight Vision, важко обґрунтовувати потенційним клієнтам, чому за їхні послуги треба платити.

Яремчук переказує свої розмови із закупівельниками: «От якесь ПЗ американське, швейцарське, європейське ми можемо закуповувати, але навіщо платити за українське?».

Подолання: трансформація ставлення до програмного забезпечення.

Культурні зміни можуть відбуватися доволі повільно. Військовим і недержавним гравцям слід наголошувати на важливості програмного забезпечення для оборони, аби пришвидшити цю трансформацію.

Технологічні Сили України виділяють ще такі виклики:

- Голос приватних виробників недостатньо залучений до напрацювання та реалізації інструментів міжнародної підтримки української ОПК-індустрії, зокрема доступ до «Данської моделі», грантів, кредитів, інвестицій та інших можливостей від країн-партнерів.
- Недостатній доступ до фінансування для підприємств ОПК, складнощі з отриманням фінансування та підтримки на вигідних умовах, необхідність розширення податкових та митних пільг.
- Відставання у сфері стандартів, багато підприємств продовжують використовувати застарілі радянські ГОСТи.

Що може допомогти розв'язати ці проблеми, за ТСУ:

- Розвиток міжнародних партнерств (B2B та B2G) для інвестування та підтримки українських виробників ОВТ, а також підсилення голосу приватної індустрії в рамках міжнародної оборонної співпраці України, зокрема між індустріальної.
- Забезпечення українським оборонним підприємствам доступу до ефективних кредитних програм, а також — створення сприятливих економічних й податкових умов для ведення бізнесу.
- Державні стандарти ОПК повинні бути наближені до сучасних міжнародних стандартів НАТО — STANAG.

Із «джунглів» в «оборонну долину»

Виконавча директорка ТСУ Катерина Михалко ставить зустрічне питання: «А які інші галузі в Україні, крім оборонної, можуть створювати високотехнологічний експорт, який приноситиме валютний виторг і податки в бюджет?».

Можна було б згадати про галузь IT, проте її експорт спадає: у 2021 році він складав $6,9 млрд, а у 2024 році — $6,4 млрд. Тож не дивно, що Андрій Побережнюк з Kara Dag Technologies називає Defense Tech «новим IT». Однак щоб не втратити цей потенціал, українському суспільству та державі необхідно допомогти оборонним стартапам. Інакше «оборонна долина» може так і залишитися «джунглями», у яких виживуть лише найсильніші компанії.

РОЗМОВА З ВІЙСЬКОВИМИ: ЩО ПОТРІБНО НА ПОЛІ БОЮ І ЯК ШВИДКО ТЕХНОЛОГІЮ ПОТРАПЛЯЮТЬ НА ФРОНТ

Перша повністю роботизована наступальна операція, штучний інтелект, що допомагає шукати противника, та дрони, які здатні доставляти їжу та воду на позиції, евакуювати поранених чи навіть вести вогонь по ворогу. Те, що вчора здавалося науковою фантастикою, сьогодні вже можна зустріти на фронті.

Ми поговорили з військовими з 12-ї бригади НГУ «Азов», Третьої окремої штурмової бригади, окремого 108-го батальйону «Вовки Да Вінчі» та 13-ї бригади оперативного призначення НГУ «Хартія» про те, як зараз виглядає розвиток технологій у війську, чого не вистачає на полі бою і як швидко новітні розробки потрапляють на фронт.

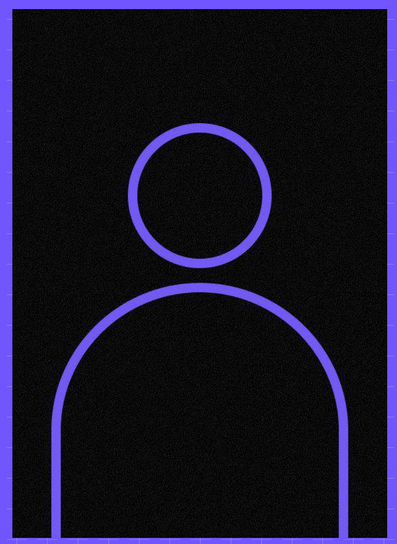
ТЕХНОЛОГІЧНИЙ СТРИБОК ВІД ПОЧАТКУ ПОВНОМАСШТАБНОГО ВТОРГНЕННЯ

ДМИТРО (ДІМІТОС) ПАВЛЕНКО-КРИЖЕШЕВСЬКИЙ

начальник розвідки 12-ї бригади НГУ «Азов»

«Коли я вийшов з полону після Маріуполя, уже всюди були Starlink та дрони; просто на КП ми могли бачити трансляції всього, що відбувається. Це для мене було великим досягненням в плані технологій»

Він на війні від її початку — з 2014 року. Каже, якби тоді йому сказали, що зараз бойові дії будуть такі — з масовим застосуванням дронів і наземними роботизованими комплексами — не повірив би.



ІНОКЕНТІЙ РАЗУМОВ

консультант благодійного фонду «Повернись живим»

«Стан справ в 2014-му і нині — речі, які абсолютно не до порівняння. На початку війни ми були з абсолютними мінімумом, який тільки можна уявити: жодних програм ситуаційної обізнаності, їхньої масштабованості у військах, мінімальна кількість навчених людей. Також можемо говорити про низький рівень цифровізації війська та використання технологій і, відповідно, майже повну відсутність людей, які вміють ці технології застосовувати.

Зараз же ми говоримо і про БпЛА, і про наземні роботизовані комплекси, і про використання Starlink, про можливість електронного документообігу тощо. На початку війни, в 2014 році, ми вступали у війну, яка велась старими методами»

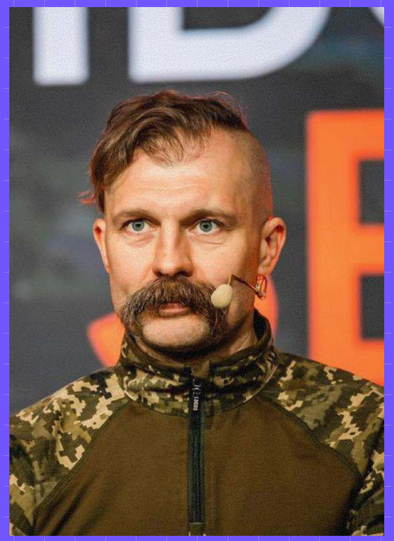
Однак, зміни відчутні навіть якщо порівнювати технологізацію війська не з 2014 роком, а з початком повномасштабного вторгнення.

«Зараз майже повністю управління переведено в цифровий вигляд. «Дельта», «Кропива» — це фактично дві основних системи управління підрозділами. Я вже не кажу про дрони. Більшість підрозділів управляють своїми бійцями за допомогою дронів: підтверджується маршрут пересування, виконання наказів і так далі. Що вже казати про роботу з артилерією», — каже Дімітос.

Щодо розвитку БПЛА, нині складно уявити лінію фронту без дронів: розвідувальних і ударних, таких, що летять не більше як на 5 кілометрів чи тих, що можуть вражати цілі глибоко в тилу противника.

Масове використання безпілотників на полю бою стало ледь не технологічною революцією, адже практично це унеможливило використання звичних для країн НАТО тактик ведення бою, писала The Wall Street Journal ще наприкінці 2023 року.

При цьому більшість інноваційних змін в армії починалася «з низів» — від самих бійців. І в цьому перевага над росіянами, переконаний керівник Служби роботизованих систем «Вовків Да Вінчі» Олександр Ябчанка.



ОЛЕКСАНДР ЯБЧАНКА

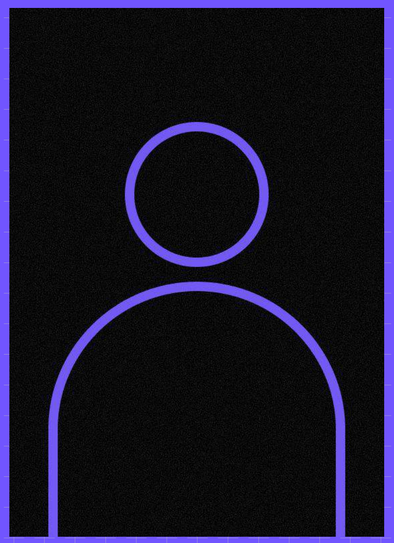
керівник Служби роботизованих систем «Вовків Да Вінчі»

«Ми коли ще тільки починали літати на «Мавіках» і навчали бійців з інших підрозділів, то вчився хто був: і піхотинець, і артилерист. Тобто ти «по штатці» один юніт, а по факту — ти той, кого в штатці ще навіть немає. Далі держава дослухалася до того, що ми робили, і змінила штатний розпис. Так само відбувається зараз і з НРК»

Усі технологічні зміни у війську розвивалися з бажання зберегти особовий склад і зменшити особовий склад противника. Російська армія кількісно переважає українську, тож аби перемогти, треба системно інвестувати час та гроші у розвиток технологій. Завдяки такому підходу, каже Олександр Ябчанка, від червня 2024 року на Покровському напрямку «Вовки да Вінчі» випереджали противника у плані технологій на пів кроку.

«Що стосується високотехнологічних засобів, назвемо їх інноваційними, зазвичай йдеться про безпілотні системи. От в цій компоненті ми мали перевагу. Якщо кількісно навіть противник мав паритет — кількісно може бути більше Mavic чи FPV — результат був на нашу користь. Чому? Тому що ми вміли цим користуватися. Ми постійно намагаємося бути хоч на пів кроку попереду в плані технологій», — говорить Олександр Ябчанка.

Аби досягти технологічної переваги над ворогом, підрозділи шукають різні шляхи: створюють R&D (Research and Development) підрозділи, майстерні, де удосконалюють засоби, які отримують від держави чи волонтерів, або окремі підрозділи, котрі займаються постійним пошуком новинок на ринку та комунікацією із виробниками.



МАТЕМАТИК

керівник Служби роботизованих сисофіцер служби БПС напрямку НРК у 13-ій бригаді НГУ «Хартія».тем «Вовків Да Вінчі»

«По різних напрямках закріплені компетентні люди. Це є основна задача — постійно моніторити, шукати і думати про будь-які нові технологічні можливості. Перший варіант — це постійно дивитися по виробниках і, бачачи навіть недосконалу систему, зв'язуватися з ними і допрацювати розробку спільно, поєднувати з іншими системами. Або маючи ідею, передавати її компаніям, які можуть цю ідею реалізувати»

ВІКТОР (СТАРК) ПАВЛОВ

боєць 3-ї ОШБ

«Ми почали з БПЛА, а точніше створили майстерню з мавіків. І зараз повний цикл розробки закривається в бригаді. Тобто є майстри, майстерня, і все це ми робимо самі. Потім об'єдналися з хлопцями і зробили майстерню по боєприпасах. Згодом почали займатися НРК. І як влізли туди, зрозуміли, що там багато нюансів. Почали досліджувати, їздили до різних виробників в Україні, знайомилися, дивилися на засоби»

Однак, попри стрімкий розвиток технологій, основною опорою і ресурсом Сил оборони України є передусім люди, вважає консультант «Повернись живим» Інокентій Разумов.

«Наразі технологічною опорою є не засоби, а люди — фахові, навчені, кваліфіковані. Можна взяти класний технологічний засіб, з великими можливостями, і наситити ним лінію фронту, але якщо немає людей, які вміють ефективно ці засоби застосовувати — це не матиме жодного сенсу та тієї результативності, яку могло б мати. Тому наразі фронт здебільшого «тримається» на ефективних людях. На фахівцях, які постійно поглиблюють свої знання, ще й часто навчають сусідні підрозділи. Саме вони є рушіями розвитку», — говорить Разумов.

ВІКТОР (СТАРК) ПАВЛОВ

боєць 3-ї ОШБ

«Чому НРК? Тому що вони реально рятують життя і здоров'я піхотинців. Тому що це невід'ємна складова всього процесу ведення бойових дій. Тому що це реальна технологія, яка може замінити в якійсь мірі піхотинця на полі бою»

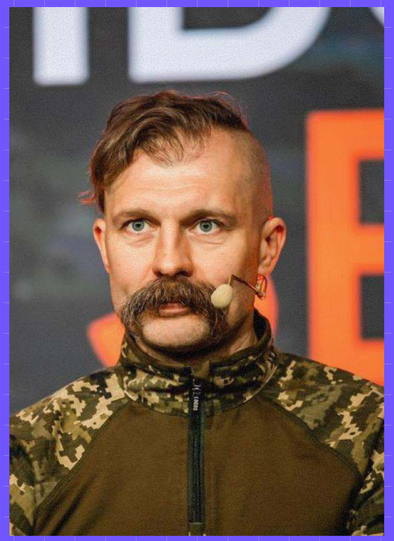
Наприкінці 2024 року 13-та бригада НГУ «Хартія» повідомила про проведення повністю роботизованої наступальної операції. Для штурму противника підрозділ використовував безпілотники та наземні роботизовані комплекси.

«Важливо розуміти, що центром самої цієї операції слугували не засоби, які диктують умови використання, а задум командира. Він для проведення такої операції має розуміти противника: слабкі його місця, які можна використати. А потім посилити свою позиції інструментом, який він має», — пояснює «Математик», офіцер служби БПС бригади, який брав участь у підготовці роботизованого наступу.

Як розказують у «Хартії», операція повністю себе виправдала. Та попри такий успіх, НРК в Силах оборони — поки новий засіб і до його масового використання ще далеко.

Хоча в майбутньому наземні роботизовані комплекси можуть забрати на себе чимало задач: логістику, евакуацію поранених і загиблих, мінування та розмінування територій, вогневу підтримку чи навіть розвідку, впевнений керівник Служби роботизованих систем «Вовків Да Вінчі» Олександр Ябчанка.

Саме через такий широкий спектр застосування та можливість зберегти життя та здоров'я більшій кількості бійців, віддавши частину задач на передовій роботам, цей напрям у себе взялися розвивати і у «Вовках Да Вінчі», і в «Хартії», і в «Азові», і в Третій штурмовій.



ОЛЕКСАНДР ЯБЧАНКА

керівник Служби роботизованих систем «Вовків Да Вінчі»

«Однак треба розуміти, що люди нерідко бачать чи чують те, що їм хотілося б чути. Думають, що все: раз роботи вже воюють, то можна не мобілізуватись, бо є кому. Це так не працює. Щоб роботи почали воювати, навпаки, людей треба більше. Просто ризик для цих людей буде неспівмірно менший»

ВІД «ВОЛОНТЕРСЬКИХ» ЕКСПЕРИМЕНТІВ ДО ШТАТНИХ СТРУКТУР

На початку лютого 2024 року міністр оборони України Рустем Умєров повідомив, що Міноборони запускає проєкт, який має масштабувати застосування безпілотних наземних комплексів у війську.

«Україна збільшує обсяги виробництва цих систем і розгортає повноцінні роботизовані підрозділи у складі бойових бригад Збройних сил на лінії фронту. Цей проєкт ґрунтується на досвіді випробувань, які проводилися з літа 2024 року у співпраці з військовослужбовцями», — написав міністр.

МИКОЛА СМЕТАНЮК

консультант БФ «Повернись живим»

Микола Сметанюк, консультант БФ «Повернись живим», каже, що така ініціатива Міноборони стимулює зацікавленість до цього процесу, що зі свого боку робить певні кроки на зустріч виробникам.

«Декларація Міноборони щодо розвитку галузі — це досить гарна ідея і важливий крок який потребує виважених рішень, щоб забезпечити військових саме якісними продуктами, оскільки на ринку багато нежиттєздатних засобів, які можуть потрапити до війська. І таким чином створювати негативне ставлення до цього напряму загалом»

«Вовки Да Вінчі» починали експериментувати з використанням НРК ще з середини 2023 року, тестуючи на полі бою турель «Шабля» — автоматизована система, що допомагає бійцям вести вогонь по ворогу дистанційно. Уже на початку 2024 «Шаблю» вперше законтрактували для війська.

У 2024 році НРК приділяють вже більше уваги. МО заявляє про розвиток сфери, кластер оборонних технологій Brave1 проводить масштабні випробування, залучивши одночасно понад 70 українських наземних роботизованих комплексів від 50 виробників, а бойові бригади починають використовувати комплекси для виконання завдань на фронті.

Однією з таких бригада стала Третя ОШБ, яка весною 2024 року на Авдіївському напрямку почала застосовувати наземні дрони.

ВІКТОР (СТАРК) ПАВЛОВ

боєць 3-ї ОШБ

«Ми створили майстерню НРК, R&D центр з наземних дронів і почали їх покращувати, робити більш адаптованими до бойового застосування. У 2024 році ми розробили штатну структуру, і за кілька місяців у нас з'явилася, мабуть, перша в Силах оборони штатна структура наземних роботизованих комплексів»

Системно виконувати бойові задачі за допомогою роботизованих комплексів почали улітку 2024 року і на Покровському напрямку «Вовки Да Вінчі», розказує Олександр Ябчанка та наводить приклад застосування НРК для виконання логістичних задач.

«Червень минулого року, Красногорівка, страшна спека, і всі шляхи логістики проглядаються противником. І подолати людині цей логістичний шлях, аби доставити на позицію воду чи їжу — величезний ризик. Я на той час був командиром піхотної роти і в мене на одній позиції, ключовій, з якої всі інші брали поповнення, було 178 бутилок води. Зрозуміти цю цифру може хіба що людина, яка воювала в спеку. Доставити їх вдалося за допомогою НРК», — розказує Ябчанка.

У таких випадках переваги роботизованих комплексів очевидні.

ВІКТОР (СТАРК) ПАВЛОВ

боєць 3-ї ОШБ

«Один дрон може тягнути 200-300 кілограм, один піхотинець — 20 кілограмів. Виходить, дрон замінює 10 проходок людини туди і назад або 10 людей. А зараз все складніше переміщатися через використання FPV та дистанційне мінування»

«Вміння» НРК нести великі вантажі дає змогу доставляти не тільки провізію на позиції, а й вибухівку на позиції російських військових. Так, у квітні 2024 року міністр цифрової трансформації Михайло Федоров повідомив, що бійці батальйону «Вовки Да Вінчі» провели операцію з використанням НРК «Гієна», котрий створив учасник Brave1 UGV Laboratory. Робот завдав удару по місцю скупченню особового складу ворога.

«Цей об'єкт був однією з локацій, де регулярно збиралася ворожа піхота, тому враження цієї цілі було критично важливим для стримування противника», — написав Федоров.

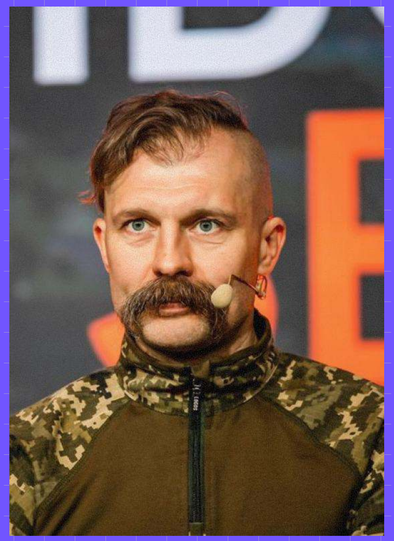
Керівник Служби роботизованих систем «Вовків Да Вінчі» Олександр Ябчанка розповів, що підрозділ нині активно працює над тим, аби збільшувати вагу вибухівки, яку може перевозити такий дрон.

«Я сподіваюся, що вже найближчим часом зможемо доставляти росіянам подаруночки у вигляді 500-кілограмових КАБів», — говорить Олександр Ябчанка.

Усе через те, що попри перспективність засобу він все ще має свої недопрацювання та проблеми. Серед основних проблем, які визначають військові:

- прохідність (засіб поки не універсальний в плані прохідності по складній місцевості);
- проблеми зі зв'язком;
- недостатній захист від БПЛА;
- висока ціна;
- вага та розміри засобів (екіпаж НРК має включати більшу кількість людей, ніж екіпаж БПЛА);
- брак навчених операторів.

Та попри наявні проблеми, ринок НРК продовжує активно розвиватися. Так, тільки від початку 2025 року Міноборони кодифікувало та допустило до експлуатації у Силах оборони шість наземних роботизованих комплексів: НРК «Гімлі», НРК Spextr, гексодрон «Тесля», НРК «Гулівер», НРК «Лють» та керовану самохідну броньовану платформу UNEX UGV.



ОЛЕКСАНДР ЯБЧАНКА

керівник Служби роботизованих систем «Вовків Да Вінчі»

«Нам зараз просто необхідно більше досвіду та грошей спрямувати на НРК. Тому що досвід і гроші даватимуть нам можливість отримувати все кращі і кращі засоби. Знову ж повертаємось до FPV. Ще півтора року тому це було казна-що, з них багато хто сміявся. Зараз це досконалий засіб вбивства. Чому? Тому що ми нескінченну кількість разів робили оновлення. Кожна наступна FPV-шка ставала кращою за попередню. Зараз нам треба пройти цей самий шлях з НРК»

Так вважає і консультат «Повернись живим» Микола Сметанюк. Він припускає, що за умови активної роботи роботи над покращенням виробів — фаховості та гнучкості виробника і якісного зворотного зв'язку від експлуатантів — вже за рік можна буде вийти на якісний та передбачуваний продукт.

«Галузь активно розвивається, на ринку вже є більше 10 виробників з непоганими продуктами. Якість НРК на даний момент я б оцінив на 6 з 10. Але порівнюючи з попереднім роком це інші і якісніші продукти. Цілком природний і багатоетапний процес. Оскільки це новий напрям, який ставить перед виробниками багато інженерно-технічних задач, які в співпраці з військовими вирішуються для появи якіснішого продукту, що повинен реалізовувати запити військових в умовах сучасної війни», — говорить Сметанюк.

РОЗВИТОК БПЛА

Більшу частину розповіді про технології у війську ми присвятили НРК, бо це новий, ще не до кінця зрозумілий, але, як відзначають військові, із якими ми поспілкувалися, перспективний напрямок. Однак основну технологій в армії нині складають БПЛА. На них тримається виконання більшості задач: розвідка, коригування, враження різного роду цілей як на лінії бойового зіткнення, так і в глибокому тилу.

Попри різноманіття виробів у цьому сегменті, військові зазначають, що мають потребу, зокрема, в ударних дронах, що здатні летіти на відстань більш як 30 км від лінії фронту.

ДМИТРО (ДІМІТОС) ПАВЛЕНКО-КРИЖЕШЕВСЬКИЙ

начальник розвідки 12-ї бригади НГУ «Азов»

«Сильно бракує чогось на кшталт російського “Ланцета”. Як СЕТ, але щоб їх почали в нормальній кількості видавати, їх сильно не вистачає, фактично їх немає, тому що ні на одне із рішень наразі не можна написати заявку й отримати. Не вистачає FPV на оптиці. Хоча вони зараз вже потроху починають заходити у війська»

Українських аналогів російського ланцету справді небагато. Перш за все тому, що виробництво дороге й тривале.

«Виробів такого формату небагато, менше ніж 10. Можна конкретно пройтися, поспілкуватися ґрунтовно і з виробниками, і з самим підрозділом, почути їх, дізнатися, щоб вони хотіли бачити й уже потім ухвалювати рішення», — пояснює Інокентій Разумов.

Вичерпного переліку «українських ланцетів» ми не знаємо, оскільки деякі компанії-виробники обирають лишатися не публічними із безпекових міркувань.

Чи не найпублічнішою є компанія DEVIRO. Вони на ринку з 2014, і минулоріч презентували на Міжнародній виставці Eurosatory 2024 ударний дрон під назвою «Булава». Він найбільше схожий на російський аналог, зокрема через X-подібні крила.

Про інший український «ланцет» — дрон CET від компанії Airlogix — нещодавно розповів керівник БФ «Повернись живим» Тарас Чмут. Саме цей БПЛА, але в досить обмежених кількостях, і використовують у бойових умовах уже кілька місяців бійці «Азову».

Є у цій категорії й іноземні аналоги. Наприклад, Switchblade 600, HX-2 від Helsing та WARMATE. Однак, всі вони значно дорожчі за українські вироби.

Окрім того, «Дімітос» відзначає, що «Азову» для виконання задач на тій ділянці фронту, яку вони тримають зараз, бракує і малих розвідувальних крил.

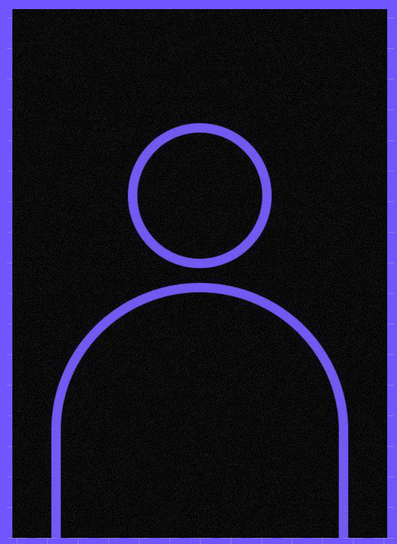
«Нам для розвідки потрібно щось дешеве, що можна було втратити для отримання інформації. Бо та ж «Лелека» — це все ж досить дорого, щоб використовувати у погану погоду чи розуміючи, що є ризик втрати з інших причин», — каже військовий.

ЯК ШВИДКО НОВІ РОЗРОБКИ ПОТРАПЛЯЮТЬ НА ФРОНТ?

Попри те, що за більш як три роки повномасштабного вторгнення українське військо отримало на озброєння чимало нових технологій, шлях нової розробки від ідеї до перших виробів, які можна тестувати у бойових умовах, може тривати місяцями, говорить Дмитро Павленко-Крижешевський.

«Ми купували GOR у Airlogix, ще перші зразки, трохи більше року тому, десь січень 2024 року. І вони нам ще тоді говорити про розробку ударного БПЛА — CET, який, якщо все буде добре, можна буде також нам протестувати. Але фактично протестували ми його майже через рік часу», — каже боєць «Азову».

Про такі терміни нині говорять і в компанії DEVIRO, котра працює над виробництвом дронів з 2014 року.



ДЕНИС ЧЕРЕДНИЧЕНКО

співвласник
компанії DEVIRO

«Шлях від розробки до використання військовими на фронті нових зразків вітчизняного озброєння скоротився майже до одного року. Насправді, це короткий термін, і важливо зазначити, що йдеться не про світовий ринок, ми говоримо лише про внутрішню потребу для Сил оборони України в умовах повномасштабної війни.

На сьогодні майже всі процеси рухаються набагато швидше, ніж 10 років тому, коли ми тільки починали, і цьому сприяють державні установи й організації, такі як Brave1 та Мінстратегпром»

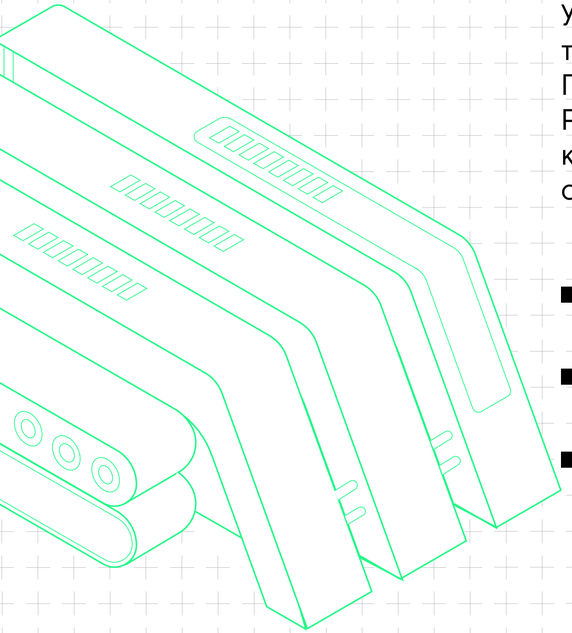
Та попри це динамічність змін технологій на полі бою часто не залишає виробникам багато часу на лабораторні тестування, тож вдосконалювати продукт часто доводиться вже у бойових умовах, спілкуючись напряму із військовими. Окрім того, важливо розуміти, що більшість безпілотних систем, випущених ще три роки тому, вже не відповідають вимогам сучасної війни.

«Ми зараз увійшли в нову еволюційну спіраль військового мистецтва. Як була індустріальна революція, то зараз у нас військова революція. Тобто, якщо колись воювали луками і стрілами, потім з'явилася артилерія, катапульти, потім порох, потім кулемети, танки, авіація, потім ядерна зброя, то зараз технологічна, роботизована зброя. Нас чекає менше залучення людей і більше використання дронів», — підсумовує Віктор «Старк» Павлов з Третьої ОШБ.

РОБОТА ДЕРЖАВИ У СФЕРІ: РЕГУЛЮВАННЯ СФЕРИ, ЗАКУПІВЛІ, БЮДЖЕТ, БРОНЮВАННЯ, ЕКСПОРТ

Що держава вже робить для розвитку українських Defense Tech компаній:

1. КЛАСТЕР ОБОРОННИХ ТЕХНОЛОГІЙ BRAVE1



У 2023 році за ініціативи Міністерства цифрової трансформації у партнерстві з Міноборони, Генштабом, Мінстратегпромом, Мінекономіки та РНБО створено платформу Brave1 — координаційний центр для розвитку інновацій у сфері оборони. Серед завдань кластера:

- об'єднати Defense Tech компанії, військових і державні інституції;
- надати юридичну, експертну та фінансову підтримку стартапам;
- пришвидшити процедури допуску технологій до бойового використання.

«Ми почали роботу у 2023 році, коли запускали кластер Brave1. Тоді стан в обороні був фрагментованим — не було системного об'єднання розробників і військових, бракувало координації та інституційної підтримки. Наприклад, на момент запуску не існувало жодного наземного робота, а у сфері РЕБ/РЕР було лише близько 10 рішень. Сьогодні — понад 3600 Defense Tech розробок на платформі, сотні з них вже кодифіковано за стандартами НАТО й застосовано на фронті. Завдяки Brave1 з'явилися нові напрями, як-от окопний РЕБ і дрони-перехоплювачі. Ми змогли об'єднати ринок, запустити конкурси та масштабувати технології, які реально рятують життя на полі бою», — коментують у Brave1.

Віцепрем'єр-міністр — міністр цифрової трансформації Михайло Федоров каже, що Мінцифри тоді зайшли у сферу Defense Tech з дронів як полісімейкер розвитку сфери.

«Уже у 2022 році зрозуміли, що це буде війна дронів. Саме тому почали розвивати проєкт "Армія дронів", який потім переріс у масштабну державну програму. Ми аналізували, які політики ухвалюють у світі, щоб технологій під час війни ставало більше. Збирали виробників, щоб зрозуміти їхні потреби й блокери.

Разом з урядовою командою і за підтримки президента ухвалили більш ніж 30 революційних постанов і законів, які, по суті, відкрили ринок. Для порівняння: у 2022 році було сім компаній, які займалися дронами, зараз їх понад 500. 96% дронів, які закуповує держава, — українського виробництва.

Потім масштабували цей досвід на інші напрями — РЕБ, НРК, боєприпаси, порох. Ми показали собі й усьому світу, що можемо за кілька років створити високотехнологічну сферу», — каже Федоров.

2. ФІНАНСОВА ПІДТРИМКА СТАРТАПІВ І ПРОТОТИПІВ

У межах Defense Tech кластера Brave1 з липня 2023 року діє грантова програма. Як зазначають у Brave1, це бюджетні гроші. Фінансування можна використати на R&D, розвиток свого продукту. За цей період вже видано 500+ грантів на 2,2 млрд грн.

«Наразі максимальна сума гранту для розробників — 8 млн грн. Ми бачимо попит серед розробників на отримання фінансування, тож надалі працюємо над збільшенням кількості й обсягів грантів», — додає Михайло Федоров, віцепрем'єр-міністр — міністр цифрової трансформації.

Галузь ОПК є стратегічно важливою і для обороноздатності України, і для її економіки. Тож, кажуть в Технологічних силах України, потрібна підтримка з боку уряду щодо можливості для залучення приватного капіталу.

«З нещодавно запущених програм є можливість від Міністерства економіки для виробників комплектуючих для озброєння та військової техніки отримати гранти на придбання, доставку та монтаж обладнання. Таких можливостей має бути більше і приватний сектор повинен відчувати підтримку держави. Крім того, українському оборонному сектору попри його стрімкий розвиток, досі бракує механізму захисту інтелектуальної власності. Це вагомий маркер для нашої держави», — зазначають ТСУ.

3. СПРОЩЕННЯ ПРОЦЕДУР СЕРТИФІКАЦІЇ ТА ЗАКУПІВЕЛЬ

Технології, які показали ефективність на полі бою, можуть бути швидко схвалені через механізм «експериментального зразка», що дозволяє уникати тривалих бюрократичних затверджень.

Також Brave1 фокусується на тому, аби українські розробники стали конкурентним на світовому ринку — для цього, за словами кластеру, українському Defense Tech потрібні інвестиції, розвиток виробництва й бізнес-експертизи.

«Brave1 вже працює над цим: у 2024 році залучено понад $40 млн, сформовано пул з 290+ інвесторів з України, США та ЄС, запущена менторська програма, проводяться Invest Days і метчмейкінг. Кластер відкритий до співпраці з міжнародними гравцями та допомагає перетворювати розробки в успішний бізнес», — кажуть в організації.

4. ПАРТНЕРСТВО З МІНОБОРОНИ ТА ГЕНШТАБОМ

Уряд допомагає Defense Tech компаніям знайти «замовника» з-поміж військових структур для проведення тестувань і подальшого впровадження.

«Brave1 тісно співпрацює з державними інституціями, зокрема з Генштабом ЗСУ та Міністерством оборони України, на всіх етапах роботи з оборонними розробками», — кажуть у кластері.

Процес співпраці такий: після того, як розробка проходить реєстрацію на платформі Brave1 та первинний комплаєнс, вона направляється на військову експертизу до Генерального штабу. Там понад 500 експертів у 12 технічних напрямках аналізують проєкт і протягом 5–7 робочих днів надають розгорнутий висновок.

«Якщо розробка отримує високу оцінку і визначається як пріоритетна, вона автоматично передається до Міністерства оборони. Команда Міноборони супроводжує її через усі необхідні процедури — від міжнародної кодифікації та включення до реєстрів НАТО до постачання на озброєння та оформлення державного замовлення», — додають у Brave1.

У Генеральному штабі ЗСУ додають, що передусім йдеться про менторську та консультаційну допомогу щодо надання виробником інноваційного проєкту на оцінювання уповноваженим експертним комісіям.

Так, запустили інтеграційну онлайн-платформу VIP1. З її допомогою Defense Tech-компанії можуть подавати заявки на отримання офіційної оцінки власної оборонної продукції без зайвої паперової роботи. Платформа містить всю потрібну інформацію щодо нормативної документації, порядку проходження оцінювання, його показників тощо.

Окрім цього, продовжують у Генштабі, запустили вебпортал «Залізний полігон». За аналогією з VIP1, компанії-виробники можуть подати заявки в режимі онлайн на проведення випробувань своїх військових розробок.

5. ЦИФРОВІЗАЦІЯ АРМІЇ

Генеральний штаб ЗСУ у коментарі AIN каже, що наразі пріоритетним напрямом розвитку Збройних сил є автоматизація і цифровізація управління військами та військового управління в цілому

«Йдеться про заміну паперових документів електронними, дистанційне керування озброєнням та військовою технікою, нарощування спроможностей для космічної підтримки операцій, розвиток штучного інтелекту в підготовці особового складу, здобуття вищої військової освіти, вдосконалення озброєння та військової техніки тощо», — кажуть у Генштабі.

Наприклад, Збройні Сили розробили та поступово впроваджують інформаційно-комунікаційну систему «Імпульс». Її завданням є автоматизація роботи служб забезпечення та супроводу персоналу, а саме: документальне забезпечення, облік особового складу тощо.

Цифровою трансформацією у війську займається й Міноборони, цей напрям до липня 2025 року очолювала CDTO Катерина Черногоренко.

«Цифрова трансформація допомагає українському війську позбуватися бюрократії та чинити супротив росіянам. Завдяки цифровим інструментам ми багато знаємо, багато бачимо та багато плануємо», — зазначає заступниця міністра оборони з питань цифрового розвитку, цифрових трансформацій і цифровізації.

Окрім цього, продовжують у Генштабі, запустили вебпортал «Залізний полігон». За аналогією з VIP1, компанії-виробники можуть подати заявки в режимі онлайн на проведення випробувань своїх військових розробок.

У контексті цифровізації війська найбільше згадують застосунки:

■ **Армія+** — сервіс для військових, де доступні документи та послуги, зокрема стандартизовані шаблони рапортів, які можна буде підписати та надіслати онлайн.

Наразі в застосунку доступні функції:

- Army ID — електронний військовий профіль на смартфоні, який підтверджує статус військовослужбовця;
- Електронні звіти — можливість подавати їх з будь-якого місця та відстежувати їхній статус. Для цього потрібен лише інтернет-зв'язок і кілька хвилин на заповнення;
- Опитування — можливість висловити свою думку щодо питань розвитку військової сфери.
- База знань: навчальні курси та програми, дотичні до військової сфери.

■ **Резерв+** —електронний кабінет призовників, військовозобов'язаних та резервістів для швидкого оновлення персональних даних без відвідування ТЦК.

■ **Оберіг** — єдиний електронний реєстр призовників, військовозобов'язаних та резервістів. Оберіг — інструмент військового обліку громадян.

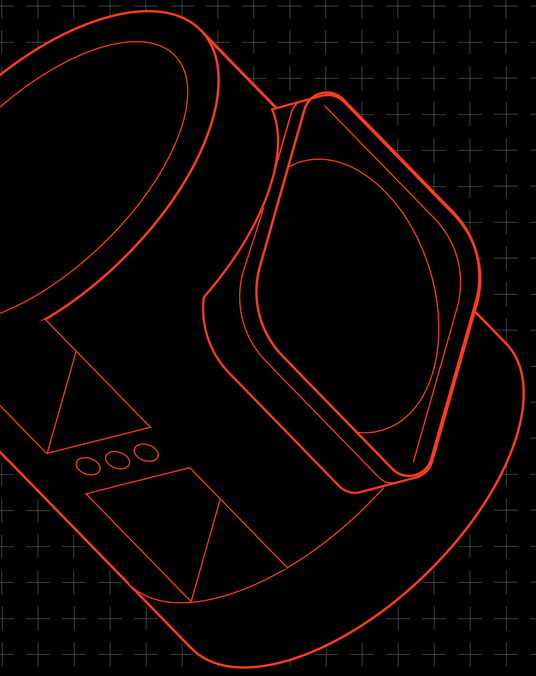
Ще у цьому контексті можна згадати систему DOT-Chain з автоматизації ключових процесів забезпечення підрозділів продовольством, додає Черногоренко. Система не лише перевела більшість процесів у цифровий формат, а й надає військовим, які відповідають за харчування, реальні інструменти контролю якості продуктів. У 2024 році система DOT-Chain скоротила час постачання продуктів для ЗСУ вчетверо.

«Тепер на її основі створюється модуль DOT-Chain Defence, який дозволить збирати онлайн запити від бойових підрозділів на БпЛА, РЕБ, наземні роботизовані комплекси тощо. Завдяки цьому модулю ми зможемо забезпечити потрапляння зброї зі складів виробників одразу на фронт — туди, де це справді потрібно, у справді необхідних кількостях», — каже заступниця міністра оборони з питань цифрового розвитку, цифрових трансформацій і цифровізації.

Черногоренко додає, що інші держави активно цікавляться українськими розробками, особливо європейські, оскільки, за її словами, перед ними зараз стоїть багато викликів, пов’язаних із потенційною військовою агресією росії.

«Ключові питання, в яких вони вбачають втілення цифрових рішень — це рекрутинг та мобілізація. Власне, якраз те, що ми вже робимо. Тому особливу увагу приділяють Резерв+ та його функціям», — говорить заступниця міністра оборони з питань цифровізації.

ШТУЧНИЙ ІНТЕЛЕКТ У ДЕФЕНС ТЕХ СФЕРІ: ВПРОВАДЖЕННЯ, ОБМЕЖЕННЯ, РОЗРОБКИ НА ОСНОВІ ШІ



Пошук ворожих цілей та ефективні влучання навіть під дією РЕБ противника — задачі, які вже вдалося успішно делегувати штучному інтелекту. Україна зараз активно працює над власними розробками та комунікує щодо впроваджень в оборонній сфері вже готових рішень.

Ми поспілкувалися із представниками кластеру для розвитку військових технологій Brave1, розробниками програмного забезпечення з ШІ та заступницею міністра оборони з цифровізації для того, аби дізнатися, який стан галузі в Україні зараз та розпитати про плани і перспективи.

ПЕРЕДУМОВИ РОЗВИТОК ШІ У ВІЙСЬКУ

У 2020 році уряд України схвалив Концепцію розвитку штучного інтелекту в Україні. Її реалізацію передбачали до 2030 року.

Що ж до штучного інтелекту в оборонній сфері, то Україна почала офіційно закладати фундамент для розвитку ШІ ще до повномасштабного вторгнення. У 2021 році Міністерство цифрової трансформації та Укроборонпром підписали меморандум про спільний розвиток цифрових інновацій у сфері оборони.

У Генеральному штабі ЗСУ пояснюють, що основними напрямами використання ШІ у Збройних силах України є: прискорення та підтримка прийняття рішень в системі військового управління та управління військами; аналіз великих масивів даних і вдосконалення розвідки, систем наведення, покращення точності тощо.

«Тобто ШІ уже став повноцінним бойовим інструментом. Він застосовується для автоматизованої обробки розвідувальних даних та аналізу відеопотоку з безпілотних засобів, що дає змогу оперативно виявляти техніку противника. Інтеграція інновацій не лише підвищує ефективність наших підрозділів, а й рятує життя українських військових», — коментують у відомстві.

Та найбільш стрімко ШІ у війську почав розвиватися все ж вже під час повномасштабного вторгнення.

У квітні 2023 року Міністерство цифрової трансформації, Міністерство оборони, Генеральний штаб Збройних сил, Рада національної безпеки і оборони, Міністерство з питань стратегічних галузей промисловості та Міністерство економіки запустили єдину координаційну платформу в галузі Defense Tech в Україні Brave1. Нова структура стала каталізатором для розвитку низки Defense Tech стартапів, серед них і чимало таких, що використовують штучний інтелект.

Першими ШІ-продуктами, з яких Brave1 починали ще в 2023 році, були системи автономності для дронів, зокрема, FPV. Ідеться про передові системи, які використовують машинний зір для виявлення та знищення цілей в автономному режимі, підвищуючи ефективність бойових дій.

Деякі з них, до прикладу розробку компанії «3IP», представили влітку 2024 року на хакатоні Precision від Brave1.

У Генеральному штабі ЗСУ пояснюють, що основними напрямами використання ШІ у Збройних силах України є: прискорення та підтримка прийняття рішень в системі військового управління та управління військами; аналіз великих масивів даних і вдосконалення розвідки, систем наведення, покращення точності тощо.

«Все більше і більше різних платформ і різних засобів намагаються використати штучний інтелект для автономності якогось функціоналу. Тільки моделей дронів, які мають на борту системи наведення, вже більше 70. І це лише один приклад», — розповіли нам у Brave1.

Загалом станом на травень 2024 року українські розробники зареєстрували на платформі Brave1 понад 1600 розробок. Із них понад 200 використовували методи штучного інтелекту та машинного навчання. І кількість таких розробок постійно збільшується, говорять Brave1.

ЯКІ РОЗРОБКИ З ШІ ВЖЕ ВИКОРИСТОВУЮТЬ НА ФРОНТІ

Як пояснюють у Brave1, загальноприйнятий світовий підхід використання штучного інтелекту в оборонній сфері базується на трьох ключових критеріях: наявність даних, час для ухвалення рішень та безпечність для людини.

«Такий підхід використовувався, зокрема, в армії США. Там це впроваджується на стратегічному рівні. Коли є велика кількість даних, їх можна дати машинам, які обробляють ці дані, приймають рішення. Машини можна навчити використовувати дані в захищеному середовищі. Наступний рівень — ухвалення рішень за менший час на основі менших масивів інформації або на основі масивів інформації, яка постійно оновлюється чи швидко надходить. Це тактичний, оперативний рівень, який допомагає командуванню на полі бою. Але це вже може нести більші ризики для людей. І третій рівень — безпосередньо на полі бою. Тут йдеться про автоматизацію якогось продукту», — пояснюють у Brave1.

Тобто класична світова модель використання штучного інтелекту — згори донизу. Тоді як в Україні, зважаючи на війну, частіше за все рішення ухвалюються навпаки — знизу вгору, тобто з розробок, які використовуватимуть безпосередньо на полі бою.

Розробки із використанням ШІ активно розвиваються як за сприяння держави, так і як приватні стартапи. До прикладу, компанія «3IP» працює над ШІ розробками з 2023 року. Її представники переконані, що у випадку, коли ворог має чисельну перевагу, ШІ є мультиплікатором сили на сучасному полі.

«ШІ дозволяє збільшити рівень автономності дронів, які не завжди можуть бути керовані оператором-людиною, але повинні продовжувати виконувати бойову задачу при відсутності зв'язку, навігації тощо, щоб зберегти життя бійців. Воювати і гинути мають машини, які легко відтворити, а не люди. Наша місія — уникнути, де можливо, прямого вогневого контакту з ворогом і дозволити дистанційне ураження за межами прямої видимості. Також в умовах асиметричної війни на виснаження із ворогом, який має чисельну та фінансову/промислову перевагу, ШІ — це мультиплікатор сили на сучасному полі бою», — додає директор та засновник компанії Twist Robotics Віктор Сахарчук.

AVENGERS

Серед розробок із використанням ШІ, які вже застосовують на фронті, — платформа Avengers. Завдяки ній Сили оборони отримують інформацію про 12 000 ворожих цілей щотижня. Нині платформа є частиною національної військової системи ситуаційної обізнаності DELTA.

«Через участь у найбільшій війні в Європі після Другої світової маємо унікальний доступ до фото та відеоматеріалів із технікою ворога. Завдяки системній роботі з цими даними (розмітка, анотація, структуризація) вдалося створити датасет із сотень тисяч об'єктів для навчання Machine Learning рішень. Щодо прогресу розробки: важливо розуміти, що машинне навчання — це передусім робота людей. Команда анотаторів за допомогою автоматизованих інструментів та чітких інструкцій обробляють окремі кадри з польотних відео, відмічають обмежувальними рамками об'єкти та присвоюють додаткові мітки», — пояснює ексзаступниця міністра оборони з цифровізації Катерина Черногоренко.

Розмову з Катериною Черногоренко ми записали у травні 2025 році. У липні стало відомо, що Черногоренко йде з посади заступниці Міністра оборони з цифровізації. Ми вирішили залишити її коментарі, аби підсумувати роботу міністерства у той час, коли Черногоренко ще працювала.

Навчання ШІ-моделі платформи Avengers на нових даних триває системно. Це дозволяє удосконалювати якість розпізнавання різноманітної ворожої техніки, навіть у складних умовах, наприклад танків, прихованих в лісових масивах, або БМП, що рухаються грунтовими дорогами.

Нині, як зазначає Черногоренко, модель автовиявлення знаходить 70% об'єктів інтересу на відеотрансляції із затримкою близько 2 секунд.

VEZHA

Платформа відеоаналізу поля бою Vezha восени минулого року стала частиною екосистеми DELTA як окремий модуль. Спочатку 411 окремий батальйон «Яструби» у складі Сил територіальної оборони створив платформу для власних потреб. Згодом Центр інновацій Міністерства оборони долучився до створення єдиної платформи відеоаналізу на базі DELTA, а команди стримінгових платформ Tube і Raven надали свій досвід і напрацювання.

Платформа надає інструменти для аналізу трансляцій, оптимізації взаємодії між підрозділами, пришвидшення циклів розвідки-ураження, а також оцінки ефективності екіпажів та використання засобів. У модулі реалізовані різні способи перегляду трансляцій та голосової комунікації, колективне дешифрування в режимі реального часу з автовиявленням техніки за допомогою Avengers, розповіла Катерина Черногоренко.

«Щодня з використанням Vezha відбуваються тисячі трансляцій та десятки уражень. І розробка триває: зараз команда активно працює над розширенням функціональності та глибшою інтеграцією з іншими модулями DELTA», — зазначила ексзаступниця міністра оборони з цифровізації.

СИСТЕМА ДОНАВЕДЕННЯ «ЗІР»

Система розроблена для самостійного виявлення цілей за допомогою штучного інтелекту або комп'ютерного зору та подальшого їх ураження в режимі автоматичного керування. Має вигляд окремого пристрою, який можна встановити на будь-який FPV.

Система не потребує додаткового оснащення дрона або станції керування. Управління дроном здійснюється за допомогою стандартного пульта. Система «ЗІР» має автоматичний детектор, який навчений визначати сім типів цілей. Як заявляють розробники, система може ефективно працювати і по рухомих цілях.

«Зараз система перебуває на тестуванні в кількох підрозділах, але до масового використання ще далеко. Перш за все, справа у людях — мало хто довіряє ШІ, всі говорять, що «краще руками». У багатьох випадках це правда, бо ШІ ще не все вміє робити краще людей. Конкретно з донаведенням була ситуація, що на ринку ще рік-півтора тому з'явились перші рішення, вони доволі масово почали поставлятись у війська, але були ще сирі. Тому зараз багато пілотів просто не вірять у те, що донаведення може працювати», — пояснює Олександр Чирва, співзасновник ТОВ «ЗІР Система».

TWIST ROBOTICS

Компанія спеціалізується на розробці та виробництві IP-камер і дронів. Ще улітку 2023 року вони предствили тестові відео свого програмного забезпечення на базі штучного інтелекту.

«Програмне забезпечення (в тому числі з елементами ШІ) є ефективним асистентом пілота (БПЛА, НРК), який дозволяє уникнути низку грубих помилок, що можуть призвести до втрати дрона чи невиконання бойової задачі. Важливим є сценарне планування в дизайні такої системи, яке збільшує ймовірність успіху оператора в умовах обмеженого часу для прийняття рішення чи неповних даних. Якщо мова йде про FPV, то є ланцюжок етапів, на кожному з яких можна мінімізувати відмову машини та збільшити успіх місії (долетіти і не впасти по дорозі через втрату зв'язку чи навігації, прицілитись в умовах обмеженого часу, долетіти до цілі після її підтвердження оператором навіть при втраті зв'язку з дроном)», — говорять в компанії.

Загалом, як пояснюють в Twist Robotics, ШІ рішення нині дозволяють щонайменше в 2-3 рази збільшити ефективність використання дрона при збільшенні його вартості на 25-50%.

Розробники заявляють, що вони забезпечують весь ланцюжок від ідеї до впровадження.

«Це включає, окрім всього іншого, навчання роботи зі ШІ. Це доволі складний та дороговартісний процес, але тільки так можна забезпечити впровадження та масштабування інновацій після їх створення. Помилково вважати інновацією розробку чи випуск продукту. Інновація в Defense Tech — це коли користувачі починають виконувати завдання на якісно новому рівні, не доступному раніше», — говорить директор та засновник компанії Twist Robotics Віктор Сахарчук.

Серед розробок компанії також застосунок «На Долоні», що дозволяє проводити обробку фото та відео розвідувальної інформації локально (без участі хмарних сервісів), бойовий симулятор польотів БПЛА та планувальник місій «ОБРІЙ», участь у розробці універсального військового датасету, який став основою Avengers.

Окрім того, компанія займалася оснащенням дронів першим українським модулем візуальної навігації по супутникових картах та ортофотопланах, що дозволяє польоти в умовах повного придушення чи відсутності супутникової навігації (400 літаків) та встановленням на БпЛА Saker Scout (ударний розвідник, ретранслятор) модуля візуальної навігації та автоматичного детектування військових об'єктів (400 одиниць).

DELTA — УКРАЇНСЬКА РОЗРОБКА, ЯКОЮ ЦІКАВЛЯТЬСЯ ПАРТНЕРИ

DELTA — національна військова система ситуаційної обізнаності, яка щодня допомагає знищувати ворожі об'єкти. До неї входять мобільний застосунок, військовий месенджер, безпечний стрімінг з поля бою, цифрова мапа, засоби планування роботи та інтеграції з іншими системами.

Система мала стрімкий розвиток. Улітку 2024 року Міноборони повідомили про її повну легалізацію та впровадження в українське військо, а вже восени DELTA увійшла в трійку найпопулярніших бойових систем, яку військові використовують найчастіше. Станом на березень 2025 року, DELTA системно використовують понад 90% бригад Сил оборони.

«Початково це була мапа ситуаційної обізнаності. Тепер вона стала екосистемою, об'єднала вже 11 модулів, які допомагають нашим військовим ефективно нищити ворога — бачити поле бою в реальному часі, планувати операції, обмінюватись інформацією в межах підрозділу, бригади, угруповання, а за потреби і з союзниками», — зазначає Катерина Черногоренко.

Сьогодні DELTA підтримує понад 50 інтеграцій, ще 30 перебувають у розробці. Серед модулів, наприклад, Mission Control для планування місій екіпажів БпЛА; Target Hub для планування й керування вогневою роботою підрозділів; Data Platform для збору, обробки й аналізу даних; DELTA Insights для отримання аналітичних відповідей на базі розвідданих тощо.

«Ключовий вектор розвитку DELTA — максимальне насичення єдиної картини поля бою актуальними даними з максимально широкого кола джерел. Підключаючи різноманітні датчики, трекери, інші військові інформаційні системи, зокрема «Кропиву», а також розвідувальні засоби — дрони, радари тощо — DELTA перетворюється на потужний аналітичний інструмент для ухвалення дієвих рішень у реальному часі. Військові додають у DELTA 1,2 млн міток щомісяця та знищують за допомогою системи понад 2,000 підтверджених цілей щодня», — пояснює ексзаступниця міністра оборони з цифровізації Катерина Черногоренко.

СПІВПРАЦЯ З ПАРТНЕРАМИ В РОЗВИТКУ ШІ

Черногоренко також розповідає, що західні партнери проявляють зацікавленість у купівлі бойової системи DELTA.

«Їх приваблює, що це продукт, який поєднує сучасні технології та стандарти НАТО, а найголовніше — він загартований реальним бойовим досвідом. Цей досвід вплинув на кожну функцію, забезпечивши її ефективність», — зазначила Черногоренко.

За словами заступниці міністра, Україна нині розглядає цей інтерес як можливість капіталізувати унікальну спроможність та вивчає різні варіанти співпраці та потенційного продажу.

«Хоча конкретна модель поширення ще обговорюється, ми впевнені, що DELTA має великий експортний потенціал і може стати одним із важливих інструментів безпеки для багатьох країн, які шукають надійні та перевірені війною рішення», — каже ексзаступниця міністра.

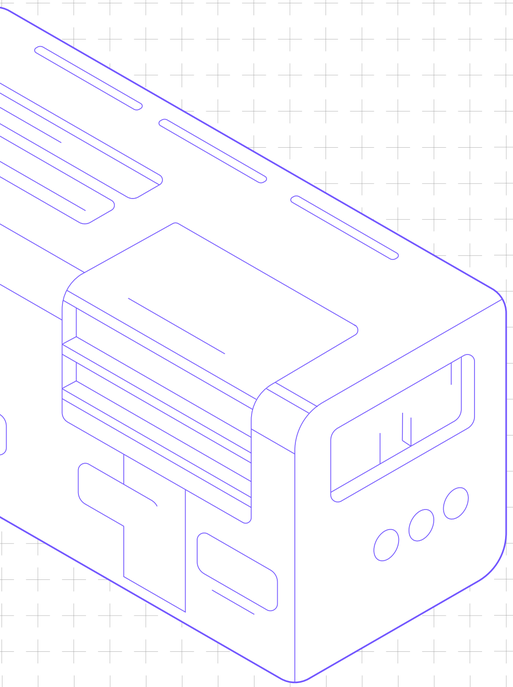
Загалом Міноборони активно комунікує із партнерами щодо різних варіантів співпраці у питаннях використання штучного інтелекту в оборонній сфері.

Так, ексзаступниця міністра оборони з цифровізації Катерина Черногоренко у травні 2024 року зустрічалася з представниками німецької компанії Helsing, яка займається інтеграцією штучного інтелекту в оборонні технології. Компанія пропонувала посилити програмні рішення щодо протидії швидкому розвитку РЕБ, а також коштом своїх розробок допомогти українським безпілотникам вражати цілі навіть при втраті зв'язку.

«Розвиток оборонних технологій вже досяг високого рівня. Використання інструментів штучного інтелекту може змінити хід війни. Взаємодія з компаніями, що готові інтегрувати рішення ШІ у вже готове програмне забезпечення, — наступний крок», — зазначила Катерина Черногоренко.

КІБЕРБЕЗПЕКА І ЇЇ РОЛЬ У ПОВОЄННІЙ УКРАЇНІ

ПЕРЕМОГА ЯРОША НА ВИБОРАХ У 2014-МУ, NOTPETYA ТА ЗЛАМ СУПУТНИКА VIASAT. ЯК РОСІЯ АТАКУВАЛА УКРАЇНУ В КІБЕРПРОСТОРІ З ПОЧАТКОМ ВІЙНИ



Хоч рф активувала кібератаки на Україну наприкінці 2013-го, повідомляють у Міноборони, російська-українська війна в кіберпросторі почалася паралельно з розгортанням бойових дій на українських територіях.

У перший рік війни, 25 травня 2014 року, російські хакери вивели з ладу інформаційну систему Центральної виборчої комісії (ЦВК) України «Вибори», намагаючись змінити результати і зробивши переможцем тодішнього очільника партії «Правий сектор» Дмитра Яроша. Раніше, у квітні, так звану «візитку Яроша» використовували як частину російської пропаганди, тож легко прослідкували слід рф у спробах вплинути на настрої українського суспільства через підтасування результатів виборів.

Контекст. У 2014-му президентські вибори в Україні відбулися позачергово, після втечі тодішнього президента Віктора Януковича. Вони відбулися в один тур, оскільки кандидат Петро Порошенко набрав понад 50% голосів виборців. Водночас в рф на провладному пропагандистському «Першому каналі» показали сюжет, в якому йшлося про перемогу Дмитра Яроша, кандидата від «Правого сектора».

Кількома місяцями пізніше — у липні 2014-го — атакували і вебпортал президента України, який внаслідок атаки був недоступний кілька годин.

У листопаді 2015 року українська енергетична мережа зазнала атаки, ймовірно організованої групами, пов'язаними з рф. Внаслідок атаки 230 000 споживачів на заході України залишилися без електропостачання на період до шести годин.

У 2017-му глобальні збитки — орієнтовно 10 млн — спричинив вірус NotPetya, який в Білому домі назвали найбільш руйнівною та найдорожчою кібератакою в історії. Вперше офіційні органи Заходу публічно приписали відповідальність за кібератаку групам, пов'язаним із російським урядом — йдеться про росіян з хакерського угруповання Sandworm. У 2022-му США оголосили винагороду у 10 млн за інформацію про шістьох працівників російської розвідки, які могли бути причетними до організації кібератаки за допомогою NotPetya.

Приблизно за місяць до повномасштабного вторгнення — 14 січня 2022 року — сайти Міноборони та Міністерства закордонних справ України атакували. Хакери залишили на сайтах повідомлення: «Українці!... Вся інформація про вас стала публічною. Бійтеся і чекайте гіршого. Це ваше минуле, теперішнє і майбутнє». Наступні атаки не змусили на себе чекати: їх влаштували 15-16 лютого та 23 лютого — за день до повномасштабної війни.

24 лютого 2022-го росія розпочала велику війну проти України. Паралельно з обстрілами рф атакувала і кіберпростір. Зокрема, наслідки зламу одного з супутників Viasat, який відповідав за надання українцям швидкісного інтернету, відчули у світі — низка європейських країн, серед яких Німеччина, Велика Британія, Франція та Чехія, мали проблеми з супутниковим інтернетом.

Протягом великої війни кількість кібератак рф зростає: у 2023-му росія здійснювала щонайменше 10 кібератак на день, заявив очільник внутрішньої розвідки країни Василь Малюк в інтерв'ю Independent.

Перший заступник голови Держспецзв'язку Ростислав Замлинський в коментарі для AIN повідомив, що у 2021 році було зафіксовано 1350 кіберінцидентів, у 2022-му — 2194, а в 2024-му — вже 4315. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Держспецзв'язку у 2024 році обробив близько три мільйонів подій інформаційної безпеки, з них 28 тисяч були критичними та потребували втручання фахівців.

Серед найсерйозніших викликів — масована атака на держресурси в січні 2022 року, масові DDoS-атаки у перші тижні вторгнення, атаки на енергетичні компанії, операторів зв'язку та державні реєстри, зокрема на «Київстар», Міністерство юстиції України та «Укрзалізницю», зазначили в CERT-UA в коментарі для AIN.

Замлинський також наголошує, що характер атак за роки повномасштабного вторгнення дещо змінився: ***«Окремо варто відзначити системну діяльність з кібершпигунства, яку ведуть спецслужби рф. У 2022-му акцент був на деструктивних атаках, у 2023 — на розвідці та прихованій присутності в системах, у 2024 — на об'єктах, пов'язаних з війною».***

Згідно з аналітикою Держспецзв'язку за друге півріччя 2024-го, минулого року Україна стикалася не лише зі знайомими кіберзагрозами з боку росії, як-от з боку головного управління генштабу збройних сил російської федерації та фсб, а і з новими гравцями, які «діють ще агресивніше та більш автоматизовано». Попри зменшення кількості критичних інцидентів, зросла їхня складність, тож потрібні більші ресурси для відбиття.

Водночас загальна кількість кіберінцидентів протягом другої половини 2024 року зросла на понад 48% порівняно з попереднім півріччям, йдеться в аналітиці Держспецзв'язку. За підсумками календарного року зростання кількості кіберінцидентів становить майже 70%.

У другій половині 2024-го збільшилася кількість кібератак, пов'язаних з розповсюдженням шкідливого програмного забезпечення (ШПЗ).

У 2025 році спостерігається тиск на критичну інфраструктуру та зростання складності атак і активності активістів, пов'язаних із рф, підсумовує Замлинський.

Кількість інцидентів, пов'язаних з ШПЗ	H1 2024	H2 2024	Зміна за період
Розповсюдження	531	1123	112%
Зараження	196	320	63%

Зростання кіберінцидентів, пов'язаних із зараженням ШПЗ, більшою мірою пов'язана зі збільшенням кількості шкідливих розсилок та збільшенням видимості, а меншою мірою — зі зміною ТТП*

дослідження Держспецзв'язку за друге півріччя 2024 р.

ПРОБЛЕМИ КІБЕРЗАХИСТУ В УКРАЇНІ

У кібербезпеці України, зокрема, у збереженні особистих даних громадян, досі залишаються прогалини. Це демонструє розслідування Kyiv Independent. Згідно з ним, протягом чотирьох років — з 2021-го до березня 2025-го — особисті документи українців (понад 900 тисяч файлів) з центрів технічних оглядів автівок зберігалися незахищеними на західному сервері.

Механізм потрапляння документів на сервер до кінця не з'ясували, водночас на питання про це журналістам не змогли відповісти у державних органах. Про витік інформації Держцентру кіберзахисту (CERT) повідомив ірландський спеціаліст з кібербезпеки та управління доступом Джейк Діксон — і не отримав реакції. У Kyiv Independent повідомили, що документи на сервері закрили перед виходом тексту про витік даних. Редакції AIN також не відповіли на питання про витік особистих даних українців.

В Україні зараз немає єдиного органу, який би встановлював стандарти, правила, контролював їх дотримання, проводив навчання, формував кіберполітику та розробляв відповідне законодавство, зазначає в коментарі AIN засновник і перший керівник CERT-UA при Держспецзв'язку, ексзаступник керівника відділу боротьби з комп'ютерною злочинністю при Департаменті контррозвідки СБУ Костянтин Корсун. Зараз, пояснює Корсун, відповідальність за кібербезпеку країни несуть щонайменше чотири організації: Держспецзв'язку, Національний координаційний центр кібербезпеки РНБО, Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ та Мінцифра.

Контекст. 30 червня 2023 року сфера електронних комунікацій перейшла у підпорядкування Мінцифри. Це відбулося в межах реформування Держспецзв'язку. Ще до повномасштабного вторгнення — в період з 2017-го до 2019-го — було відкрито кілька проваджень щодо діяльності структури, зокрема:

- У 2017 році Держспецзв'язку у змові з ТОВ «Спеціальні телекомунікаційні рішення» (код ЄДРПОУ 38811928) завдали збитків держбюджету на загальну суму 9,4 млн грн.

- У 2018 році Держбюро розслідувань знайшли ознаки того, що посадові особи Державного центру кіберзахисту Держспецзв`язку та ТОВ Фірми «Валтек» заволоділи майже 100 000 грн з держбюджету. Слідчі схилялися до думки, що договори між Мін'юстом і «Валтек» мали ознаки фіктивності й, можливо, метою підписання було заволодіння державними грошима.

- У 2019 році СБУ викрила зловмисників, які розкрадали виділені на захист секретної інформації в держустановах і силових відомствах України кошти. Зловмисники могли завищувати ціни на послуги — і, як наслідок, завдали держзбитків на суму 20 млн грн. Компанія-надавач послуги мала відповідну ліцензію від Держспецзв'язку, а серед її клієнтів у 2018-2019 — Нацполіція, Нацгвардія, АТ «Укрзалізниця», Міністерство молоді та спорту, ДП «УКРАЕРОРУХ», ДП «Укренерго».

20 листопада 2023 року Кабмін звільнив голову Держспецзв'язку Юрія Щиголя та його заступника з питань цифрового розвитку, цифрових трансформацій і цифровізації Віктора Жору. Національне антикорупційне бюро (НАБУ) та Спеціалізована антикорупційна прокуратура (САП) повідомили колишнім очільникам структури про підозру в корупції.

За рік — у листопаді 2024-го — очільника Держспецзв'язку Юрія Мироненка звільнили, а саме відомство перевели у підпорядкування Кабміну замість Мінцифри.

«Попри 11-й рік активної кібервійни, у нас досі немає єдиного центру національної кібербезпеки, який би міг би бути не тільки ідеологічним хабом та точкою довіри всередині країни, але також мозковим центром, базою для адаптації кіберзаконодавства із законодавством ЄС», — додає Корсун. Також, за його словами, такий центр також міг би слугувати єдиною точкою входу для іноземних партнерів.

Подібним витокам можна запобігти, якщо створити спеціалізований підрозділ кіберзахисту з кваліфікованими фахівцями, які буду застосовувати сучасні інструменти та практики, вважає Корсун: ***«Кіберпідрозділ аналізуватиме існуючі мережі та системи і робити їх безпечнішими, знижуючи ризики, впроваджуючи політики бекапів та резервування, запроваджуючи регулярні навчання персоналу».***

За його словами, ці процеси довгі та витратні, тож більшість державних установ не можуть і не хочуть їх реалізовувати: «Тим паче, що особливих покарань за недотримання кібербезпеки не передбачено через відсутність чіткої державної політики».

У Мінцифри в коментарі для AIN пояснили, що співпрацюють з органами кібербезпеки, як Державна служба спеціального зв'язку та захисту інформації, Служба безпеки, Рада національної безпеки та оборони, Національний банк, Генеральний штаб Збройних сил тощо.

«Крім того, ми перебуваємо у тісній взаємодії із міжнародними урядовими та неурядовими організаціями, сфера діяльності яких безпосередньо пов'язані з інформаційною та кібербезпекою, — зазначили в коментарі. Також Мінцифра обмінюється законодавчими ініціативами з країнами ЄС, впроваджуючи нові нормативно-правові акти, гармонізовані з регуляціями ЄС».

У CERT-UA в коментарі для AIN повідомили, що CERT-UA взаємодіє з усіма ключовими суб'єктами національної системи кібербезпеки, а також з державними органами, місцевою владою, силовими структурами, операторами критичної інфраструктури, приватним сектором: «Співпраця здійснюється відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» і включає обмін інформацією, спільну роботу над інцидентами, проведення навчань і практичних семінарів, а також взаємодію у глобальних мережах CSIRT, зокрема FIRST».

Відкриті дані як подарунок росіянам. Також серед кібербезпекових проблем, з якими стикається Україна, — відкриті дані в реєстрах, де міститься, наприклад, особиста інформація про директорів та власників оборонних підприємств — зокрема, з їхніми адресами. Цим можуть скористатися російські спецслужби: УП нагадує про замахи на людей, причетних до постачання зброї українській армії. Також залишається проблемою такі відкриті реєстри, як-от державний реєстр речових прав та земельний кадастр, де можна знайти інформацію про власність, призначення приміщень та ділянок землі.

ЯК УКРАЇНСЬКУ КІБЕРБЕЗПЕКУ ПІДТРИМУЮТЬ ІНШІ ДЕРЖАВИ?

- У 2023 році Велика Британія подвоїла підтримку кібербезпеки для України до 25 млн фунтів стерлінгів.
- Того ж року Україна та 10 країн-партнерів — Канада, Данія, Естонія, Франція, Німеччина, Нідерланди, Польща, Швеція, Велика Британія та Сполучені Штати — створили Талліннський механізм із кібербезпеки для захисту країни від кіберзагроз.
- USAID інвестувало близько $90 млн у проєкти кіберзахисту України за останні кілька років. Серед реципієнтів — Мінцифри, Апарат РНБО, Міністерство культури та стратегічних комунікацій, МОЗ, лікарня «Охматдит», ДСНС, «Укренерго» (перелік не є повним).
- Європейський Союз підтримав ЗСУ внеском у 3 млн євро ЄС для встановлення кіберлабораторії та кіберкласу.

Підтримка України Сполученими Штатами, зокрема і в галузі кібербезпеки, скоротилася внаслідок політики новообраного президента Дональда Трампа. Новий американський уряд відкидає узгодження поглибленої співпраці у кібербезпековій сфері з попереднім урядом.

«Україна стала «легкою мішенню» для російських хакерів після припинення допомоги США» — такий заголовок має стаття Bloomberg, присвячена кібербезпековій ситуації у країні. У тексті йдеться, що за останні п'ять років лише Агентство США з міжнародного розвитку виділило Україні понад $200 млн на допомогу в галузі кібербезпеки, яка була «критично важливою» для запобігання кібератак і відновлення після їхніх наслідків.

Посилаючись на власні джерела, медіа повідомляє, що США допомогли Україні відбити спроби рф саботувати електростанції та проникнути до Кабміну. Після лютого 2022-го фінансування USAID проєктів кібербезпеки в Україні збільшилося через посилення російських кібератак. За каденції Трампа Департамент ефективності уряду США (DOGE) почав ліквідацію USAID, і це вплинуло зокрема на підтримку кібербезпеки України.

Водночас, підсумовують у статті, Україна отримала і, ймовірно, отримуватиме надалі підтримку від приватного сектору: зокрема, від компаній Mandiant, Palo Alto Networks Inc. та Symantec (належить Broadcom Inc.,), які надали допомогу в кібербезпеці через американську організацію під назвою Cyber Defense Assistance Collaborative (CDAC) у розмірі близько 40 мільйонів доларів. Від них Україна отримувала розвіддані про хакерські загрози, а також інструменти для виявлення кібервторгнень.

■ Кібербезпека і її роль у повоєнній Україні

КІБЕРБЕЗПЕКА І ШТУЧНИЙ ІНТЕЛЕКТ

Мінцифра інтегрує ШІ в процеси та послуги за принципом «Людина-в-циклі», коли перевірка результатів роботи ШІ та ухвалення рішення щодо використання згенерованих даних залишається за людиною, зазначають в міністерстві в коментарі для AIN.

Додають, що штучний інтелект допомагає Міністерству робити цифрову експертизу проєктів нормативно-правових актів: «ШІ аналізує проєкт цих актів на наявність «цифрового компонента» та суперечностей із чинним законодавством у сфері цифровізації, а юрист перевіряє коректність аналізу та готує висновок за результатом цифрової експертизи. Це допомагає уникнути потенційних ризиків «галюцинацій» і багів ШІ-інструментів».

Основним запобіжником витоку даних є використання суверенної інфраструктури: «ШІ-інструменти Мінцифри, які використовують чутливі дані, працюють на локальних моделях. Завдяки цьому дані залишаються у межах міністерства».

Навчання. Спільно з партнерами Мінцифра опублікувала рекомендації з відповідального використання ШІ для публічних службовців. Крім інструментів і кейсів використанні ШІ в держсекторі, у документі є практичні поради, як використовувати AI, дбаючи про безпеку даних та уникаючи інших ризиків AI, як-от «галюцинації», упередження й дискримінація тощо, зазначають в міністерстві.

Також Мінцифра запускає освітні ініціативи з ШІ для держслужбовців. На Дія.Освіта вийшло вже чотири профільні курси:

- **«Штучний інтелект»** — пояснення користі ШІ для держсектору, практичні кейси України та світу;
- **«ChatGPT для підвищення власної ефективності»** — поради президента KSE Тимофія Милованова з використання ШІ в управлінні, для планування, оптимізації робочих процесів і зменшення рутини;
- **«ChatGPT: ваш особистий асистент у роботі, навчанні та житті»** — як правильно формувати запити, складати офіційні документи, формувати звіти та створювати плани заходів;
- **«Штучний інтелект» від BecomingX Ukraine** — освітній серіал від української ініціативи міжнародної платформи, що відкриває глобальні перспективи розвитку ШІ та дає розуміння його етичного і стратегічного значення.

ПІСЛЯ ВІЙНИ

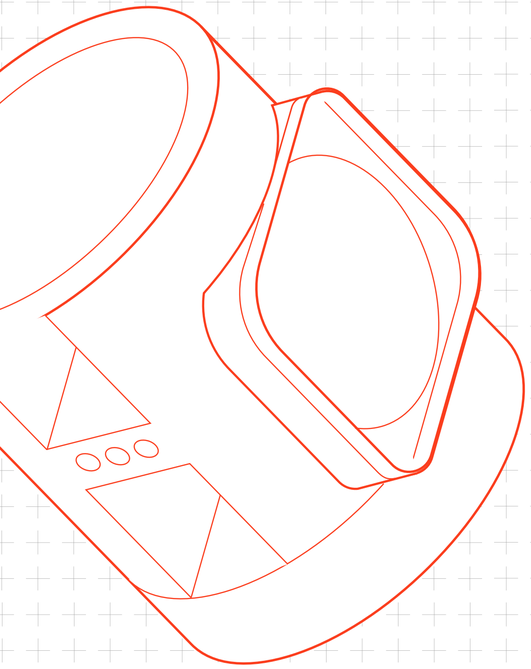
«У 2022-му почалась перша у світі кібервійна, і її темпи будуть тільки наростати з розвитком технологій, — коментують для AIN в Мінцифри. У міністерстві зазначають, що питання кіберзахисту завжди залишатимуть актуальними, змінюватимуться лише акценти та напрямки боротьби залежно від політичної та військової ситуації. — ***Повоєнній Україні також треба бути готовою до нових викликів в різних сферах, а, зважаючи на глобальну цифровізацію життя, у сфері кібербезпеки — насамперед».***

Зміни у кібербезпекововій ситуації можливі у разі кардинальних зміни підходів на національному рівні, вважає Костянтин Корсун. На його думку, шанс на зміни може виникнути лише після зміни правлячого класу та «у разі, якщо до керівництва країною прийдуть люди, які не вважають роль кібербезпеки перебільшеною».

Кібербезпека є і залишатиметься одним із ключових компонентів національної безпеки, зазначає в коментарі для AIN перший заступник голови Держспецзв'язку Ростислав Замлинський: ***«Зі зростанням цифровізації в управлінні, обороні, економіці та сфері публічних послуг потреба у надійному кіберзахисті тільки зростатиме. Необхідно постійно вдосконалювати спроможності з реагування, розвивати кіберзахист критичної інфраструктури, підвищувати обізнаність суспільства та формувати сучасну архітектуру цифрової безпеки».***

РОСІЙСЬКИЙ DEFENSE TECH: ЩО У РОСІЯН Є З ТЕХНОЛОГІЧНИХ РОЗРОБОК, ЯК ВОНИ ЇХ ПРЕДСТАВЛЯЮТЬ У СВІТІ, ІНВЕСТИЦІЇ ТА БЮДЖЕТ, КОМПАНІЙ І РОЗРОБКИ, ЯКІ ЗА 10 РОКІВ ВИНИКЛИ

РОСІЯ: DEFENSE TECH МІНУС ВЕНЧУРНІ ІНВЕСТИЦІЇ ДОРІВНЮЄ «НАРОДНИЙ ВПК»



До початку повномасштабного вторгнення у росії фактично не існувало Defense Tech екосистеми, якщо визначити її як синергійну співпрацю між технологічними стартапами, приватними інвесторами та державними закупівельниками. Причина очевидна — в СРСР не було місця приватній ініціативі, особливо в оборонній сфері, і Росія успадкувала цей промисловий комплекс.

■ Російський Defense Tech:

Утім, це не єдина передумова. Важливо також і те, що радянський ВПК часто перебував у реактивному положенні. У 1984 році майбутній секретар США з оборони Вілльям Перрі так описав роль інновації у американському ВПК: «Оскільки з високою ймовірністю ми й далі будемо мати чисельну перевагу, наші збройні системи мусять і далі демонструвати суттєво кращі результати за радянські».

Натомість у культурі радянських ЗС не існувало прагнення уникнути людських втрат, а це – важливий драйвер для впровадження неапробованих технологій, пише професор Університету Хайфи Дмітрій Адамскі.

Крім того, Радянський Союз хоч й інвестував значні ресурси в інновації, проте відставав від технологічного розвитку Заходу. Доводилося шукати антидот проти північноатлантичних новел або просто досліджувати західний досвід. Так, наприклад, начальник служби радіоелектронної протидії Генштабу ЗС СРСР вивчав застосування РЕБ у локальних війнах Південно-Східної Азії та Близького Сходу, а офіційний журнал Міністерства оборони СРСР наголошував на необхідності застосування засобів РЕБ для протидії західним інноваціям у сфері «діп страйків».

Після розпаду СРСР російський оборонно-промисловий комплекс був значною мірою приватизований. Водночас на той час більшість виробничих підприємств стали залежними від експортних замовлень. Це суттєво ускладнило фінансування науково-дослідних інститутів та конструкторських бюро, які в радянських системі відповідали за R&D.

■ Російський Defense Tech:

РОСІЯ І БЕЗПІЛОТНИКИ: НАЗДОГАНЯЮЧИ

З 2001–2002 року, після приходу до влади Владіміра Путіна, приватизований ВПК був реінтегрований назад у державну власність завдяки широкому інструментарію «злиттів, конфіскація та примусових угод купівлі-продажу». Станом на 2008 рік цей процес не приніс бажаних результатів у сфері інновацій. Під час російського вторгнення в Сакартвело російські ЗС майже не мали власних безпілотників, натомість у 50 разів менша картвельська армія використовувала ізраїльські БпЛА.

Тому не дивно, що вже у 2009 році рф закупила ізраїльські IAI Searcher і згодом почала виробляти ліцензійну копію під назвою «Форпост» на потужностях російського державного ВПК. Вперше «Форпост» збили саме на території України, у 2015 році сили полку «Дніпро-1».

У російському приватному секторі справжній розвиток БпЛА розпочався лише після вторгнення в Сакартвело. Наприклад, «Спєциальний технологічєскій центр» (далі — СТЦ), приватний розробник найвідомішого російського безпілотника «Орлан», станом на 2011 рік все ще спеціалізувався на засобах радіорозвідки. Лише у 2012 році компанія почала зростання завдяки «Орланам». СТЦ ділить російський ринок БпЛА із такими приватними «старожилами»:

■ Російський Defense Tech:

Назва компанії	Рік початку розробок БпЛА	Назва найвідоміших продуктів	Виторг у 2023 році, млрд рублів
СТЦ	~2011	Орлан-10	16,1*
ЦСТ / ZALA	~2004	Zala 421-16EM, Ланцет	~10**
ЭНИКС	~1988	Элерон-3	1,1*
Альбатрос	~2017	Albatros M5	1,1
АФМ-Серверс / Птеро	~2004	Птеро-GO (Картограф)	0,5
Кронштадт	~2009	Дозор-85, Орион	0,5*
Суперкам	~2012	Supercam S350	0,4**

* Не подає бухгалтерську звітність, дані за 2021 рік
** Оцінка на основі фрагментарних даних

Отже, російські БпЛА здебільшого розроблялися приватними компаніями. Натомість ВПК загалом між 2008 та 2023 роком і далі залишався насамперед державним. Не змінили цю ситуацію і вторгнення в Україну 2014 року, участь російської армії та приватних військових компаній у війнах в Сирії, Судані, Лівії та країнах Сахелю. У цих війнах росія переслідувала обмежені цілі, виконання яких не привезло до суттєвих трансформацій промисловості.

■ Російський Defense Tech:

КРИЗА ЯК ПОШТОВХ

Натомість у лютому 2022 році російська федерація спробувала виконати грандіозне завдання – знищити українську державність. Проте для досягнення цієї цілі були виділені обмежені сили та засоби. Унаслідок цього восени 2022 року Силам оборони України вдалося звільнити близько 8000 квадратних кілометрів Харківщини та близько 2000 квадратних кілометрів Херсонщини.

«Російські пропагандисти були найбільш чесними саме тоді — наприкінці 2022 року та на початку 2023 року, коли багато з нових технологій були дефіцитними на фронті, а в Telegram відбувалися дебати щодо неефективності російського війська, закупівель, надходження технологічних засобів у війська», — розповідає в коментарі AIN Самуель Бендетт, радник Центру військово-морського аналізу у Вірджинії.

Після того кремлю вдалося приборкати цю критику, продовжує Бендетт, «проте росіяни і досі скаржаться у своїх каналах у Telegram». Саме ці канали та інші джерела у соціальних мережах становлять основу для вивчення того середовища, яке доволі умовно можна назвати російським Defense Tech.

Проєкт Trap Aggressor аналітичного центру «StateWatch» провів дослідження «FPV-дрони як один з основних інструментів війни росії: ключові виробники, технології, постачання та санкційний тиск». Воно звертає увагу на важливий факт: з 1 січня 2023 року по 1 липня 2024 99% комплектуючих для FPV проімпортувала в росію одна компанія — «Рустакт», зареєстрована 22 лютого 2022 року.

Більшість конкурентів з'явилася на рік пізніше, демонструє портал ГУР «Війна і санкції». Ще у липні 2022 року «Рустакт» брав участь у тендері щодо ремонту системи водопостачання у селищі, де розміщується навчальний центр ВДВ, а вже восени того ж року їхні дрони «ПВХ» почали надходити на фронт. Відтоді російський приватний сектор виробників FPV стрімко зростає.

«НАРОДНИЙ ВПК»: РОЗВИТОК ТА ОСОБЛИВОСТІ

«Протягом усіх попередніх століть військові технології в росії розвивалися державою або за її сприяння і лише близькими до держави компаніями, — говорить Бендетт і додає: Зараз вперше в історії у росії формується приватна індустрія». Росіяни називають це явище «народним ВПК». До того ж, за словами Бендетта, виникла «безпосередня співпраця між розробниками та військовими на лінії фронту — ***такого теж раніше не було».***

У 2022 році «Рустакт» задекларував 82 млн рублів доходу, а у 2023 році — 1,1 млрд рублів. То звідки, власне, ці кошти? Як фінансуються російські приватні компані, які постачають на фронт інноватівну зброю? Як працюють закупівлі таких засобів?

Можна припустити, що для «Рустакту» ключовим фактором є наближеність до російських закупівельників. ***«Інші гравці постійно скаржаться на каналах у Telegram, що їхні вироби кращі за «Рустакт», але держава їх не купує»,*** — каже аналітикиня Trap Aggressor Дар'я Кузьміна.

Проте отримати додаткові дані складно. «Загалом російські закупівлі зброї є закритими», — говорить вона. «Інколи в інтернет просочуються інформація якихось закупівель, проте це фрагментарні дані, які навіть не містять тактико-технічних специфікацій, а отже не дозволяють встановити конкретну модель закупленої зброї», — додає аналітикиня.

Бендетт відзначає існування низки інших джерел доходу приватних гравців, про які відомо публічно.

■ Російський Defense Tech:

Донати на картки.

Росіяни почали долучатися до волонтерської діяльністю майже відразу, коли стало очевидно, що виділених державою ресурсів не достатньо для досягнення її максималістських задач. Наприклад, на початку травня 2022 року, після того, як СОУ деокупували райони Житомирської, Київської, Чернігівської та Сумської областей, російський далекобійник Владімір Шилов запропонував допомогу 76-й десантно-штурмовій дивізії ЗС РФ, яка воює проти України з 2014 року та брала участь у воєнних злочинах в Бучі. Він зібрав кошти зі своїх підписників, на які придбав в Естонії три DJI Mini 2 — згодом естонська служба безпеки його затримала.

А от Катерину та Валентину Корнієнко з тимчасово окупованої Макіївки Донецької області естонська поліція затримати не може. Вони, на відміну від Шилова, з 2015 року займаються збором коштів для фінансування російської війни. У 2024 закупили біля тисячі квадрокоптерів та передали їх різноманітним підрозділам, від незаконних збройних формувань «ДНР» до 56 десантно-штурмового полку ЗС рф.

Жінки звертаються до приватних виробників: «Ми витрачаємо народні гроші лише на те, що дійсно працює». Доказом цього для них є не полігонні випробування, а застосування на фронті.

«Не варто недооцінювати волонтерський рух в Росії, – відзначає Дар'я Кузьміна з Trap Aggressor. — ***Звичайно, в Україні краще сформована культура благодійності, проте і в росії вибудовується довіра до великих фондів».***

Одним із найбільшим є фонд «Все для побєди» громадської організації «Народний фронт», який за 2024 рік зібрав 8.1 млрд рублів. Ця сума співставна з надходженнями найбільших українських фондів. Водночас цей показник треба сприймати критично, оскільки «Народний фронт» – організація, створена безпосередньо кремлем з метою об'єднати низку лояльних партій в один рух. Це означає, що частина надходжень цього фонду може мати бюджетне походження, а не становити реальні пожертви фізичних осіб.

Так чи інакше, «Народний фронт» вів збори спільно з інлфлюенсерами та спрямував залучені кошти на закупівлі технологічних засобів у приватних виробників. Наприклад, пропагандист Юрій Подоляка спільно з «Народним фронтом» збирав на засоби РЕБ, які були розроблені, як він сам казав, «народним ВПК». На зображеннях, використаних для збору, можна ідентифікувати антидронову рушницю «ПАРС» від приватної компанії «Ступор».

■ Російський Defense Tech:

«Меценати»

Заможні росіяни також можуть фінансувати проєкти «народного ВПК» з ідейних переконань чи для того, аби довести свою лояльність до влади. Приклад — Юрій Усков, IT-підприємець. Його компанія «iSpring» найбільш відома за своїм програмним забезпеченням для корпоративного навчання «iSpring Suite». Лише одна юридична особа, через яку він веде бізнес, задекларувала у 2023 році 2,3 млрд рублів доходу. У лютому 2025 року Ускова затримали за підозрою у шахрайстві.

Тоді засновник націоналістичного книжного магазину «Ліства» Дмітрій Бастраков виступив на захист Ускова і заявив, що той спонсорує «народний ВПК».

Допомагати залучати таких спонсорів може і місцева владна еліта. Наприклад, у лютому 2025 року мер Казані Ільсур Мєтшин пообіцяв приватній компанії «Аркодім», що розробляє наземні роботизовані комплекси, знайти меценатів для постачання пілотної партії НРК на фронт.

Бюджети регіональних органів влади та інших установ

У жовтні 2022 року уряд рф також дозволив різноманітним гравцям — від органів місцевого самоврядування до субсидійованих державою підприємств — використовувати кошти платників податків для закупівель безпілотників, засобів зв'язку та інших технологічних виробів оборонного призначення. Водночас ця постанова втратила силу 1 січня 2025 року.

■ Російський Defense Tech:

Організаційні віддзеркалення

Можна припустити, що скасування постанови спричинено реформами у сфері впровадження у війська новітніх технологій. Вони були започатковані міністром оборони рф Андрєєм Бєлоусовим і містять віддзеркалення деяких українських новел. Наприклад, виокремлення безпілотних систем в самостійний рід військ, про яке Бєлоусов оголосив наприкінці 2024 року.

У другій половині 2024 року створено центр «РЕВІР», метою якого є інтеграція технологій з недержавного сектору у державний військово-промисловий комплекс. Дійшло до того, що у вересні 2024 року путін окремо наголосив на необхідності співпрацювати з приватними інноваторами. А у квітні 2025 року, на зустрічі з представниками державного ВПК, наказав «без бюрократичних зволікань» адаптовувати засоби до нових умов поля бою, інтегрувати бойовий досвід у програми військових навчальних закладів та пришвидшити виробництво роботизованих комплексів і безекіпажних катерів.

«Це все кроки до більшої стандартизації нових технологій», — говорить радник Самуель Бендетт і додає, що Україна у цьому питанні «на роки попереду, але росіяни намагаються її наздогнати».

На цьому шляху у них буде багато перешкод. «Зараз у військово-промисловому секторі багато недовіри», — говорить Бендетт.

Як пояснює радник Центру військово-морського аналізу, ситуація виглядає так: «Представники так званого «народного ВПК» дивляться на традиційні підприємства і бачать великі неповоротні структури, які не здатні швидко змінюватися та впроваджувати нові технології. Натомість представники традиційних підприємств дивляться на «народний ВПК» і думають: «Що це взагалі за люди? Хто вони такі? Якийсь мужик на балконі паяє дрон і думає, що може подаватися на ті ж закупівлі, що і ми. Та ці люди взагалі не знають, що вони роблять. Вони ж не тестують свої вироби, не сертифікують їх»».

■ Російський Defense Tech:

Одним із прикладів цього протистояння є скандал навколо дрону «Добриня», який був представлений російським концерном «Алмаз-Антей», який на 100% належить державі та об'єднує в собі низку підприємств, створених за радянської доби для розробки засобів протиповітряної оборони та радіолокації.

У жовтні 2022 року компанія заявила, що розгорнула серійне виробництво квадрокоптерів. У листопаді 2022 року виріб під назвою «Добриня» рекламували різноманітні владні медіа. Наприкінці листопада російські діячі з середовища «народного ВПК», а також критичні до російської влади медіа, почали твердити, що «Добриня» — це копія китайського iFlight Nazgul5. На це провладні інфлюенсери відповіли заявами про те, що нічого погано в копіюванні іноземних виробі немає, мовляв, усі так роблять.

Згодом очільник підрозділу «Алмаз-Антей», відповідального за «Добриню», сам стверджував, що цей дрон — іграшка. Проте чи може взагалі традиційна оборонна промисловість виробляти засоби такого типу?

«Росіяни стверджують, що хоч великі підприємства і виробляють FPV, проте найкращі вироби все одно надходять від приватних гравців», — говорить Бендетт. Він вважає, що це логічно, адже «народний ВПК» перебуває у набагато тіснішому контакті з російськими військами і може швидше адаптовувати технології під ситуацію на фронті.

АНАТОМІЯ ОПТОВОЛОКНА

Водночас російські інноватори не лише повторюють за Україною. На зламі 2024 та 2025 років в українській Defense Tech екосистемі активно обговорювалося питання щодо того, чому росіянам вдалося першим масштабувати застосування дронів на оптоволокні, хоч українські інженери й раніше роздумували над таким використанням ненової технології.

Остаточну відповідь на основі публічних даних отримати неможливо. Водночас аналітикиня Дар'я Кузьміна вважає, що ключову роль у цьому відіграють ресурси.

«Уявімо, у нас є 10 технологій, які мають перспективу, і обмежені ресурси для їх розвитку, – говорить вона. — ***У такому разі рішення про розвиток технологій приймається на основі оцінок щодо того, які напрямки мають найбільший потенціал. У росіян більше ресурсів, тож і вища ймовірність довести технологію до стану, коли її можна ефективно масштабовувати».*** Відповідно, підсумовує експертка, подібні ситуації неуникно виникатимуть в російсько-українському протистоянні, у якому баланс сил є асиметричним.

Бендетт пропонує інше пояснення. Він звертає увагу на голос колишнього генерального директора «Роскомоса» Дмітрія Рогозіна у російських технологічних дебатах. «У нього була така мантра: нам потрібна проривна технологія, ми не можемо просто повторювати шлях України, нам потрібно знайти коротший», — говорить Бендетт. Ймовірно, постійне повторення цієї тези вплинуло на середовище російських інноваторів.

Російський Defense Tech:

Навесні 2024 року перші російські дрони на оптоволокні помітили на фронті. Тоді ж про тестування такого БпЛА прозвітувала українська інженерна школа FPV «Дронарня». 6 серпня 2024 року Сили оборони України змогли досягти швидкого просування у Курській області не в останню чергу через те, що під прикриттям артилерійського вогню розгорнули засоби радіоелектронної боротьби недалеко від безпосередньої лінії фронту. Це унеможливило застосування більшості російських безпілотників.

13 серпня керівник російського виробника дронів «Ушкуйнік» Алєксєй Чадаєв* заявив, що армія РФ на Курщині застосовує розроблені ним БпЛА на оптоволокні проти СОУ, захищених засобами РЕБ.

*Чадаєв — не зовсім стандартний представник середовища оборонних інновацій, оскільки його бекраунд у політичних, а не фізичних, технологіях. Він переконаний російський націоналіст, який у 2009-2010 роках працював у кремлі, а у 2010–2011 роках входив до керівництва партії «Єдіная Росія». Після початку повномасштабного вторгнення став одним із ініціаторів події-нетворкінгу «Дронніца», яка творить російську екосистему безпілотних технологій.

Виступаючи на черговому форумі «Дронніца» у вересні 2024 року Чадаєв наголосив, що тактико-технічні характеристики будь-якого виробу не є достатніми для досягнення переваги над супротивником. Необхідною є здатність швидко не лише збільшити виробництво засобу, а й створити організаційні елементи, необхідні для масштабного застосування засобів. В іншому разі технологічні переваги будуть швидко нівельовані інноваціями супротивника, розгорнутими у відповідь.

■ Російський Defense Tech:

МЕРЕЖУВАННЯ В РОСІЇ

Форум «Дронніца» відбувається у рф третій рік поспіль. Форум ініціював Чадаєв з метою мережування між пілотами БпЛА, волонтерами-постачальниками та виробниками. Організатором форуму виступає «Координационний центр помощі Новороссіі». У 2022 році до події долучилося загалом близько 200 росіян, натомість у 2024 лише виробників було близько 100.

У 2024 році ця подія вже мала загальноросійський масштаб, її висвітлювали найбільші інформаційні ресурси країни. Крім того, у форуму з'явилися спеціалізовані відгалуження: IT-Дронніца, присвячена дискусіям щодо програмного забезпечення військового призначення; IQ-Дронніца, присвячена дискусіям щодо воєнної думки; Медіа-Дронніца, присвячена інформаційному виміру війни.

Найпопулярнішою лекцією Дронніци 2024 року була про українську екосистему Defense Tech, метою якої було знайти спосіб інтегрувати досвід України в російську систему. Один із учасників заходу пригадує, що доповідь «справила на всіх шокуюче враження», особливо на представників влади.

Відбуваються в Росії й більш нішеві події. Наприклад, наприкінці березня 2025 року у Санкт-Петербурзі пройшов форум «Захист цивільних об'єктів від атак безпілотних систем». На полях цієї події представили прототип засобу, який використовуватиме лазер для знищення безпілотників. В Україні подібні дискусії активізувалися також у момент, коли в росії з'явилися БпЛА, здатні завдавати ударів по цивільним об'єктам, тобто з появою Shahed восени 2022 року.

Паралельно з цим у рф тривають традиційні виставки озброєння, зокрема форум «Армія», який відбувається регулярно з 2015 року. Організатори звітують, що кількість відвідувач зросла з 200 тисяч людей у 2015 році до рекордних 1,9 млн у 2022 році. Проте відтоді кількість бажаючих подивитися на російські розробки почала спадати, а про дані за 2024 рік організатори взагалі говорять не охоче.

Виставка 2024 року була присвячена досвіду вторгнення в Україну та «новим формам збройної боротьби», тому не дивно що у павільйонах можна було натрапити на експортну версію «Ланцета», локалізовані в рф коптери, а також і зовсім нестандартні вироби, як от 14-метровий безпілотник літакового типу «Гром», який начебто зможе нести озброєння вагою до 2000 кілограм. А от новинок з інших країн на «Армії-2024» майже не було, оскільки пік активності іноземних виробників спав. Якщо у 2021 році можна було натрапити навіть на французькі компанії, то у 2024 році на «Армії» були представлені лише підприємства з Білорусі, Ірану, КНР та Індії.

РОСІЙСЬКА ДРОНИ НА ЕКСПОРТ

Меншою за кількістю відвідувачів, проте набагато більшою за впливом є International Defence Exhibition. Вона відбувається що два роки в Абу-Дабі. У 2025 році її відвідало понад 200 тисяч людей. Було представлено 41 національний павільйон, зокрема і російський. Серед відвідувачів російського павільйону була і виконавча директорка Технологічних Сил України Катерина Михалко.

«Це дивне відчуття — дивитися в очі людям, які створюють зброю, що щодня обстрілює Київ», — пригадує вона. Павільйон включав в себе вироби таких підприємств:

Назва	Вироби
Роселектроніка	Широкий перелік засобів обробки та передачі інформації, зокрема обладнання для авіації; розробляє засоби РЕБ серії «Серп»; концерн «Вега», складова частина «Роселектроніки», намагалася налагодити виробництво ударних БпЛА «Корсар», проте в останнє цей безпілотник бачили впавшим в Україні у 2022 році.
ZALA	Розвідувальні БпЛА серії ZALA 421; баражуючі боєприпаси «Куб» та «Ланцет»
Ремдізель	Двигуни для суден
Швабе	Оптично-електронні компоненти, зокрема тепловізійні; БпЛА «Блокпост»
Калашніков	Від стрілецької зброї до розробок у сфері НРК (комплекс «Соратнік» застосувався під час боїв за Авдіївку)
Алмаз Антей	Засоби протиповітряної оборони як малої, так і великої дальності; прагне освоїти виробнитцво БпЛА, зокрема розробило «Гарпію 3»
Технодінаміка	Комплектуючі для літаків та вертольотів стратегічної та армійської авіації РФ; ймовірно, у 2024 році «Технодінаміка» поглинула Уральський завод гражданской авіації, який випускає згадані вище БпЛА «Форпост»
Високоточниє комплєкси	Балістична ракета 9М723 Іскандер-М, корегований артилерійський боєприпас ЗОФ39 «Краснополь»

■ Російський Defense Tech:

Окремо також експонувалася продукція «Російських вертольотов». Серед цих компаній частково приватними є лише ZALA і Технодінаміка. ZALA належить державі у вигляді концерну «Калашніков» на 49%. Технодінаміка належить державі у вигляді «Ростех» на 25%.

Разом вироби цих компаній становили «великий, вражаючий стенд, який у чотири рази перевершував за масштабами те, що привезла Україна», говорить Михалко і відзначає, що росія, на відміну від України, «активно нарощує експортні можливості та захоплює ринки збуту».

Дійсно, це не єдина міжнародна виставка, на якій російська зброя рекламувалася як така, що «перевірена боєм». AIN використав дані «Вокс Україна» та ТСУ, аби підрахувати охоплення, якого російське ВПК отримало на міжнародних подіях за час повномасштабного вторгнення

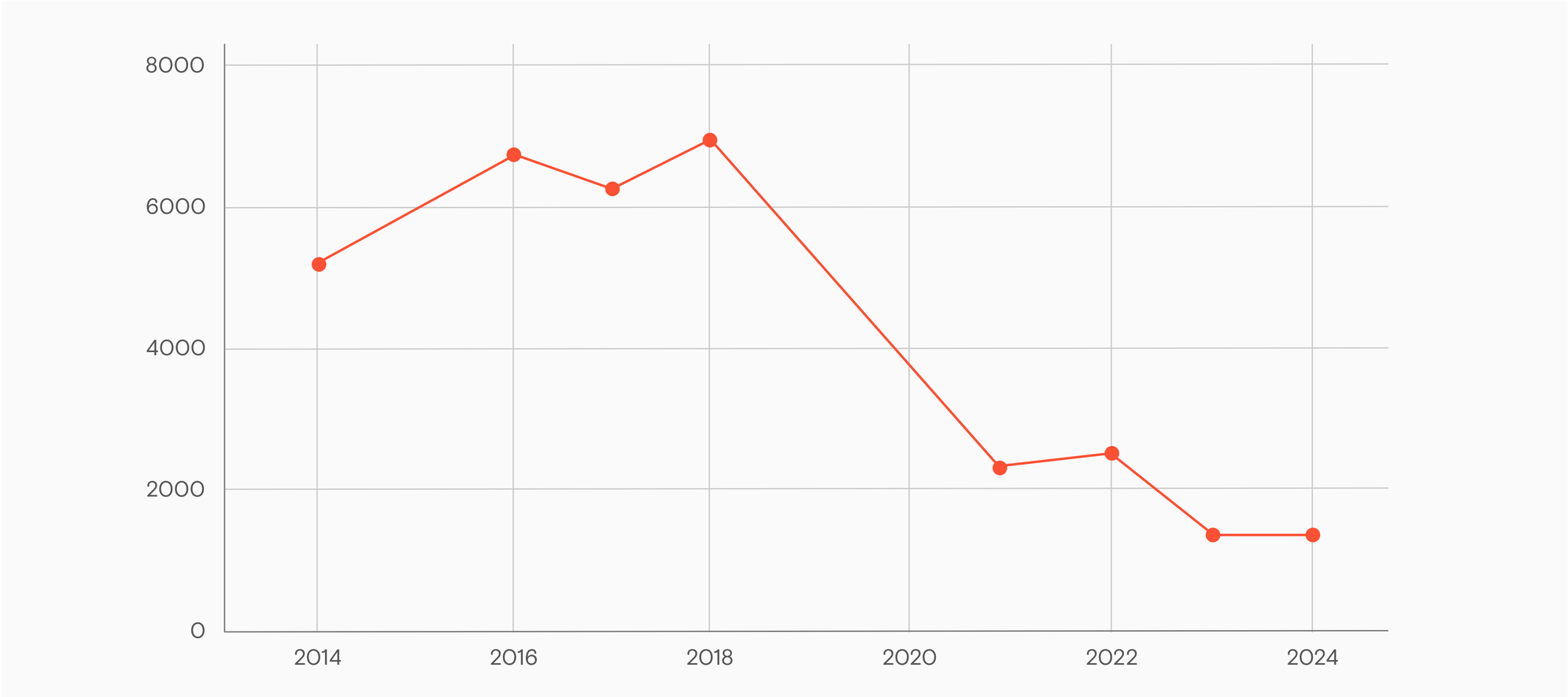
Назва події	Рік	Кількість учасників (учасників та глядачів у випадку авіашоу)
IDEX	2023	132500
Airshow China 2024	2024	590000
World Defense Show 2024	2024	106000
Africa Aerospace and Defense Expo 2024	2024	70000
IDEX	2025	206000
Aero India-2025	2025	700000

■ Російський Defense Tech:

Росія має причини вкладати багато зусиль у ці PR заходи. Як демонструють дані* Стокгольмського інституту дослідження проблем миру, у 2022 році росія продовжувала постачання виробів свого ВПК за контрактами, укладеними до початку повномасштабного вторгнення.

*Дані підраховані у млн SIPRI trend-indicator value (TIV). Ці умовні одиниці обраховують SIPRI на основі даних про собівартість зброї, а не на основні тих цін, за якими реалізується продукція.

Натомість у 2023 році обсяг експорту різко впав, не в останню чергу через політичну невизначеність: укладати договори з рф у 2022 році було непросто навіть для тих країн, які не надто переймалися долею України. Аби хоча б частково відновити свої позиції на глобальному ринку зброї, росії доведеться серйозно вкластися у рекламу.



■ Російський Defense Tech:

Водночас ці дані демонструють також і ефект самостримування. У березні 2022 року російський уряд заборонив експорт безпілотників, а влітку 2023 року дію заборони подовжили до кінця 2025 року. Якась кількість експорту дронів може залишитися непоміченою: їх, на відміну від поставлених нещодавно в Алжир винищувачів Су-35, не помітиш на супутникових знімках.

Наразі російські дрони можна побачити поза росією та Україною хіба що, коли вони літають над безпековою інфраструктурою європейських країн. Водночас присутність ZALA на IDEX 2025 свідчить про плани розпочати експорт відразу після скасування заборони. Це також передбачено у затвердженій влітку 2023 року стратегії уряду рф щодо розвитку БпЛА на період до 2035 року. Згідно з ним, за позитивного сценарію розвитку індустрії росія розгляне можливість «організації експорту БпЛА в дружні країни».

Іншим потенційним способом перетворити російський досвід вторгнення в Україну у валютні надходження може бути створення спільних підприємств. Наприкінці 2020 року російське підприємство «Альбатрос» вело перемовини з бірманською компанією щодо локалізації виробництва безпілотників «Альбатрос-М5» у М'янмі. Цей безпілотник застосовується російським військом проти України, тож директор компанії хвалився бірманцям про «успішність застосування» БпЛА.

Чи вдалося створити виробництво — невідомо. Крім того, у другій половині 2024 року розвідувальні служби європейських країн передали Bloomberg та Reuters інформацію про те, що Китай та росія спільно працюють над БпЛА «Гарпія-3». Після цього Міністерство фінансів США застосувало санкції проти російського розробника проєктної документації завод «Купол», що входить до державного концерну «Алмаз Антей», та китайського підприємства Xiamen Limbach Aircraft Engine, яке виробляє дрони за російськими кресленнями.

■ Російський Defense Tech:

НАРОДНИЙ ВПК ПІСЛЯ

Перевага «народного ВПК» над виробами, які експонуються на таких виставках, у здатності швидко враховувати зміни на полі бою та впроваджувати інновації. Проте що станеться із цими приватними підприємствами, якщо швидкість трансформацій поля бою зменшиться через зменшення активності бойових дій? Приватні підприємці бояться, що у такому разі «їх поглинуть великі компанії, а їхні знання будуть втрачені», — говорить Бендетт. Тому вони зацікавлені у подальшому веденні бойових дій.

Аналітикиня Дар'я Кузьміна зауважує, що дослідження Trap Agressor — це ескіз індустрії на певний момент часу. «Якби ми публікували цей звіт сьогодні, там була би вже більша кількість цих виробників», — говорить вона про російський ринок FPV.

Її колега Соня Максимів щотижня публікує дайджест новин зі середовища російських оборонних інновацій, аби вчасно помічати важливі події. Наприклад, вона звертає увагу на те, що наприкінці березня державний концерн «Калашніков» заявив про створення системи оптичної навігації для польоту БпЛА без супутникового сигналу. Ця технологія давно використовується в українських дронах. Натомість один із найбільш відомих російських приватних розробників БпЛА «Лабораторія будущего» представив посилений вантажний безпілотник «Грузовік М500», який начебто може транспортувати на відстань до 7 кілометрів вантаж до 50 кілограмів. Ці показники є близькими до публічно відомих характеристик українських аграрних дронів.

■ Російський Defense Tech:

Водночас, за даними Стокгольмського міжнародного інституту дослідження проблем миру (SIPRI), у 2024 році Україна витратила на оборону $64,7 млрд, що становить близько 43% від обсягу військових витрат росії за цей самий період.

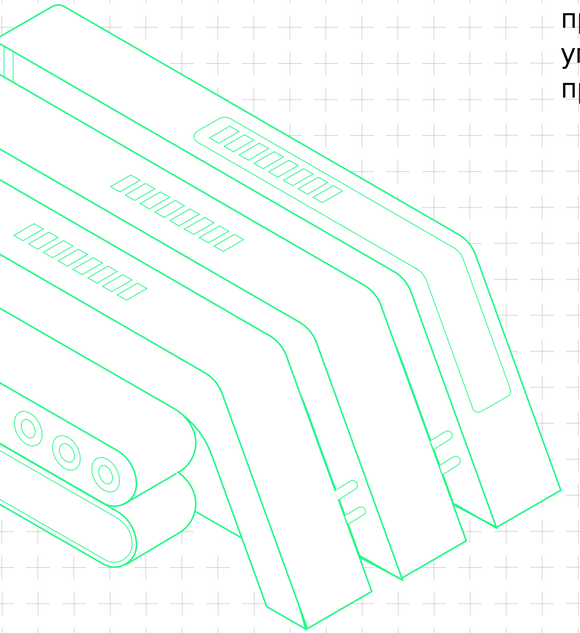
Згідно з даними, військові витрати України зросли на 2,9% порівняно з 2023 роком і склали 34% валового внутрішнього продукту країни — це найвищий показник військового навантаження у світі. Для порівняння, частка військових витрат у ВВП росії становила 7,1%.

SIPRI зазначає, що всі податкові надходження України у 2024 році були повністю спрямовані на фінансування армії. Уся соціально-економічна підтримка держави фінансувалася виняткова коштом міжнародної допомоги. Україна отримала щонайменше $60 млрд зовнішньої військової допомоги, переважно зі США, Німеччини та інших європейських країн. Оскільки SIPRI зараховує військову допомогу до витрат країн-донорів, ці кошти не враховані в загальній сумі українських витрат. Якщо їх додати, фактичні витрати України на оборону у 2024 році склали б близько $125 млрд, що зробило б її четвертою найбільшою військовою державою світу після США, Китаю та рф.

На початку року Україна планувала спрямувати 74% військового бюджету на зарплати військовослужбовців та 23% — на закупівлю та ремонт озброєння. У липні бюджет переглянули, передбачивши додаткові витрати в розмірі майже $13,5 млрд, переважно на підвищення виплат військовим і підтримку родин загиблих і поранених.

Світові військові витрати у 2024 році зросли на 9,4% у реальному вимірі та досягли $2718 млрд, що стало найвищим показником за всю історію спостережень SIPRI. Це також десятий рік поспіль, коли зафіксовано зростання витрат на оборону. Водночас витрати росії зросли на 38% і досягли $149 млрд. Проте реальні витрати можуть бути ще вищими через високий рівень засекреченості бюджету: близько 30% російських оборонних витрат у 2024 році були позначені як «секретні». Значна частина коштів пішла на виробництво озброєнь для війни проти України та на соціальні виплати військовослужбовцям.

ЛАБОРАТОРІЇ В УНІВЕРСИТЕТАХ: УМОВИ РОБОТИ, РОЗРОБКИ ТА ПРОФІЛЬНА ОСВІТА



У часи війни стрімких змін зазнає не лише оборонна галузь, але й освіта, зокрема технічна. У відповідь на ці виклики в Україні розгортається мережа навчальних програм — від університетських курсів і професійно-технічної освіти до спеціалізованих тренінгів для військових і цивільних. Такі програми об'єднують знання з аеродинаміки, електроніки, програмування, тактики та практичного управління дронами. Водночас деякі подібні програми існували ще з 2014 року.

У цьому розділі аналізуємо, як профільна освіта в Україні взяла у фокус професії, дотичні до війни. Ми не розглядаємо курси, які за бажанням може пройти будь-хто охочий, а зосереджуємо увагу на середню та вищу освіту.

ОНОВЛЕНИЙ КУРС ЗАХИСТ УКРАЇНИ ДЛЯ ВСІХ УЧНІВ 10-11 КЛАСІВ

3 вересня навчального 2024 року в українських школах викладають оновлену програму «Захисту України» для 10-11 класів, яка складається з шести модулів:

- військові технології*;
- домедична підготовка в умовах бою з елементами тактичної медицини;
- озброєння та військова техніка, стрілецька підготовка;
- орієнтування на місцевості та інженерна фортифікація;
- комунікація та взаємодія в бою;
- форми та методи ведення інформаційної війни (пропаганда, дезінформація, кібератаки, психологічні операції, інформаційні операції);
- цивільна безпека населення (навички поводження в екстрених ситуаціях, формування плану виживання тощо).

*На цьому модулі розглядають такі теми:

- Основи радіозв'язку. Види, типи та способи налагодження зв'язку
- Подвійне застосування та безпека зв'язку: телефон, Wi-Fi, Starlink
- Основи радіоелектронної боротьби: військові системи РЕР, РЕБ. Призначення та типи засобів
- Безпілотні (роботизовані) системи.
- БпЛА: види та призначення. Сфери застосування БпЛА.
- Основні складові конструкції та технічні параметри БпЛА.
- Основні властивості та моделі БпЛА (мультиротори, FPV, крила)
- Основи пілотування. Базові вправи на FPV-дронах та БпЛА літакового типу.
- Правила польоту, заборонені зони та рекомендації щодо безпеки
- Симулятори та тренажери для підготовки операторів БпЛА
- Військові інформаційні системи та платформи.
- Військові професії. Особливості професій, пов'язаних з аналізом інформації; радіотехнічних засобів електромагнітної (радіоелектронної) боротьби, пілотуванням та розробкою БпЛА.

Учні 11 класу вчаться літати на симуляторах, а потім переходять до пілотування FPV Tiny Whoop. В осередках облаштовані функційні зони для пілотування, а все обладнання закуплено за кошти субвенції, відповідно до Типового переліку обладнання.

У професійно-технічних навчальних закладах також введуть спеціальність «оператор цивільного дрона».

Оновлений предмет «Захист України» здійснюється не у класах, а у спеціально облаштованих осередках. Такі осередки створюються на базі закладів загальної середньої освіти або професійно-технічних закладах.

«Це означає, що в одному осередку можуть навчатись діти з різних закладів, що проживають у громаді. Таких осередків станом на квітень маємо 963», — розповідають у Міністерстві освіти і науки.

Викладачами оновленого курсу є вчителі предмету, серед яких ветерани, військові фахівці, які пройшли навчання на базі Інститутів післядипломної педагогічної освіти — серед таких близько 3000 вчителів. До розробки курсу залучили Victory Drones, Військову школу «Боривітер», 12-ту бригаду спеціального призначення НГУ «Азов», БФ «Солом'янські котики», який фокусується на тактичній медицині, Госпітальєри тощо.

«Для підвищення кваліфікації вчителів МОН спільно з Демократичною школою «Майбутні», 12-ою бригадою спеціального призначення НГУ «Азов» та Мольфаром провели дві хвилі навчання тренерів-педагогів з окремих модулів програми, серед 120 людей — 95 отримали сертифікати й викладають в інститутах післядипломної освіти.

А до викладання предмета «Захисту України» залучаємо людей, які мають вищу освіту та/або відповідну професійну кваліфікацію, насамперед звільнені з військової служби, ветерани війни або ветерани військової служби», — коментують у МОН.

Як зазначають в Міносвіти, проєкт є експериментальним, а його охоплення сягнуло понад 360 тисяч учнів. З 2027 року викладання за оновленою програмою в осередках стане обов'язковим.

«Наразі МОН працює над підготовкою навчання супервізорів, оновленням переліку обладання та розробкою типових програм підвищення кваліфікації вчителів для поглибленого вивчення за модулями «Основи стрілецької підготовки та тактики» й «Пілотування FPV-дронів»», — кажуть у міністерстві.

Також Victory Drons спільно з МОН розробили безплатний курс «Безпекові технології». Він має теоретичну частину у форматі онлайн-лекцій та практичну, яка передбачає тренування на полігоні.

ФАХОВІ КОЛЕДЖІ

Деякі фахові коледжі окремо розробили програми, на яких можна навчатися після 9 класу. Серед таких Галицький фаховий коледж імені Чорновола, Меденицький аграрно-технологічний професійний коледж, Львівське вище професійне училище комп'ютерних технологій та будівництва, Київський та Тернопільський професійні коледжі з посиленою військовою та фізичною підготовкою.

Навчання у Тернопільському коледжі, наприклад, триватиме від півтора місяця до трьох років, а сам заклад освіти отримає 30 державних місць для програми «Оператор наземних засобів керування безпілотним літальним апаратом (дроном)».

«Це буде цивільна професія. Ми готуватимемо спеціалістів на базі 9 класів. А також будемо проводити курси підвищення кваліфікації», — зазначають у коледжі.

Подібну програму — курс «Управління БПЛА» — запровадили влітку 2023 року у приватному навчальному закладі «Фаховий коледж Вінницька IT-Академія». Тут програма розрахована не лише на цивільних, але й військових, триває 32 години і включає теоретичні основи конструювання, програмування, аеродинаміки та навички складання, ремонту і управління сучасними БПЛА. Безоплатно навчають також студентів інших навчальних закладів будь-якого рівня і форми власності. Протягом навчання кожен студент складає FPV-дрона, якого заклад передає українським захисникам.

Крім того, вже з грудня цього року стартує пілотний проєкт підготовки вчителів, викладачів навчальних закладів Вінницької області.

«Влітку 2024 року пройшли сертифікацію від Національного агентства кваліфікацій і затвердили процедуру здачі іспиту, який включає теоретичну частину з цифровими тестами і практичну (польоти на симуляторі і в польових умовах з виконанням обов'язкових вправ, складання FPV-дрона і його налаштування, тестування для виконання бойових задач). З лютого 2025 року, після проходження сертифікації від Міноборони, проводимо навчання вже на всіх типах БПЛА, як мультироторного, так і літакового типу», — розповідає Роман Мельник, засновник та директор Vinnytsia IT-Academy.

Усі виготовлені студентами дрони академія передає військовим — таких нараховується вже 10 тисяч FPV.

■ Лабораторії в університетах

ВИЩА ОСВІТА

«Отримайте практичний досвід у розробці БпЛА та втілюйте інноваційні рішення разом з лідерами оборонної галузі». Таку рекламу від Київської школи економіку можна побачити у соцмережах — заклад освіти закликає вступників розглянути навчання на одній з їх магістерських програм, які тепер відповідають вимогам воєнного часу. Деякі заклади вищої освіти України — як КПІ або НАУ — подібні програми мали до повномасштабного вторгнення та активного розвитку Defense Tech галузь.

У цьому розділі аналізуємо освіту (середні та вищі навчальні заклади; до аналізу не потрапили школи та короткострокові курси) та зміни, які вона впроваджує через війну.

Київська школа економіки

Програми: Мікро-нано електроніка, БпЛА

Запуск: 2024 рік

Перший випуск магістрів: взимку 2025 року

Кількість студентів:

На програму БПЛА вступило всього 96 людей (79 студентів + 17 слухачів), з них станом на сьогодні навчається 56 студентів; на мікро-та наноелектроніку — всього 44 людини (26 студентів + 18 слухачів), з них станом на сьогодні навчається 21 студент.

«Для нас це був перший досвій і серйозний поворот — від економіки до інженерних програм. Мікро та наноелектроніка у партнерстві з ETH Zurich, а програма з дронів більш локалізована та кастомна.

Чому вирішили запустити? Бо зараз тема безпеки та інновацій сама важлива. Хтось має робити чіпи та дрони. Також після війни тема технологій подвійного призначення буде ключовою для нашої економіки. Дрони, які скидали вибухівку та збирали розвідувальну інформацію. Будуть скидати добрива та робити доставку. Інженерна школа це стратегічний напрямок, без якого не може існувати жоден університет, який хоче бути актуальним та мати вплив», — розповідає Тимофій Брік, ректор КШЕ.

Це повноцінні магістерські програми: за результатами півторарічного навчання студенти пишуть дипломну роботу, яка є проєктно орієнтованою, захищають її і отримують магістерський диплом. Серед дисциплін, які вивчають, — аеродинаміка, автоматичне керування, системи навігації, безпілотні системи. Практичні заняття проводять з використанням сучасних симуляторів та реальних безпілотних літальних апаратів.

Як зазначають в КШЕ, студенти можуть проходити стажування і продовжувати кар'єрне зростання в українських та міжнародних компаніях і корпораціях.

«Ми співпрацюємо з різними компаніями, адже БПЛА — це не тільки про воєнні технології або про війну. Ми беремо участь і у проєктах щодо гуманітарного розмінування, і щодо використання дронів для аграрних потреб, і щодо застосування ГІС-технологій для забезпечення ортофотопланами місцевості», — коментують в КШЕ.

КПІ ім. Ігоря Сікорського

Програми:

Інженерія авіаційних та ракетно-космічних систем, Інженерія безпілотних та автономних систем, Системи управління літальними апаратами та комплексами; Факультет приладобудування та Інститут оборонних технологій.

У 2025 році Defense Tech компанія SkyFall, що спеціалізується на безпілотниках, відкрила лабораторію сигналів та процесів у радіотехніці на базі Радіотехнічного факультету КПІ.

Кількість студентів:

Лабораторія розрахована на 24 студенти одночасно. Упродовж року тут навчатимуть 180 майбутніх інженерів.

«Радіотехнічний факультет Київського політехнічного інституту імені Сікорського — один із перших створених і досі один із провідних факультетів в Україні за радіотехнічним напрямом, із сильною програмою та вузькогалузевими спеціальностями. Один із небагатьох факультетів, де навчають таких спеціалістів — RF-інженерів широкого профілю, які працюють із широким спектром напрямів, зокрема РЕБ і РЕР, які сьогодні критично важливо вдосконалювати на фронті», — зазначають SkyFall.

Студенти вивчають методи проєктування та експлуатації систем керування літаками, ракетами, супутниками, безпілотними літальними апаратами. У програмі навчання факультету 70% становлять практичні заняття, тому відкриття лабораторії — необхідний крок до покращення навчання. Опановують також теоретичні та практичні навички роботи із сигналами та процесами в радіотехніці: студенти мають можливість опановувати роботу з аналізаторами спектру частот, генераторами сигналів та осцилографами.

«Одна з цінностей компанії SkyFall — допомога фронту через розвиток технологічної сингулярності. Інновації без навчання неможливі. Саме тому ми готові вкладати в навчання та покращення освітнього процесу майбутніх спеціалістів різними способами. У планах — багато проєктів, якими обов’язково поділимось згодом», — кажуть у SkyFall.

Програми доступні як для рівня бакалавр, так і магістр.

КПІ ім. Ігоря Сікорського

На базі університету з 2012 року діє також Sikorsky Challenge Ukraine — інноваційна екосистема, яка об'єднує стартапи, науковців, інженерів, бізнес та інвесторів для розробки технологічних рішень.

У фокусі інновації в різних сферах, зокрема в Defense Tech: дрони, кібербезпека, розвідка, штучний інтелект, роботизовані та сенсорні системи, засоби захисту. Сереж прикладів проєкту: бойовий дрон-камікадзе, що отримав інвестування від Міноборони, та система навігації без GPS.

Sikorsky Challenge має кілька напрямів:

- Інкубатор стартапів;
- Фонд Sikorsky Challenge Venture Fund;
- Щорічний конкурс стартапів;
- Освітні програми.

- Лабораторії в університетах

Національний університет біоресурсів і природокористування

НУБіП запустив науково-дослідний кластер БПЛА та спеціальний курс для навчання викладачів і студентів, аби навчати застосовувати безпілотними у сфері природокористування.

Національний університет водного господарства та природокористування

Започаткували курс «Оператор БПЛА». До програми підготовки входять:

- тренувальні польоти на симуляторах і тренажерах;
- основи виготовлення та ремонту БПЛА типу квадрокоптер та типу крило;
- практичне пілотування й операторська діяльність на БПЛА типу квадракоптер та типу крило ;

Хмельницький університет економіки та підприємництва

Університет економіки і підприємництва спільно з Хмельницьким фаховим економіко-технологічним коледжем створили курс з підготовки операторів безпілотних літальних апаратів (БПЛА). Програма розрахована не лише на студентів, але й школярів.

Програма включає:

1. Управління сучасними БПЛА

- Знайомство з різними типами дронів: квадрокоптерами, гексакоптерами та іншими типами безпілотників.
- Навчання основам управління, маневрування та автоматичних режимів польоту.
- Робота з додатковим обладнанням: камерами, сенсорами, системами тепловізійного спостереження.
- Відпрацювання сценаріїв польотів для різних задач – зйомка, картографія, моніторинг.

2. Теоретичні основи аеродинаміки та конструювання БПЛА

- Основи аеродинаміки та принципи польоту безпілотних літальних апаратів.
- Вивчення конструкцій різних типів дронів, особливості їхньої будови та функціональність компонентів.
- Ознайомлення з електронікою та навігаційними системами, що забезпечують стабільність і керованість польоту.
- Основи безпеки польотів, дотримання вимог повітряного простору та законодавчих норм.

Хмельницький університет економіки та підприємництва

3. Складання, ремонт та обслуговування БПЛА

- Практичні навички складання дронів з базових комплектуючих – двигуни, пропелери, корпуси та системи живлення.
- Техніка ремонту та обслуговування БПЛА, діагностика несправностей та усунення неполадок.
- Навчання правил технічного обслуговування, що дозволить забезпечити довгий термін експлуатації обладнання.

4. Програмування політних контролерів та налаштування

- Робота з польотними контролерами, налаштування дронів під різні задачі та умови експлуатації.
- Програмування автоматичних польотних маршрутів та налаштування функцій повернення, навігації та збереження енергії.
- Використання спеціалізованого програмного забезпечення для управління дронами і отримання точних даних.

Державний університет інформаційно-комунікаційних технологій

Заснували гурток на кафедрі МВТ. Під час заняття студенти вивчають:

- техніка безпеки;
- класифікація БПЛА;
- конфігурація БПЛА, складові компоненти;
- методи проектування та розрахунку вартості таких систем;
- особливості застосування рам, двигунів, пропелерів, регуляторів швидкості, різних датчиків, модулів та сенсорів;
- основи тестування БПЛА-систем;
- живлення та надійність пристроїв;
- технології та протоколи передачі даних;
- налаштування прошивки БПЛА.

- Лабораторії в університетах

Львівська політехніка

Culver Aviation та Національний університет «Львівська Політехніка» підписали Меморандум про співпрацю. Спеціалісти компанії долучаться до підготовки студентів в рамках нової освітньої програми «Безпілотні літальні апарати». Новий напрям навчання — «Безпілотні літальні апарати» — стартує в Інституті механічної інженерії та транспорту на кафедрі нафтогазової інженерії та зварювання.

Серед напрямів програми:

- Проєктування та виробництво БПЛА;
- Обслуговування та експлуатація БПЛА;
- Технології зварювання при виробництві БПЛА.

Створили також інкубатор Tech Startup School, в рамках якого студенти працюють над системами зв’язку, мобільними застосунками для військових та БПЛА.

Хмельницький національний університет

Діє вибіркова дисципліна «Технології та експлуатація дронів», завданням якої є навчити використовувати безпілотники для застосування їх у сільському господарстві, будівництві та охороні природи.

Студенти вивчають історію та кваліфікацію FPV, принцип роботи та конструкцію, особливості зв’язку, програмне забезпечення та правила експлуатації.

Національний аерокосмічний університет ім. Жуковського «Харківський авіаційний інститут»

Програми:

Системи автономної навігації та адаптивного керування літальними апаратами, Оператор наземних засобів керування безпілотними літальними апаратами.
На кафедрі студенти вивчають принципи автоматичного керування літаками, вертольотами та безпілотними апаратами. Також здобувають навички математичного та комп'ютерного моделювання руху літальних апаратів.

Серед інших дисциплін:

- Основи аеродинаміки мультикоптера.
- Основи управління і динаміки польоту.
- Основи конструкції мультикоптера.
- Електро та радіообладнання.
- Основи експлуатації мультикоптера.
- Техніка безпеки при експлуатації мультикоптера.
- Закони, які регламентують польоти БПЛА.
- Основи метеорології.
- Особливі випадки польоту.
- Основи пілотування на тренажері.
- Вправи на літаючої техніці.

Харківський національний університет радіоелектроніки

Університет орієнтований на радіоелектронну боротьбу, захист інформації, робототехніку. Працюють зі студентами над розробками ППО-модулів, камер-розвідників та програмних засобів.

Дніпровський національний університет ім. Олеся Гончара

Студенти працюють над стартапами з автономної техніки, мобільних інженерних рішень (як укриття, зарядні станції тощо) та військового IoT.

У Дніпровському національному університеті навчають проєктувати та збирати безпілотники. В університеті обладнали аудиторію, де виготовляють корпуси та електроніку для БпЛА, а також лабораторію з виробництва безпілотників.

Національний університет «Запорізька політехніка»

Програма:

Безпілотні літальні апарати

Предметом вивчення є загальні відомості про створення різноманітних безпілотних літальних апаратів, динаміку польотів, основи аеродинаміки і конструкція безпілотних літальних апаратів, принципи керування та розробки систем керування.

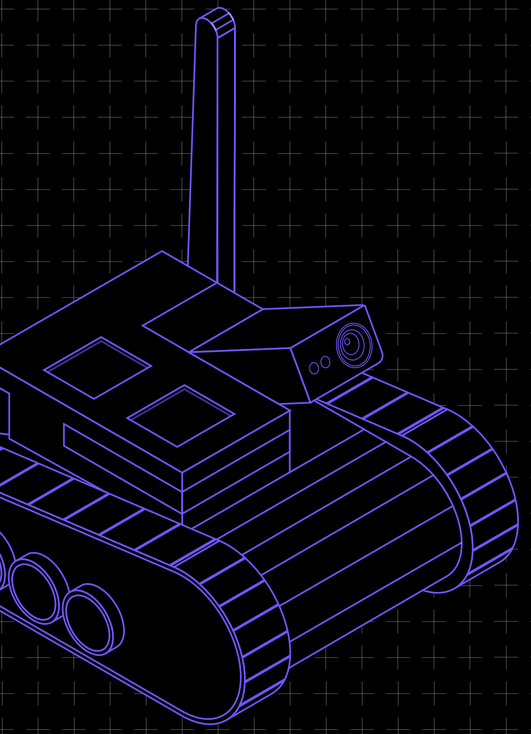
Одеський політехнічний університет

Запровадили AeroDrone Hub для навчання операторів БПЛА, створення власних дронів та технічної підтримки для фронту. Співпрацюють із ЗСУ та волонтерами.

Український католицький університет

Запустили Центр ШІ та оборони, який працює над аналізом супутникових зображень, розпізнаванням об’єктів на полі бою та прогнозуванням загроз. Співпрацюють з Brave1.

РИНОК ПРАЦІ В УКРАЇНСЬКОМУ DEFENSE TECH: ПОРТРЕТ ПРАЦІВНИКА, НАЙМ ВЕТЕРАНІВ, ЗАРПЛАТИ



Навряд в українській економіці існує галузь, яка зростає швидше за Defense Tech. На початку цього року співзасновник одного з українських оборонних стартапів сказав у коментарі AIN, що цей сектор — new black для української економіки загалом. Згідно з нещодавно опублікованими розрахунками Державними служби статистики України, у січні 2025 року виробники літальних апаратів реалізували своєї продукції на 3,9 млрд гривень. Це майже вдвічі більше ніж за аналогічний період 2024 року, навіть якщо скорегувати цей обсяг на курс гривні до долара.

Водночас існує безліч факторів, що обмежують цей ріст: від невисокої прогнозованості контрактування до обмеженості експорту. Чимало із цих факторів мають політично-організаційне походження, тобто характерні суто Defense Tech сфері, а не українській економіці загалом.

Проте тиснуть на галузь і фундаментальні фактори. Насамперед йдеться про дефіцит людського капіталу, що спричинений російськими вбивствами, тимчасовою окупацією території України, еміграцією та мобілізацією працездатних людей.

Цей фактор — не новина для української економіки. З червня 2022 року стабільно зростає частка підприємців, які в опитуваннях Інституту економічних досліджень називали брак робочої сили основною перешкодою для ведення бізнесу. З листопада 2024 року ця проблема займає перше місце у результатах опитувань.

Ринок продовжує адаптуватися до цих умов. Згідно з опитуваннями Info Sapiens, у березні 2025 року частка зайнятих людей досягла найвищого рівня за весь час повномасштабного вторгнення. Це відбулося не лише завдяки зменшенню частки безробітних, а і завдяки зменшенню частки економічно неактивних. Таких людей в Україні близько 12 мільйонів — це учні, студенти, пенсіонери та люди, які не шукають роботу з інших причин.

Іншими словами, це результат зусиль підприємств із «залучення до ринку праці тих осіб, які раніше були менш представленими на ньому: студентів, пенсіонерів, осіб з інвалідністю, ветеранів», відзначає Національний банк України. У квітні 2025 року частка вакансій на платформі work.ua, що не передбачали досвіду, була на 5 процентних пунктів більшою ніж у квітні 2024 року.

Такі політики впроваджують також і ті компанії, що розробляють інноваційні оборонні продукти. Такий інтерес є взаємним: близько 15% кандидатів на профільній кар'єрній події «Арсеналі Талантів» мали до 1 року досвіду, розповіла AIN рекрутингова агенція Lobby X.

«Це важливо — розвивати, формувати і орієнтувати молодь, яка навчається зараз», — сказав CEO виробника інфрачервоних камер Oko Camera Денис Ніколаєнко під час форуму Brave1 Defense Tech Era. Водночас є очевидним, що найбільш високотехнологічні вироби не можуть розроблятися суто молодими людьми без досвіду. Тому виробничі компанії як Oko Camera залучають також і людей з таким стажем, який дозволяє їм виходити на пенсію. Наприклад, найстаршому працівнику виробника інфрачервоних камер понад 75 років.

У результаті Defense Tech об’єднує відразу дві категорії людей, які зазвичай є економічно неактивними: студентів та пенсіонерів. Таке поєднання створює ще один виклик для компаній: як організувати співпрацю настільки відмінних людей?

«Мусимо будувати такі культури, де молодь спільно та ефективно співпрацює з досвідченими розробниками», — зауважив Ніколаєнко. Потрібно це не лише для ефективного виконання короткострокових завдань, але і для передачі знань від старшого покоління до молодшого.

Команда Ніколаєнка так само як і низка інших лише розпочинає роботу над такими культурами. AIN поспілкувався із ними, аби зберегти та розповсюдити їхній досвід.

СТУДЕНТИ ТА/АБО МОЛОДІ СПЕЦІАЛІСТИ?

Станіслав (ім’я змінено з міркувань безпеки) приєднався до розробника систем звукової розвідки Vidar Systems ще до того, як вступив в університет. А от Григорій (ім’я змінено з міркувань безпеки) навпаки почав працювати у виробника систем зв’язку HIMERA вже студентом. Спеціалізація його вищої освіти має безпосередній стосунок до задач, із якими він стикається.

«Хотілося не просто працювати, а розвиватися саме в тій сфері, яку вивчаю», — пояснює Григорій. Таке ж прагнення було і в Марка, наймолодшого працівника виробника наземних роботизованих комплексів Roboneers: «Лише теоретичних знань із університету недостатньо», особливо коли йдеться про настільки швидку галузь, як Defense Tech.

Натомість Світлана (ім’я змінено з міркувань безпеки), яка зараз завершує бакалаврат у провідному українському технологічному університеті, мотивувала необхідність інвестувати в кар’єру, а не лише у знання. Так вона потрапила у Oko Camera. ***«Мотивує мене розуміння того, що я приношу користь, а також бажання розвиватися та отримувати новий досвід»,*** — додала вона.

Світлана, до всього, навчається на стипендіальній програмі і визнає, що поєднувати все буває складно. Компанії можуть уникати найму студентів через побоювання того, що молоді люди можуть гірше виконувати свої обов’язки під час збільшення навантаження в університеті.

Найкращим антидотом проти цього страху є власний досвід лідерів та менеджерів компаній. Наприклад, CEO Vidar Systems Денис Собчишак також працював у одній з найбільших українських IT компаній. ***«Я завжди був наймолодшим співробітником, і новий погляд на речі був затребуваним»,*** — пригадує він. Схожий досвід мав і Ніколаєнко з Oko Camera: ***«Я сам почав працювати за фахом з третього курсу університету». Це ж стосується і HRD виробника засобів радіозв’язку HIMERA Руслани Пірог. «Знаю точно: поєднувати навчання з роботою можливо, і це дає потужний поштовх до зростання»,*** — пояснює вона.

Крім того, компанії можуть адаптовувати рівень залученості своїх молодший працівників, залежно від рівня тиску навчання. ***«У нашій компанії з розумінням ставляться до навчального процесу — під час сесії я маю змогу сфокусуватися на навчанні й закрити всі хвости»***, — говорить Марк з Roboneers.

Проте це не єдиний страх працедавців. Протягом останніх років в український інформаційний простір регулярно потрапляли інфоприводи про покоління Z, що засновані на дослідження чи спостереження, характерних північноамериканському контексту. Наприклад, 45% менеджерів з найму в США, опитаних агенцією «Resume Genius», назвали Gen Z найскладнішими у співпраці.

Крім того, у американських медіа ширилася паніка про те, що покоління Z часто вдається до «тихого звільнення» чи «звільнення-помсти». ***«Це сильно перебільшена історія стосовно покоління Z»,*** — вважає Ніколенко з Oko Camera. Він стикався з «тихим звільненням», проте це не стосувалося молодих людей. У Roboneers таких випадків «зникнення» молодих людей не було. HR розробник систем звукової розвідки Vidar Systems погоджується із оцінкою CEO Око Камера і додає: відсіювати людей з недостатньо відповідальним ставленням до роботи треба на етапі найму, і це стосується не лише студентів.

Це не означає, що усім молодим людям завжди вдається отримувати бажані посади чи успішно поєднувати роботу з навчанням. Проте такі ситуації навпаки можуть слугувати поштовхом до розвитку чи переосмислення.

Світлана працює в парі з Андрієм (ім'я змінено з міркувань безпеки). Він старший за неї, має досвід у галузі розробки електроніки. Попри різницю у досвіді, йому нескладно працювати в парі. Андрій взагалі пропонує перевизначити слово «молодь» таким чином: молодою є та людина, яка знає менше, ніж не знає, але працює для більшого знання. Себе він відносить саме до цієї категорії.

«З колегами, яким подобається те, чим вони займаються на роботі, і які мають мотивацію рости професійно, особисто мені працювати легко і комфортно незалежно від їхнього віку», — підсумовує він.

Світлана також не бачить проблем у співпраці. ***«Усі колеги прогресивні та відкриті, з ними цікаво спілкуватись»,*** — говорить жінка. Вона відчуває нестачу досвіду, проте це лише підштовхує до навчання. Чи відчуває Григорій те, що є наймолодшим працівником HIMERA? Відповідає жартома, мовляв, не завжди розуміє деяких приколів та не жаліється на здоров'я.

ПОДІЛИТИСЯ ДОСВІДОМ: НАЙСТАРШІ ПРАЦІВНИКИ DEFENSE TECH

У XX сторіччі в Україні функціонувала низка підприємств оптичної сфери. Їхня дослідницька та виробнича діяльність суттєво зменшилася після занепаду радянської планової економіки. Багатьох провідних розробників цих підприємств уже немає в живих, чимало досвіду втрачено. Roboneers розуміє це і свідомо шукає «фахівців, які є носіями знань і досвіду, особливо у сферах, які довгий час залишались поза увагою держави», навіть якщо вони «давно не на ринку».

Проблема відсутності передачі досвіду була очевидна й найстаршому працівнику Oko Camera Василю (ім'я змінено з міркувань безпеки), якому понад 75 років. ***«Я завжди шукав людей, кому можна було б передати і які б захотіли перейняти мої знання та майже півстолітній досвід у галузі оптичного та оптико-механічного приладобудування», — говорить він. «Така нагода випала — компанія самостійно розшукала його. У нього унікальна експертиза, таких спеціалістів в нашій країні одиниці»,*** — розповідає про нього CEO компанії.

Проте особливість таких кадрів не лише у їхньому досвіді. Вони також приносять із собою «зважений підхід до роботи та побудови процесів, чудове почуття гумору й здатність бути менторами», — ділиться HR спеціаліст Roboneers Саша. Водночас можуть повільніше адаптовуватися до швидкості зміни в галузі.

Василь з Oko Camera звик до «рваного» темпу роботи у індустрії, яка швидко розвивається. Він має чітку місію — хоче, аби колеги «набралися досвіду та знань і рухалися далі на основі нових технологій». Ця мотивація — не єдина причина, чому він продовжує працювати. ***«Я не можу існувати без роботи,*** — говорить він і жартує. — ***Мене винесуть з роботи».*** Він закликає експертів зі свого покоління також приєднуватися до молодих українських команд, підтримувати навіть, на перший погляд, найбільш фантастичні ідеї, аби сприяти «технічному і технологічному прогресу».

Люди старшого віку часто самостійно подаються на вакансії Oko Camera, проте це не завжди призводить до таких історій успіху. Причина насамперед у «рваному» темпі, про який згадував Василь. ***«Із багатьма кандидатами проводили співбесіди, але в більшості випадків ми не були готові до співпраці через занепокоєння, що людина не віллється в робочий процес»,*** — пояснює Ніколаєнко. У багатьох командах компанії застосовуються agile методології, аби не відставати від трансформації поля бою та галузі.

Олександру (ім'я змінено з міркувань безпеки) майже 70, він працює і в HIMERA і визнає — «темп справді високий». Проте для нього втома відходить на другий план, коли він відчуває вплив своєї роботи на збереження життів на фронті.

Із ним погоджується Святослав (ім'я змінено з міркувань безпеки), якому понад 60 років. Він працює на виробництві Roboneers, одного із найбільших розробників наземних роботизованих комплексів. Або, як каже знайомим, «робить возики». ***«Головна причина, чому я тут — це бажання бути корисним і допомагати хлопцям і дівчатам на фронті»,*** — пояснює він.

Команда також може бути джерелом мотивації для досвідчених працівників. У Vidar Systems працює Микола, йому близько 60 років. Напрямок роботи компанії безпосередньо співвідноситься зі знаннями, які він здобув ще в інституті, а згодом поглиблював працюючи у спеціальному конструкторському бюро. Для Миколи важливим є колектив, а саме націленість колег на результат та постійний пошук нових рішень. У спілкуванні з молодшими колегами він не тільки передає свій досвід, а і може «постійно навчатися нового».

Олександр з HIMERA має подібні переживання: ***«Я намагаюся залишатися відкритим до нового — іноді почуваю себе навіть молодшим за колег».*** Святослав з Roboneers також відзначає, що йому цікаво слухати свіжі ідеї молодших колег.

Разом вони спростовують уявлення щодо неготовності старшого покоління змінювати свої підходи. ***«Трохи побоювались, що старші колеги можуть повчати, як треба правильно робити, що їм буде складно дослухатись до думки молодших і менш досвідчених людей»,*** — пояснює HR-спеціалістка Vidar Systems. Першої співбесіди з Миколою було достатньо, аби позбавитися цього страху.

Руйнують стереотипи також і старші працівники в HIMERA. Нещодавно команда впроваджувала нову систему внутрішніх комунікацій. Більш досвідчені члени колективу без жодних труднощів перейшли на неї, адже є технологічно підкованими.

Зрештою, Денис Ніколаєнко з Oko Camera нагадує про ще один аспект. У компанії не було можливості забронювати ключових спеціалістів, яких згодом мобілізували. Такий ризик є значно більшим аніж ті, що асоціюються з наймом старшого покоління, наприклад щодо їхнього здоров'я.

Досвід Roboneers навпаки демонструє, що ці страхи також можуть бути перебільшеними. Найстарший працівник за півтора року роботи в компанії жодного разу не брав лікарняного. Інший його досвідчений колега працює на низці стратегічних підприємств без відпусток.

Саме фактор здоров'я обмежує потенціал залучення цієї категорії економічно неактивного населення до Defense Tech компаній. Обмежує, але не нівелює. «Шановні однолітки, — звертається Микола з Vidar Systems, — за наявності здоров'я, приєднуйтесь до тих компаній, де будете відчувати свою потрібність, можливість реалізувати свій досвід, та зможете отримувати стабільний дохід».

За даними платформи з працевлаштування та рекрутингової агенції Lobby X, галузь Defense Tech почала користуватися більшим попитом останні роки повномасштабного вторгнення, зокрема через кращі умови порівняно з мобілізацією та за можливості бронювання.

Кількість працівників на серійних виробництвах*: від 3000 до 5000 людей на компанію.

Кількість працівників у стартапах*: до 50 людей на проєкт.

*Критерії відбору серійного виробника для оцінки:
- Офіційна реєстрація юридичної особи в Україні (ТОВ, ПАТ, тощо).
- Наявність серійного виробництва продукції військового або подвійного призначення (зокрема для ЗСУ або на експорт).
*Критерії відбору стартапів:
- Наявність розробки продукту/рішення військового призначення або подвійного призначення.
- Проходять або пройшли випробування/ демонстрації для ЗСУ, МОУ, Brave1, тощо.
- Офіційна або фактична реєстрація в Україні (іноді у формі ПЗО стартапу без юрособи).

МЕДІАННА ЗАРПЛАТА В ГАЛУЗІ DEFENSE TECH ЗА ДАНИМИ LOBBY X:

Спеціальності	Сума
Робітничі	$800 – $1000
Інженерні	$2000 – $4000
Вузькопрофільні	$3000 – $10 000
Топменеджмент	$6000 – $15 000
Адміністративні	Як і по ринку +20-30%

За словами Lobby X, медіанна зарплати суттєво не відрізняється від масштабності виробництва (серійне або стартап), оскільки ринок один — конкуренція за працівників зберігається.

Як пояснює засновник Lobby X Владислав Грезєв поділ категорій:

- робітничі спеціальності, де знання, досвід та експертиза не грають першочергову роль при наймі — монтажники, слюсарі, електрики, паяльники, складальники тощо. Працедавці звертають увагу на стан здоров'я та можливість людини опанувати професію у короткий термін.
- Інженерні спеціальності, де потрібно мати політехнічний досвід та знання або освіту у суміжних галузях.
- Вузькопрофільні спеціальності, де потрібна експертиза по конкретному фаху, наприклад радіочастоти, мікропроцесорне програмування тощо.
- Топменеджмент виробничих департаментів, тобто керівники виробництв, керівники R&D, Delivery директори тощо.
- Адміністративні вакансії — від офіс-менеджерів, фінансистів та юристів до піарників.

«Ще можна додати про закордонні компанії, які відкривають в Україні офіси: вони усі додають до середньоринкової зарплати 30%, щоб забирати до себе людей», — коментує Владислав Грезєв.

КУЛЬТУРА — КЛЕЙ

Ці інтерв'ю демонструють, що насправді в різних поколінь, об'єднаних галуззю, багато спільного. Більшість приходить в Defense Tech заради внеску в обороноздатність. «Людям важливо бачити результати своєї роботи», — говорить CEO Oko Camera Денис Ніколаєнко.

«Коли ви працюєте у компанії, де у всіх спільна мета та мотивація – перемога у війні, то багато із проблем нівелюється», — погоджується Руслана Пірог, HRD у HIMERA. Таку ж оцінку висловлює HR спеціаліст Roboneers Саша: «Найкращим об'єднуючим компонентом є спільне усвідомлення місії».

Водночас Станіслав прийшов у Vidar Systems, аби зменшити свою економічну залежність від батьків. Про стабільний дохід згадував і його найстарший колега Микола. Усі опитані наголошували на важливості співнавчання.

Як допомогти цим людям відчувати цю синхронізацію? Oko Camera вкладає багато зусиль у налаштування внутрішньої комунікації. Все заради того, аби чути та обговорювати ідеї усіх працівників, незалежно від віку чи досвіду.

Таку ж культуру прагне будувати Roboneers. Марк, її наймолодший працівник, це відчуває і каже: «До моїх думок та пропозицій в робочому процесі завжди дослуховуються». Його це мотивує.

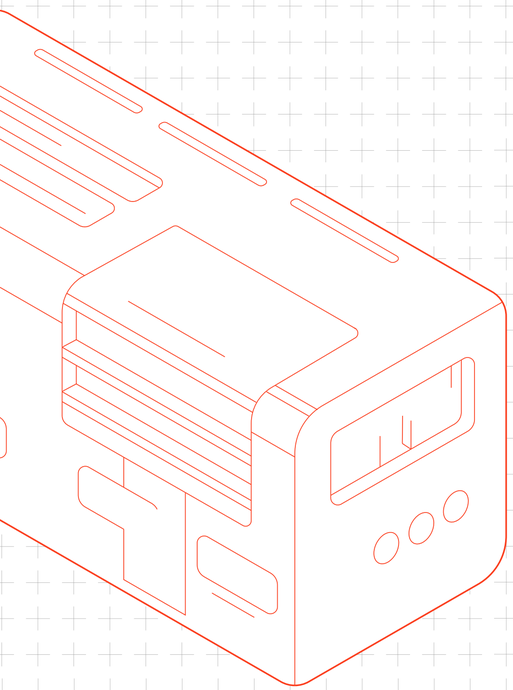
Аби ця модель працювала, необхідно щоб усі її учасники були зацікавлені в цьому. Тому Vidar Systems не візьме в команду кандидатів, якщо вони не мають «базової поваги до людей, їхньої роботи». Це ж стосується і людей, очевидні проблеми з комунікаціями яких оприявнилися ще на етапі співбесід.

Проте навіть тим, у кого ці характеристики є, слід далі їх розвивати. Наприклад, HIMERA допомагає своїм працівникам у тому, аби ті розуміли не лише власні ролі, а і цінність колег. Інструментом для досягнення цієї цілі може бути живе спілкування, офлайн-зустрічі в межах кросфункціональної роботи, пояснює Пирог.

Чи вийде «склеїти» цей пазл так, аби забезпечити передачу експертизи від старшого покоління молодшому і попередити ті втрати експертизи, що відбулися у період між дев'яностими та початком повномасштабного вторгнення? Український Defense Tech зараз має дещо більше гнучкості для утримування персоналу та збереження експертизи, аніж державні оборонні підприємства 30 років тому. «Наприклад, ми можемо пропонувати опціони [право на продаж чи купівлю визначеної кількості акцій компанії. — ред.] ключовим спеціалістам», — говорить CEO Oko Camera Ніколаєнко.

Звичайно, політики на рівні компаній не можуть самостійно забезпечити збереження людського капіталу. CEO Vidar Systems Денис Собчишак наголошує, що це напряму залежить від «подальшого успіху і росту українського приватного оборонного сектору».

ЯК DEFENSE TECH ТЕХНОЛОГІЇ ЗМІНЯТЬ ЦИВІЛЬНІ БІЗНЕСИ



Після повномасштабного вторгнення частину Defense Tech та Dual Use розробок потенційно зможуть використовувати цивільні бізнеси. Водночас поки що не всі готові говорити про можливість такого використання. AIN звернувся до великих українських бізнесів з проханнями про коментар — втім, частина з них пояснила, що поки не готова ділитися цими даними з безпекових міркувань.

Серед тих, хто активно досліджує можливості використання технологій Defense Tech — «Нова пошта».

«Ми маємо досвід використання подібних технологій ще до 2022 року і ділилися ним із Силами оборони України, — зазначають у компанії в коментарі для AIN. — ***Наприклад, у 2021 році тестували у форматі R&D безпілотну доставку між містами України. Йдеться, як про гексокоптери, які до повномасштабного вторгнення використовували, зокрема, в агросекторі, так і про «крила»*** — дрони літачкового типу, здатні долати відстані у сотні кілометрів».

■ Як Defense Tech технології змінять цивільні бізнеси

Наразі спеціалісти НП також працюють над системами «машинного бачення», що дозволятимуть за камерами відстежувати операційні процеси.

У МО в коментарі для AIN зазначають, що започаткували Управління космічної політики, яке буде опікуватись спроможностями України на орбіті: «Супутники, дані — зараз це питання передусім безпеки. Космос потрібен нам для якісного зв'язку, розвідки, раннього виявлення ракетної небезпеки».

У мирні часи, пояснюють в МО, космічні потужності можуть використовуватись в економічних, комерційних цілях: «Завдяки супутникам працює безліч галузей — логістичні компанії, сервіси таксі, у сільському господарстві супутники використовують, щоб слідкувати за врожаєм і його станом, в екології слідкують за зміною ландшафтів тощо».

«Ми бачимо великі перспективи у напрямку dual-use, адже велика частина технологій, зароджених у війні і для війни, можуть успішно застосовуватися і в цивільному житті. І це вже зараз відкриває великі можливості для залучення інвестицій, зокрема для фондів, які принципово не інвестують у Defense Tech», — кажуть у Brave1 в коментарі AIN.

Повномасштабне вторгнення рф стало приводом для багатьох українських стартапів подивитися в бік Dual Use розробок, якщо це дозволяли їхні потужності. Серед компаній, яка почала виробляти рішення подвійного призначення — Ailand Systems. Понад 10 років Ailand Systems спеціалізувалася на ПЗ у сфері комп'ютерного зору, а з 2021-го почала створювати рішення для землеробів.

Повномасштабне вторгнення трансформувало її роботу: CEO компанії Дмитра Титова мобілізували, а в компанії почали розробляти проєкти для розмінування. Серед таких розробок — безпілотний літальний міношукач ST1, який дозволяє значно прискорювати процес розмінування порівняно з роботою людини. Потенційно в Україні залишаються замінованими 139 тис. км² (23% території), тож попит на розробки, пов'язані з розмінуванням, не зникне після закінчення війни.

■ Як Defense Tech технології змінять цивільні бізнеси

«Усі проєкти, пов'язані з дронами, мають значний потенціал до росту, — каже в коментарі для AIN Дмитро Титов. Водночас він також підкреслює: зростання можливо у стартапів та компаній, які зможуть вийти на західні ринки шляхом залучення значних інвестицій. — У нашому випадку закінчення війни буде тільки сприяти зростанню, бо розмінування стане головним пріоритетом, яким, на даний момент, є зброя та засоби ураження».

За словами Титова, у проєкті вже є цивільна складова, оскільки розробку можна використовувати і для військового, і для гуманітарного розмінування. Крім того, плануємо налагодити виробництво дронів для сільського господарства. «Насправді наша компанія розпочиналась саме з дронів сільськогосподарського призначення, які ми адаптували під розмінування після початку повномасштабного вторгнення», — додає він.

Серед українських стартапів, які активні на міжнародних ринках — Bavovna.ai. Dual Use стартап, заснований у 2022-му, вже наступного року став першим українським стартапом, що пройшов до програми Air Force Labs Masschallenge, яка координується Міноборони США і фінансується американським урядом. А 2024-го Bavovna.ai залучила $1,7 млн інвестицій.

Стартап забезпечує рішення і для оборонного сектору, і для цивільних індустрій — логістики, безпеки, інфраструктури та енергетики. Bavovna.AI розробляє систему навігації на базі ШІ для безпілотників, що здатні працювати в умовах відсутності GPS-сигналу та загрози радіоелектронної боротьби.

«Глобальний тренд на переозброєння створює величезне вікно можливостей: країни оновлюють арсенали, фокусуючись на автономних системах нового покоління», — каже СМО та співзасновник стартапу Максим Прасолов у коментарі для AIN, додаючи: цей процес триватиме щонайменше 10 років.

За його словами, Bavovna уже інтегрується у ці процеси, створюючи системи, які працюють без GPS і готові до майбутніх конфліктів. Прасолов пояснює: після війни технології знайдуть широке застосування в цивільному секторі — агро, логістика, інфраструктура, безпека.

■ Як Defense Tech технології змінять цивільні бізнеси

«Технології Bavovna можуть використовуватись для інфраструктурного моніторингу, георозвідки, надзвичайних ситуацій та доставки в складних умовах, — зазначає він. — ***Окремо ми бачимо перспективу у створенні електронних кордонів. Уже сьогодні тисячі кілометрів українського кордону не мають стабільного GPS-покриття — і це лише питання часу, коли країни масово почнуть використовувати системи постійного контролю повітряного простору. Ми вже працюємо над цим».***

Ukrainian Cluster Alliance, посилаючись на дані Brave1, DataDriven та Мінстратегпрому, зазначає — у 2024-му в Україні було понад Dual Use 1000 активних стартапів і малих та середніх підприємств (МСП).

■ Як Defense Tech технології змінять цивільні бізнеси

СЕРЕД DUAL USE СТАРТАПІВ УКРАЇНСЬКОГО ПОХОДЖЕННЯ:

Назва	Напрям роботи	Про стартап
Ailand Systems	Роботизовані системи, БПЛА	компанія працює та створює рішення для землеробів, зокрема для розмінування
Aspichi	VR, медицина	рішення з VR-терапії для лікування психологічних розладів
Bavovna AI	Штучний інтелект	системи автономної навігації для безпілотників
Byne	Штучний інтелект	рішення зі створення захищеної інфраструктури для розгортання великих мовних моделей (LLM) на основі ШІ
Farsight Vision	Мапи, Штучний інтелект	платформа, яка дозволяє пілотам дронів і користувачам відеоматеріалів взаємодіяти для аналітики та ситуаційної обізнаності, використовуючи 3D-моделі та ортофотозображення
DrillApp	IT, Застосунки	застосунок для підготовки військових до використання різних типів зброї
Dropla	Роботизовані системи	технології робототехніки та безпілотників для розмінування
Esper Bionics	Медицина	
EYA	Медицина, Застосунки, ШІ	застосунок для комунікації для людей з обмеженими можливостями на основі ШІ

Назва	Напрям роботи	Про стартап
Falcons	IT	компанія, що виробляє софт і хардвер рішення для військових
Frontline	Роботизовані системи, БПЛА	компанія, що спеціалізується на розробці та виготовленні роботизованих систем
Griselda	Штучний інтелект	геоінформаційна платформа на основі ШІ для військових та гуманітарних операцій
Himera	Зв'язок	тактичні системи захищеного зв'язку
Kara Dag Technologies	Штучний інтелект, БПЛА	детектори БПЛА на основі ШІ
Kolossal	Штучний інтелект, OSINT	платформа, яка збирає та обробляє OSINT-дані (аналіз загальнодоступних супутникових зображень, геоприв'язаних джерел тощо)
Mantis Analytics	Штучний інтелект	платформа моніторингу інформаційного поля в режимі реального часу, керована ШІ
M-FLY	БПЛА	стартап розробляє карданні підвіси для БПЛА, які забезпечують точне визначення дальності, геолокацію та підвищену стабільність
LifeSaver SIM	Медицина, Застосунки	застосунок із тактичної медицини
Logics7	Застосунки	віртуальні рішення для симуляторів вогневої підготовки
Octava Defence	Роботизовані системи	компанія, що розробляє рішення з оптичного та акустичного спостереження.
Osavul	Штучний інтелект	проєкт із захисту від інформаційних загроз на основі ШІ

■ Як Defense Tech технології змінять цивільні бізнеси

Назва	Напрям роботи	Про стартап
Resq Pods	Захист	deep-tech компанія, що розробила рятівну капсулу для індивідуального захисту людей
Rovertech	Роботизовані системи	розміновувачі і безпілотні наземні комплекси для ЗСУ та гуманітарного розмінування
Seismo Analytics	Захист	охоронна система з датчиками прихованого розміщення
Skiftech	Симулятори	симулятор навчання для військових та виробник тренувальних систем від програмного забезпечення до елементів електроніки
Swarmer	Штучний інтелект	ШІ-рішення для управління роями безпілотників
TELETACTICA	Зв'язок	виробник завадостійких модулів телеметрії та відеозв'язку
Tippy Talk	Медицина, Застосунки, ШІ	цифрові інструменти альтернативної і додаткової комунікації для людей з розладами комунікації
Webasto	Роботизовані системи	компанія займається виробництвом кліматичних систем, інтегрованих у різноманітні транспортні засоби, як бронетранспортери
Конструкторське бюро «Логіка»	Симулятори	розробник спеціалізованого комп'ютерного забезпечення, навчально-тренувальної продукції, симуляторів та систем автоматизації

*Список може бути неповним.

■ Як Defense Tech технології змінять цивільні бізнеси

ЩО БУДЕ ЗІ СТАРТАПАМИ

В коментарі для AIN співзасновник ZAS Ventures, голова комітету з венчурних інвестицій і член правління Techosystem Андрій Зінчук зазначав про можливість луснутої «бульбашки» після закінчення війни: на його думку, Defense Tech стартапи можуть перестати отримувати фінансування від держави та не стануть конкурентоздатними на світовому ринку.

«Думаю, це просто доля стартапів. Більшість з них — незалежно від Defense-приналежності — є «бульбашкою». Бульбашки лопаються», — коментує для AIN Антон Тарасюк, Co-Founder стартапу Mantis Analytics.

За його словами, світ входить в епоху «ШІ-перегонів», за аналогією з «перегонами озброєнь»: ***«У 2025 стало зрозуміло, що ШІ — це не про обслуговування консьюмеристських звичок користувачів, на кшталт посилення якості таргету в рекламі чи кращих рекомендацій в сервісах доставки. Системи автоматизованого прийняття рішень — драйвер, що рухатиме проєкти у сфері національної та корпоративної безпеки».***

У XX столітті програмне забезпечення створювалось для обслуговування потреб апаратного забезпечення: від систем управління польотом до бронетранспортерів. З появою ШІ цей взаємозв'язок змінюється. Апаратне забезпечення і люди все більше служать засобом для реалізації рекомендацій штучного інтелекту. Цю траєкторію не змінити.

Світ не є єдиним — політична та мілітарна карта фрагментується. Конкуренція між державами у сфері ШІ буде зростати. Не знаю щодо відсотків тих, хто залишиться, але робота для ШІ-ініціатив буде. Ми бачимо це і по собі. За останній рік Mantis Analytics покращив свою співпрацю з країнами НАТО».

У Mantis Analytics також коментують коментують, що їхні розробки, наприклад, допомагатимуть захищати цивільні бізнеси: йдеться про ситуаційну обізнаність, статус активів, швидку реакцію на загрози.

■ Як Defense Tech технології змінять цивільні бізнеси

Загалом трансформація стартапів після війни — це про серйозний підхід до проблем, рішення справді важких та амбітних задач, говорять в Mantis Analytics.

«Тривалий час стартапи займалися тим, що допомагали людям споживати більше. Це дало гарні комерційні результати, але вбило дух інновацій та прагнення робити речі, які трансформують світ (попри звичний startup-talk) — технології подвійного призначення, люди, які роблять defense-tech рішення, повернуть великі мрії в бізнес. Врешті, альтернативи немає. Ми — не одні в світі, у нас є вороги, і вони хочуть нашої смерті. Добра мотивація, щоб бути амбітним», — зазначають у стартапі.

Після завершення війни потреба в армії залишиться, коментують для AIN в Міністерстві оборони: «Ми маємо справу з підступним ворогом, який має звичай порушувати свої обіцянки. Тому повинні мати таке військо і такі спроможності в обороні, щоб ні у кого в голові не промайнула думка про можливу атаку».

У цьому, зазначають в МО, допомагають інструменти цифровізації — насамперед заощаджуючи час: «Застосунок Резерв+ економить зусилля військовозобов'язаних, які зазвичай витрачаються на поїздки до ТЦК та очікування в чергах. Армія+ пропонує електронні рапорти, які подаються за кілька хвилин, та зручні відеокурси у смартфоні. Військо має орієнтуватися на сьогодення та майбутнє, мати чіткий roadmap для реалізації себе. Звісно, це не так просто, як в IT, але можливо».

Робота Brave1 триватиме, поки є потреба в розвитку оборонних технологій, кажуть у кластері. ***«Після завершення війни ми продовжимо підтримувати інновації, зміцнювати обороноздатність і технологічну спроможність країни. Україна вже має унікальний досвід у сфері оборонних розробок, і ми може стати центром експертизи, який фокусуватиметься на впровадженні та вдосконаленні технологій навіть у мирний час»,*** — зазначають у кластері.

У Brave1 впевнені, що український Defense Tech консолідуватиме зусилля, щоб разом працювати над розв'язанням конкретних проблем на фронті.

«Такий шлях проходили більшість країн, — зазначають у кластері в коментарі для AIN. — ***І це те, що дозволить українським виробникам далі тримати високий темп інновацій як для технологічної переваги над ворогом, так і для конкурування з компаніями, які працюють на ринках НАТО. Хтось займається БПЛА, хтось займається НРК, і для того, щоб більш ефективно працювати в Європі, продавати свої продукти, ці компанії мають об'єднуватися. В такий спосіб вони доповнюватимуть одне одного інженерно і зекономлять ресурси на фінансову підтримку, на юридичний супровід тощо».***

■ Як Defense Tech технології змінять цивільні бізнеси

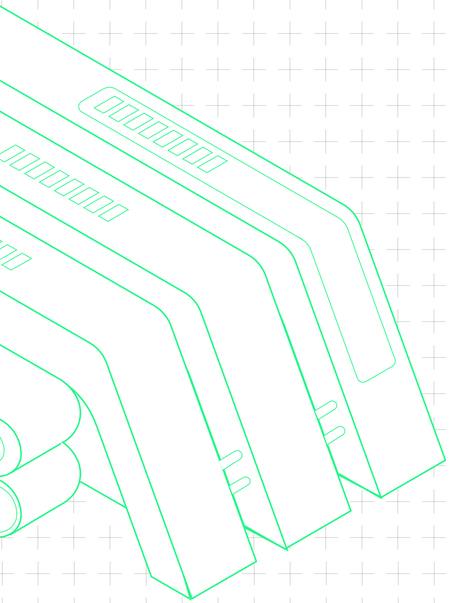
У перспективі, підсумовують у Brave1, закінчення гарячої фази війни однозначно змінить ринок — але не в гірший бік: «Якість команд, якість продукції підвищуватиметься, між командами лишатиметься конкурентність. Виграють і наші військові, і ринок, і держава в цілому. В майбутньому наші команди почнуть конкурувати з іноземними компаніями, і консолідація буде важливим кроком, щоб успішно вигравати міжнародні контракти».

Зміни ринку, вважають у Brave1, насправді не збільшують можливості, зокрема, для залучення інвестицій. Йдеться не лише про інвестиції від венчурних фондів та ангельських інвесторів, а й від великих українські дефенс-компаній: «Компанії вже декларують готовність підтримувати молоді стартапи, щоб тримати швидкість інноваційності, і щоб підтримувати, зокрема, й власну конкурентоспроможність — адже в якийсь момент великі компанії можуть запропонувати стартапам стати частиною великого бізнесу.

«Також ми бачимо, що, крім українських компаній-інвесторів, міжнародні компанії теж розуміють, що українська екосистема інноваційна, створює багато класних проривних рішень. Щоб розділити цей успіх, треба сьогодні заходити як стратегічний партнер. І сьогодні ми вже бачимо перші кейси інвестування від великих іноземних виробників в українські компанії. Іноземний бізнес хоче бути частиною розвитку інноваційних українських компаній, хоче зрозуміти, куди рухаються технології в Україні, щоб в перспективі теж від цього виграти» , — кажуть у Brave1.

Михайло Федоров запевняє, що український Defense Tech став цікавим не тільки з погляду технологій, а й як бізнес. «Кожна війна породжує технології, які згодом стають невід'ємними і в цивільному житті: інтернет, GPS, мікрохвильові печі, інфрачервоні камери та багато інших. ***«Наша війна не стане винятком, і ми вже бачимо великий інтерес інвесторів до так званих dual-use стартапів — коли технологія, яка активно використовується на фронті, уже може застосовуватися в мирному житті. Наприклад, дрони зможуть служити для цілей розвитку та безпеки, логістики й доставки, в агросекторі тощо. Зараз до українських розробок проявляє зацікавленість понад 100 інвестиційних партнерів з більш як 30 країн світу»,*** — каже він.

ПЕРСПЕКТИВИ І ДОЛЯ DEFENSE TECH У ЧАСТЦІ ВВП ПІСЛЯ ЗАКІНЧЕННЯ ВІЙНИ: ЯК ОБОРОННІ ТЕХНОЛОГІЇ ПЕРЕБУДУЮТЬ СТРУКТУРУ ЕКОНОМІКИ НОВОЇ УКРАЇНИ



ДИНАМІКА НОМІНАЛЬНОГО ВВП УКРАЇНИ ТА ОБСЯГІВ ОБОРОННИХ ВИТРАТ У ПЕРІОД З 2007 ПО 2024 РОКИ:

Рік	Номінальний ВВП, $ млрд	Видатки на оборону, $ млрд	Частка оборонних витрат у ВВП, %
2007	148,73	0,49	0,33
2008	188,11	0,60	0,32
2009	121,55	0,64	0,53
2010	141,21	0,70	0,50
2011	169,33	0,70	0,41
2012	182,59	0,79	0,43
2013	190,5	0,83	0,44
2014	133,5	1,1	0,82
2015	91,03	1,8	1,98
2016	93,36	2	2,14

- Перспективи і доля Defense Tech у частці ВВП після закінчення війни

Рік	Номінальний ВВП, $ млрд	Видатки на оборону, $ млрд	Частка оборонних витрат у ВВП, %
2017	112,09	2,3	2,05
2018	130,89	3	2,29
2019	153,88	3,8	2,47
2020	156,62	4,4	2,81
2021	199,77	4,4	2,20
2022	161,99	32,1	19,82
2023	178,76	57,1	31,94
2024	201,5	64,7	32,11

*З 2014 року у розрахунки не входять тимчасово окуповані території України
*Частку оборонних витрати у ВВП ми вираховували за такою формулою: суму оборонних витрати поділили на загальний обсяг номінального ВВП, і результат помножили на 100, щоб отримати відсоток.

■ Перспективи і доля Defense Tech у частці ВВП після закінчення війни

Прогнози. Згідно зі звітом Європарламенту щодо стану української економіки за лютий 2024-го, навіть якби повномасштабна війна закінчилася до кінця того ж року, реальний ВВП України зміг би досягти довоєнного рівня лише у 2030-му. Потенційний обсяг виробництва скоротився більш ніж на 150 млрд (або приблизно на 20%) у 2022 році, водночас чимала частина виробничих потужностей та інфраструктури України зруйновані росією.

У колонці для Atlantic Council голова Українського центру безпеки та співробітництва (УЦБС), колишній радник Секретаря Ради нацбезпеки і оборони України Сергій Кузан зазначає: українська армія підтримується вітчизняним військово-промисловим комплексом. Попри зменшення підтримки від США, Україна зараз є великою військовою державою сама по собі, каже Кузан.

«Хоча ці потужності ще не використовуються повністю через обмеження оборонного бюджету, Україна зараз виробляє близько третини всієї зброї, боєприпасів та обладнання, що використовуються збройними силами країни. У таких критичних сферах, як виробництво безпілотників, цей показник зараз близький до ста відсотків», — говорить він.

■ Перспективи і доля Defense Tech у частці ВВП після закінчення війни

ПОТЕНЦІЙНІ ВИДАТКИ НА ОБОРОНУ ТА БЕЗПЕКУ У 2020–2027 РОКАХ:

Рік	Бюджетні (план), $ млрд	Примітка
2025	49	Ймовірне перевищення бюджету. Військові видатки на 2025-й, згідно з ухваленим ВР бюджетом, мають становити майже всемеро більше порівняно з початком 2022 року і на 47,6 млрд грн більше порівняно з уточненим планом 2024 року. Крім того, видатки на оборону у державному бюджеті на 2025 рік збільшили і протягом поточного року. У липні 2025-го року Верховна рада ухвалила зміни до бюджету сумарно на майже 30 млрд грн. Із них 1,4 млрд грн виділили на нову програму для закупівлі спеціальної техніки, дронів та обладнання для тестування у бойових умовах. Та 2,8 млрд грн — гранти на розвиток виробництва у сфері defense tech.
2026	35	
2027	33	

Дані: DataDriven

Автори:	Анастасія Ампілогова, Олександр Ігнатенко, Анастасія Горпінченко, Юлія Бондар
Редактори:	Юлія Бондар, Олександр Стрельников, Анастасія Іванцова
Дослідники:	Molfar
Партнер дослідження:	Calibrated
Літературна редакторка:	Вікторія Оліщук
Артдиректорка:	Поліна Цай
Продюсерка:	Вікторія Хоровець
Дизайн і верстка:	Artycoders
Фото:	BRDO, Олександр Ябчанка, Катерина Черногоренко / пресслужба Міноборони, Артем Романюков, пресслужба «Азов», Олег Берестовий
За підтримки:	**Офіс ефективного регулювання BRDO**