

DOI <https://doi.org/10.32782/2956-333X/2025-3-8>

OBRONA I MASKOWANIE W PRZECIWDZIAŁANIU ATAKOM BEZZAŁOGOWYCH SYSTEMÓW NA BLISKIM DYSTANSIE

MULTI-LAYERED DEFENSE AGAINST CARRIER-CONFIGURED UAVS: FROM CAMOUFLAGE TO CLOSE-RANGE COUNTER-FPV

Serhii Kryvoshlykov,

*kandydat nauk technicznych, PrAT «Wyższa uczelnia „Międzyregionalna Akademia Zarządzania
Personelem”», docent Katedry Bezpieczeństwa Narodowego, m. Kijów, Ukraina*

orcid.org/0009-0008-5494-8880

Summary. The article examines multi-layered defense against carrier-configured UAV employment, in which high-altitude fixed-wing platforms perform supplementary reconnaissance, target designation, and the launch of suspended FPV “kamikaze” drones with subsequent handover to dedicated operators. Drawing on consolidated field experience of Ukrainian aerial reconnaissance teams, the paper proposes a science-to-practice model that integrates physical, electromagnetic, and organizational protective measures and positions unit-level operational security as the first and mandatory layer of countermeasures. The model covers the full cycle of actions: from position camouflage; control of sound, light, and heat signatures; communication hygiene and EMCON; to regulated take-off/landing procedures at offset points; secure wiping and encryption of data carriers; the use of remote antennas and work from cover; as well as the integration of situational awareness systems.

Key “windows of vulnerability” in carrier schemes are identified: the activation and separation interval of FPV drones; the separation of control channels and short-term spikes of electromagnetic emission; recurrent logistical patterns of launches; and dependence of detection quality on weather and scene contrast.

It is shown that targeted signature reduction, rotation of in-the-clear code phrases on the radio, recipient verification via video calls, controlled disinformation inside the unit, and deployment of decoy electronic beacons significantly increase position survivability. The close-range counter-FPV layer is highlighted as the terminal shield of defense, encompassing local jamming assets, intercept solutions, deception tools, and action protocols during artillery fire, telemetry loss, or navigation jamming.

A system of SOPs and checklists is substantiated for standard and non-standard scenarios, tied to defense effectiveness metrics: time-to-detection, share of disrupted attacks, attrition of enemy assets, and frequency of relocating own launch sites. The proposed approach is applicable to personnel training, operational planning, and the standardization of tactical procedures in aerial reconnaissance units.

Keywords: UAV; carrier configurations; swarming links; electronic warfare (EW); electromagnetic silence (EMCON); camouflage; communication hygiene; operational security (OPSEC); counter-FPV; SOPs; situational awareness.

1. Wprowadzenie

Współczesny etap wojny dronów charakteryzuje się pojawieniem się przenośnych konfiguracji zastosowania bezzałogowców, w których wysokościowe platformy typu „skrzydło” na pułapach do 2–3 km wykonują dozwiad, wskazywanie celów oraz uruchamianie podwieszonych dronów FPV-kamikadze z dalszym przekazaniem sterowania poszczególnym operatorom. Taka architektura zmniejsza skuteczność frontowych środków walki radioelektronicznej, skraca czas dolotu dronów uderzeniowych i minimalizuje ich przebywanie w strefie aktywnych zakłóceń, jednocześnie rozdzielając w przestrzeni i czasie kanały sterowania oraz maskując źródła emisji elektromagnetycznej. W tych warunkach tradycyjne podejścia do ochrony pozycji, opierające się głównie na lokalnych systemach walki radioelektronicznej, środkach maskujących oraz fragmentarycznych rozwiązaniach inżynieryjnych, okazują się niewystarczające: nie obejmują pełnego cyklu oznak demaskujących (wizualnych, akustycznych, cieplnych, elektromagnetycznych), nie standaryzują procedur startu i lądowania w oddalonych punktach, nie regulują higieny informacyjnej oraz weryfikacji kanałów komunikacji, a także słabo uwzględniają „okna podatności” przeciwnika podczas aktywacji i odłączania FPV.

Brak jednolitego, naukowo uzasadnionego regulaminu wielowarstwowej obrony – od maskowania i reżimów EMCON/OPSEC po bliski kontur przeciwdziałania FPV oraz system SOP i list kontrolnych dla scenariuszy rutynowych i niestandardowych – prowadzi do zwiększonej podatności pozycji, wzrostu strat

i niestabilności działań taktycznych pododdziałów rozpoznania powietrznego. Zatem zadanie naukowo-praktyczne polega na zbudowaniu zintegrowanego modelu obrony, zdolnego zmniejszyć prawdopodobieństwo wykrycia, zakłócić cykl ataku przenośnego i zapewnić odporność pododdziałów w warunkach eskalacji zagrożeń rojowych.

2. Analiza ostatnich badań i publikacji

Współczesny zbiór źródeł dotyczących wojny dronów rozwija się w kilku powiązanych kierunkach: opis i klasyfikacja FPV jako narzędzia taktycznego rażenia; rozpoznanie i wskazywanie celów z użyciem wysokościowych platform typu „skrzydło”; środki i tryby walki radioelektronicznej przeciwko małogabarytowym dronom; bezpieczeństwo organizacyjne pododdziałów (OPSEC/EMCON) i standaryzacja procedur użytkowania; a także środki przeciwdziałania krótkiego zasięgu przeciw odłączonym dronom-kamikadze. W otwartych źródłach przeważają materiały praktyczne – polowe instrukcje zwiadowców powietrznych, podręczniki inicjatyw wolontariackich, wykłady instruktażowe i listy kontrolne, które kryształizują doświadczenie frontu w regulaminy zachowań na pozycjach, zasady maskowania, algorytmy startu/lądowania, wymagania dotyczące higieny komunikacyjnej i obiegu danych. Publikacje naukowe i techniczne skupiają się na modelach wykrywania i przechwytywania małych dronów, na charakterystyce sygnałów sterowania i nawigacji, na wpływie warunków pogodowych i kontrastu scenicznego na wykrywalność, a także na integracji lokalnych zagłuszcaczy, węzłów sensorycznych i taktycznej OPL w jednolity system C-UAS. Osobną grupę stanowią prace dotyczące odporności informacyjnej i elektromagnetycznej pododdziałów, które dowodzą kluczowej roli reżimów ciszy radiowej, rozdzielania kanałów, rozwiązań retransmisyjnych i dyscypliny personelu w redukcji ryzyka naprowadzania celów.

Cel badań – opracować i naukowo uzasadnić zintegrowany model wielowarstwowej obrony przeciwko przenośnym konfiguracjom dronów, łączący środki fizyczne, elektromagnetyczne i organizacyjne (OPSEC/EMCON, regulaminy startu/lądowania, ochronę wymiany danych i bliski kontur przeciwdziałania FPV) oraz weryfikowany poprzez identyfikację „okien podatności” przeciwnika i system operacyjnych miar skuteczności.

3. Architektura i zasady wielowarstwowej obrony

Współczesna ewolucja bojowego zastosowania dronów świadczy o przejściu od izolowanych lotów taktycznych quadropterów do przenośnych konfiguracji, w których wysokościowe platformy typu „skrzydło” wykonują dozwiad i wskazywanie celów z następnym uruchomieniem podwieszonych dronów FPV-kamikadze, które przejmują sterowanie poszczególni operatorzy. Taki „rozwiązany” w przestrzeni i czasie cykl – wykrycie celu na pułapie 2–3 km, aktywacja dwóch dronów uderzeniowych, rozdzielanie kanałów sterowania oraz krótki, energooszczędny nalot na cel – znacząco obniża skuteczność frontowych środków walki radioelektronicznej, omija lokalne strefy zagłuszania i minimalizuje czas przebywania dronów uderzeniowych w polu zakłóceń. Odpowiednio, środki przeciwdziałania obronnego muszą być budowane jako system wielowarstwowy, w którym „pierwsza warstwa” – bezpieczeństwo operacyjne zwiadowcy powietrznego i pozycji – jest równie ważna jak techniczne rozwiązania przechwytywania bliskiego zasięgu czy taktyczna OPL.

W punkcie wyjścia takiego systemu znajduje się pełna inwentaryzacja kanałów ryzyka. Zewnętrzne źródła demaskowania obejmują oznaki wizualne i akustyczne, zapachy dymu i paliwa, kontur cieplny ludzi i sprzętu, a także promieniowanie elektromagnetyczne wszystkich włączonych urządzeń. Źródła wewnętrzne – czynnik ludzki, wycieki przez niedyscyplinowaną komunikację, nieautoryzowany obieg współrzędnych, lokalne agentury. Na pułapie 2–3 km optyka „skrzydła” wychwytuje drobne wzorce niewidoczne z ziemi, dlatego dyscyplina niewidzialności opiera się na profilu pozycji: ruch i światło – tylko w razie potrzeby; kontur cieplny obniżony przy pomocy prostych ekranów i warstw, np. brezentowego płaszcza na hełmie i kamizelce kulo odpornej; brak kontrastowych geometrii w terenie dzięki starannemu planowaniu osłon i inżynierskiemu wyposażeniu. Takie zasady nie są abstrakcją – to praktyka, która bezpośrednio zmniejsza prawdopodobieństwo pierwotnego wykrycia przez drona rozpoznawczego.

Maskowanie sprzętu i pozycji powinno jednocześnie eliminować kilka spektrów obserwacji. Wizualnie – dzięki naturalnym formom osłon, unikaniu świeżych śladów prac leśnych w bezpośrednim

sąsiedztwie, maskowaniu pni i gałęzi, rozmieszczaniu nowych drzew pod koronami istniejących, a nie na otwartych sylwetkach. Ciepłnie – poprzez ekrany nad punktami oddawania ciepła, dyscyplinę nocną (brak gorących płam nad schronami, minimum urządzeń grzewczych), krótkie i przewidywalne tryby pracy kuchennych punktów i generatorów. Elektromagnetycznie – poprzez systematyczne stosowanie EMCON: wszystkie urządzenia, od radiostacji i smartfonów po terminale łączności satelitarnej, utrzymywane są w trybie „ciszy” i włączane tylko na krótkie sesje pracy, po których są natychmiast wyłączane; ładowanie z „cichych” buforowych akumulatorów zamiast głośnych generatorów; minimum Wi-Fi, Bluetooth, danych mobilnych i geolokalizacji. Innymi słowy, pozycja powinna pozostawać „zimna” i „niema”, gdy nie realizuje zadania.

Higiena komunikacyjna – krytyczny moduł architektury obrony. Komunikacja robocza odbywa się z czystych kont i kart SIM, oddzielonych od numerów osobistych; aplikacje o podwyższonym ryzyku kompromitacji nie są używane, a wiadomości mają politykę automatycznego kasowania, brak otwartych powiązań z profilami publicznymi. Połączenia głosowe z telefonów komórkowych w strefie walk otwierają drogę do radiolokacji; zamiast tego stosowane są krótkie, kontrolowane kanały z wcześniej uzgodnionymi zwrotami kodowymi, regularnie rotowanymi. Przekazywanie danych wrażliwych odbywa się w towarzystwie obowiązkowej weryfikacji osoby połączeniem wideo, co eliminuje część „legendowanych” kontaktów. W ramach pododdziału wprowadza się praktykę kontrolowanej dezinformacji dla wykrycia wewnętrznych wycieków. Wszystkie te działania bezpośrednio ograniczają sytuacje, w których „skrzydło” otrzymuje wskazówki celów nie tylko z optyki, ale również z naprowadzonych kanałów komunikacji.

Procedury lotne tworzą odrębny kontur przeciwdziałania rozpoznaniu. Start i lądowanie nie odbywają się na pozycji; punkt startowy jest oddalony o setki metrów i zmieniany, lądowanie – w przygotowanym punkcie z natychmiastowym odejściem. Tryb wejścia do „swojego” kwadratu jest przećwiczony na małej wysokości z użyciem terenowych „kieszeni” ukrywających promieniowanie. Nagranie rozpoczyna się w bezpiecznej odległości od swoich i kończy przed wejściem w „cieplą” strefę. Dla DJI bez anonimizera obowiązuje osobny regulamin: wyłączona geolokalizacja, Wi-Fi i Internet mobilny, kolejność „najpierw pilot – potem dron”, a przy wyłączaniu odwrotnie; po lądowaniu – natychmiastowe odłączenie zasilania i zmiana miejsca. Takie drobne na pozór procedury często decydują o tym, czy przeciwnik doprowadzi trasowanie do rzeczywistego miejsca pracy operatora.

4. Operacyjne wdrożenie obrony i dyscyplina pola

Bezpieczeństwo danych – to kolejna linia obrony. Pamięć pokładowych urządzeń jest czyszczona przed lotem, pamiętając, że proste „usunięcie” kasuje jedynie nagłówki plików, pozostawiając ich zawartość możliwą do odzyskania; stosuje się narzędzia nieodwracalnego nadpisywania, szyfrowania oraz opcję „secure erase”, jeśli jest dostępna. Nośniki z pokładu są natychmiast przenoszone do bezpiecznego obiegu, unika się przechowywania dużych zbiorów nieprzetworzonych materiałów wideo w jednym miejscu. Na samych platformach celowe jest posiadanie śladów GPS, które pozwalają szybko odnaleźć urządzenie lub, w razie jego zdobycia przez przeciwnika, naprowadzić ogień na współrzędne utraty. W kompleksie te działania uniemożliwiają przekształcenie zestrzelonego lub przechwyconego drona w dane wywiadowcze przeciwko własnej pozycji.

Oddzielnego podkreślenia wymaga moduł współdziałania i przygotowania topograficznego. Każdy dzień lotu planowany jest jako scenariusz: role i rezerwy, linie łączności i formaty przekazywania danych, wymagania dotyczące osłony operatora, timing i „okna” między ostrzałami przeciwnika dla przemieszczania się, co najmniej dwa alternatywne trasy odwrotu. Sąsiednie pododdziały są wcześniej poinformowane o ogólnych założeniach działań, aby uniknąć ognia sojuszniczego, lecz bez ujawniania dokładnych punktów startu/lądowania. Szczegółowe poznanie mapy w promieniu 15–20 km to nie „bonus”, lecz obowiązek: szybkość podejmowania decyzji w powietrzu wprost zależy od „pamięci mięśniowej” ukształtowania terenu.

Ludzki wymiar przeżywalności jest nie mniej istotny niż technika. Podstawowy zestaw żołnierza – broń, amunicja, woda, racja energetyczna, taktyczna apteczka, powerbank, zapasowe skarpety, prosty „klawiszowy” telefon w stanie wyłączonym – powinien być tak samo oczywisty, jak naładowany kontroler i pięć–sześć baterii do drona. Taktyczna medycyna to obowiązkowy komponent przygotowania;

testowanie wyposażenia pod obciążeniem na początku cyklu pomaga wcześniej wyeliminować elementy przeszkadzające w rzeczywistej dynamice. Wszystko to jest bezpośrednio związane z reżimami ataku przenośnego: gdy w powietrzu działa już „skrzydło”, czas reakcji się skraca, a organizm musi „pamiętać” działania tak samo pewnie jak głowa.

W warunkach szerokiego zastosowania łączności satelitarnej kluczowe znaczenie ma prawidłowa eksploatacja terminali. Każda sesja pracy obliczana jest według „kosztu” sygnatury elektromagnetycznej: miejsce rozstawienia wybiera się tak, aby istotne kontury pozycji nie zamieniały się w stałe punkty orientacyjne, czas pracy – minimalny, konfiguracje – z priorytetem trybów „cichych”. W razie potrzeby stosuje się fałszywe „światła” – kontrolowane aktywne urządzenia na fikcyjnych pozycjach, które „przyjmują” na siebie próby naprowadzania lub rozpoznania przeciwnika. Narzędzie to jest szczególnie przydatne przeciw przeciwnikowi, który przyzwyczaił się „doklejać” optykę „skrzydła” do telemetrii i sygnałów od naziemnych abonentów.

Kiedy schemat przenośny przechodzi w fazę ataku – aktywacja FPV i ich odłączanie – powstają „okna podatności” przeciwnika. W tym momencie następuje krótkotrwałe manewrowanie kanałami sterowania, pojawiają się szczyty emisji elektromagnetycznej i zauważalne zmiany w wzorcach ruchu „skrzydła”. Właśnie wtedy największą wartość ma wcześniej przygotowany system bliskiego kontratakowania: lokalne środki zakłócające, przechwytywacze, środki imitacyjne, które zaburzają naprowadzanie, oraz standaryzowane protokoły działań podczas ostrzału artyleryjskiego, utraty telemetrii lub zakłócenia nawigacji. Taki kontur nie istnieje w próżni: jego skuteczność rośnie, gdy podstawowe warstwy – maskowanie, EMCON, higiena komunikacyjna, regulaminy startu/ładowania – już „usunęły szum” i zmniejszyły prawdopodobieństwo skutecznego rozpoznania.

Standaryzacja w SOP i listach kontrolnych przenosi wymienione praktyki z poziomu „dobrych rad” do trwałej rutyny organizacyjnej. Oddzielne listy kontrolne celowe jest powiązać z fazami: przygotowanie przed wyjazdem; przygotowanie do lotu; zachowanie na pozycji; osobny regulamin dla DJI z uwzględnieniem ryzyk Aeroscope; działania po locie na PDD/miejsu dyslokacji; scenariusze odchyłeń – zakłócenie GPS, zanik telemetrii, spadek jakości kanału wideo, ostrzał. System powinien być kompaktowy, a jednocześnie wyczerpujący, z oznaczeniem odpowiedzialnych i harmonogramami. Takie podejście nie tylko zwiększa prawdopodobieństwo sukcesu konkretnego lotu, ale także gromadzi pamięć organizacyjną pododdziału.

Ocena skuteczności wielowarstwowej obrony wymaga metryk odzwierciedlających rzeczywistą złożoność zagrożenia przenośnego. Czas do wykrycia nalotu lub aktywacji FPV, odsetek udaremnionych ataków w stosunku do liczby zarejestrowanych podejść, straty środków przeciwnika (zestrzelone lub zakłócone FPV, zmuszone do odwrotu „skrzydła”), częstotliwość zmiany własnych platform startowych, średni „cykl życia” fałszywych pozycji, średni czas sesji EM na pozycji, dyscyplina wykonywania SOP – wszystkie te wskaźniki stanowią podstawę decyzji zarządczych: co skalować, co korygować, co odrzucać jako zbyt ryzykowne. W rezultacie powstaje system adaptacyjny, zdolny przeciwdziałać nie tylko aktualnej wersji konfiguracji przenośnych, ale i ich kolejnym iteracjom.

Integracja przedstawionego „jądra bezpieczeństwa” z danymi wywiadowczymi o konkretnych wzorcach stosowania przez przeciwnika schematu „skrzydło + dwa FPV” zapewnia obronie przewagę w tempie podejmowania decyzji. Tam, gdzie przeciwnik opiera się na wysokości, optyce i rozdzieleniu kanałów, naszą odpowiedzią powinno być połączenie „zimnej” pozycji, racjonalnego obiegu danych, uregulowanej dyscypliny lotniczej, umiejętnego wykorzystania łączności satelitarnej i bliskiego kontrataku. To nie „jednorazowa instrukcja”, lecz operacyjny model zdolny działać dzień po dniu – zarówno na tyłach, jak i na pierwszej linii – niezależnie od tego, czy przeciwnik atakuje rojami FPV, czy kontynuuje eksperymenty z nowymi konfiguracjami przenośnymi i algorytmami naprowadzania celów.

Przenośne konfiguracje zastosowania bezzałogowców z wysokościowym skrzydłem jako platformą dozwiadu i startu dwóch podwieszonych FPV-kamikadze zmieniają logikę ryzyka dla pododdziałów naziemnych. Na wysokościach dwóch–trzech tysięcy metrów skrzydło długo utrzymuje orbitę, wyszukuje oznaki demaskujące pozycję i w dogodnym momencie aktywuje drony uderzeniowe, przekazując ich sterowanie poszczególnym operatorom. Cykl ataku jest rozdzielony w przestrzeni i czasie, więc standaryzowane protokoły taktyczne walki radioelektronicznej w strefie bliskiej nie gwarantują już udaremnienia

podejścia. W tych warunkach wielowarstwowa obrona zaczyna się nie od środka technicznego, lecz od dyscypliny organizacyjnej i niewidoczności pozycji: braku zbędnych ruchów w polu widzenia, zerowego tła świetlnego i akustycznego, obniżonego profilu cieplnego i laboratoryjnej precyzji energetycznego zachowania wszystkich urządzeń elektronicznych, włącznie z terminalami łączności satelitarnej.

Cisza elektromagnetyczna staje się poziomem bezpieczeństwa równym przemysłanej inżynierii osłon. Każde urządzenie traktowane jest jak nadajnik, a każda transmisja danych – jak operacja z jasno określonym celem, miejscem i czasem trwania. Komunikacja włączana jest tylko na okres pracy i natychmiast wyłączana, sesje łączności satelitarnej planowane są w oknach, gdy pozycja nie prowadzi innej aktywnej działalności, a miejsce rozstawienia terminala nie pokrywa się z roboczym jądrem pododdziału. Ładowanie organizowane jest przez buforowe akumulatory, co pozwala nie uruchamiać generatora bez konieczności. Telefony komórkowe, zegarki, tablety i radiostacje działają w trybach minimalnej emisji, geolokalizacja i interfejsy bezprzewodowe są wyłączone domyślnie, a wznowienie łączności po przerwie odbywa się z nowego punktu, aby nie tworzyć przeciwnikowi powtarzalnych sygnatur radiowych na mapie.

Niewidzialność termowizyjna i wizualna wymaga codziennej wrażliwości na drobiazgi. W nocy pozycja nie tworzy „gorących plam” nad schronami, źródła ciepła są osłonięte ekranami, a trasy podejścia nie tworzą wyraźnych linii kontrastu w roślinności. Maskowanie sprzętu rozwiązuje się nie materiałami, lecz logiką sylwetki: świeże wycinki wykonuje się w oddaleniu, pniaki i gałęzie maskuje, nowe elementy wbudowuje pod koronę istniejących drzew, aby z góry nie powstawała geometria „chwytająca” optykę. Nawet tak prosta rzecz jak brezentowy płaszcz na kamizelce kuloodpornej i hełmie zmniejsza czytelność ciepłej sylwetki człowieka na tle gruntu lub roślinności i utrudnia maszynową klasyfikację celu na obrazie z wysokości.

Procedury lotne stają się równie ważne jak maskowanie taktyczne. Start i lądowanie odbywają się w oddalonych punktach, które zmieniają się według scenariusza, aby uniknąć powtarzalności; operator pracuje spod osłony, przez wysunięte anteny, a sam ma ochronę dwóch żołnierzy. Nagranie rozpoczyna się z dala od własnych pozycji i kończy przed wejściem w „ciepłą” strefę, aby uniemożliwić ustalenie trasy do miejsca sterowania. Podczas podejścia do własnych sektorów dron prowadzony jest w załamaniach terenu na minimalnej wysokości, ukrywając emisję. Dla platform bez anonimizera utrzymuje się ścisłą kolejność włączania i wyłączania pokładów i kontrolerów, geolokalizacja i interfejsy bezprzewodowe są wyłączane z wyprzedzeniem, a po wylądowaniu urządzenie jest natychmiast odłączane od zasilania, a grupa zmienia pozycję, nie pozostawiając przeciwnikowi czasu na analizę śladów.

Higiena cyfrowa sprowadza do zera wartość zestrzelonego lub utraconego drona dla rozpoznania przeciwnika. Karty pamięci są czyszczone nie nominalnie, lecz pełnym nadpisaniem, a tam, gdzie to możliwe – szyfrowaniem pokładowym. Surowe materiały są zdejmowane z urządzeń polowych do chronionego obiegu i nie są gromadzone w jednym miejscu, aby jedno niepowodzenie nie stało się punktem kompromitacji całego pododdziału. Na pokładzie celowe jest umieszczenie trackera, który pomaga odzyskać drona lub zamienić miejsce jego utraty w współrzędne dla ognia. Osobno dyscyplinuje się konta osobiste i robocze kanały: do operacyjnych komunikacji stosuje się odrębne profile i karty SIM, ustawia automatyczne kasowanie wiadomości, unika się rozwiązań o znanych ryzykach dla poufności, a dane wrażliwe nie są przekazywane otwartymi kanałami bez weryfikacji tożsamości połączeniem wideo.

Bezpieczeństwo komunikacyjne uzupełnia się taktyką kontrolowanej dezinformacji i weryfikacji kontaktów. Podejrzane kanały testuje się małoistotnymi informacjami, które oznaczają wyciek, a wykryte strefy ryzyka izoluje bez tworzenia atmosfery nieufności w zespole. Wszelkie połączenia głosowe w strefie działań bojowych są minimalizowane, zamiast tego stosuje się krótkie sygnały według uzgodnionych fraz, które regularnie się zmieniają. Kontakty z ludnością cywilną odbywają się z chłodną uprzejmością i uwagą na markery behawioralne, a profile w mediach społecznościowych są blokowane lub czyszczone tak, aby przeciwnik nie uzyskał punktów zaczepienia do presji w przypadku niewoli.

Bliski kontur przeciwdziałania FPV zamyka ostatnie sekundy przed uderzeniem. Działa tu prosta logika: agresywny FPV zależy od stabilnego kanału wideo, rozpoznawalnych kontrastów i przewidywalnego ruchu celu. Lokalne środki zakłócające, nawet niskiej mocy, przykrywają finałowy nalot i tworzą krótki korytarz niepewności, w którym połączenie dymnych lub termicznych wabików z manewrem personelu może zakłócić podejście. Proste przechwytywacze i środki walki bliskiej nie zastępują dyscypliny

maskowania i ciszy, ale potęgują ich efekt, gdy pozycja nie emituje wyraźnych sygnałów. Decydujący staje się czas reakcji, dlatego jednostka wcześniej ćwiczy przejście od obserwacji do przechwycenia lokalnego, a trasy uderzeń dla środków rażenia przygotowuje w okresach spokoju, aby w kryzysie nie tracić sekund na uzgadnianie.

Dziesiątki drobnych decyzji składają się na trwałą przewagę nad nosicielem. Pozycja unika powtarzalności ogólnej i czasowej: platformy startowe rotuje się częściej, niż tego oczekuje przeciwnik; trasy dojsčia są zmieniane; nawet czas ładowania elektroniki nie staje się rutyną. Profil inżynierski osłony planowany jest tak, aby operator mógł przechodzić między wcześniej przygotowanymi punktami bez wychodzenia na otwartą sylwetkę. Przy braku zagrożenia artyleryjskiego lepiej poświęcić godzinę na pogłębienie pozycji i przygotowanie schowków na sprzęt niż raz szybko przeprowadzić lot i narazić się na wykrycie przez pozostawione plamy cieplne i ślady cyfrowe.

Współpraca z sąsiednimi pododdziałami tworzy kontur bezpieczeństwa szerszy niż jedna pozycja. Ogólne założenie działań uzgadniane jest osobiście, z minimum szczegółów – tyle, by uniknąć ognia sojuszniczego i zapewnić wzajemne wsparcie, lecz bez ujawniania pełnego obrazu w razie przechwycenia łączności. Oddzielne ustalenia dotyczące znaków umownych na mapach, kolejności przekazywania wskazań celów, priorytetów użycia kanałów komunikacyjnych i miejsc rozstawienia terminali satelitarnych zmniejszają prawdopodobieństwo tworzenia „węzłów” emisji przyciągających skrzydło. W kluczowych obszarach celowe jest stosowanie fałszywych punktów elektronicznych na pustych miejscach, by zmuszać przeciwnika do weryfikacji fikcyjnych celów.

Przygotowanie personelu i kultura SOP zamieniają każdą rekomendację w nawyk, a nawyk w automatyzm. Przygotowanie przed wyjazdem odbywa się według kart kontrolnych, w których każdy punkt ma odpowiedzialnego; przygotowanie lotne obejmuje sprawdzenie dronów, anten, akumulatorów i nośników; zachowanie na pozycji określone jest tak, aby żadna czynność nie tworzyła odwrotnej sygnatury; osobne zasady uwzględniają specyfikę platform, które mogą być identyfikowane przez przeciwnika za pomocą środków monitoringu technicznego; działania po locie zamykają cykl bez pozostawiania danych i artefaktów. Sytuacje awaryjne opisane są jako algorytmy z ostrymi ramami czasowymi na przypadki zakłócenia nawigacji, utraty telemetrii, ostrzału czy konieczności awaryjnego zakończenia misji. Regularne analizy akcji z rejestracją prostych metryk – czasu wykrycia, odsetka udaremnionych ataków, średniej długości sesji komunikacyjnych, częstotliwości rotacji platform startowych – utrzymują system w stanie ciągłego doskonalenia.

Czynnik ludzki sprowadza się nie do abstrakcji, lecz do konkretnej wytrzymałości, ergonomii i samoontroli. Operator powinien pracować w sprzęcie, który wytrzymuje stres ruchu i nagłego schronienia, a nie tylko spokój w punkcie sterowania. Podstawowy zestaw do długiego pobytu w terenie trzymany jest pod ręką; nawyki korzystania z mediów społecznościowych i fotografowania są modyfikowane w kierunku zerowej widoczności; zasady zachowania wobec ludności cywilnej są ściśle przestrzegane, nawet gdy okoliczności kuszą do kompromisów. Próba oszczędzenia czasu lub pominięcia drobiazgu w tym kontekście niemal zawsze kończy się problemem, ponieważ właśnie w szczegółach skrzydło z wysokości znajduje punkt zaczepienia, a FPV – swój ostateczny wektor.

Ostatecznym celem przyjętej architektury obrony nie jest stworzenie nieprzeniknionej kopuły, lecz uczynienie cyklu ataku nosiciela niestabilnym w krytycznych punktach. Gdy pozycja pozostaje zimna i niema przez większość czasu, gdy procedury lotne nie pozwalają prześledzić trasy do operatora, gdy dane nie stają się bronią przeciwko nam, gdy bliski kontur potrafi wytworzyć sekundową niepewność w końcowej fazie ataku, gdy jednostka działa według SOP i doskonalą je analizą przeprowadzonych misji – schemat nosiciela traci najważniejsze: przewidywalność wyniku. Tego właśnie potrzebuje obrona naziemna, by wytrzymać tempo nowoczesnego zagrożenia powietrznego i stopniowo odwracać równowagę na swoją korzyść.

5. Wnioski

W pracy opracowano i uzasadniono zintegrowany model wielowarstwowej obrony przed przenośnymi konfiguracjami dronów, w których wysokościowe skrzydło wykonuje dozwiad, wskazywanie celów i start podwieszonych FPV z dalszym przekazywaniem sterowania poszczególnym operatorom.

Podstawową warstwą uznano bezpieczeństwo operacyjne pododdziału: maskowanie profilu wizualnego, akustycznego i cieplnego, ciszę elektromagnetyczną oraz higienę komunikacyjną. Wykazano praktyczne znaczenie regulaminów startu i lądowania w oddalonych punktach, pracy operatora spod osłony przez wysunięte anteny, polityki zerowego wycieku danych oraz zastosowania bliskiego konturu przeciwdziałania FPV dla zakłócenia finalnego ataku. Zidentyfikowano kluczowe „okna podatności” przeciwnika podczas aktywacji i odłączania FPV i pokazano, że standaryzowane SOP i listy kontrolne, wzmocnione systemem metryk operacyjnych (czas do wykrycia, odsetek udaremnionych ataków, długość sesji EM, rotacja platform startowych), przekształcają obronę w sterowany, powtarzalny proces nadający się do szkolenia i planowania.

Perspektywy dalszych badań. Wymagają rozszerzonej empirycznej weryfikacji skuteczność środków bliskiego przeciwdziałania FPV w różnych warunkach terenowych i pogodowych oraz wobec zmiennych profili zagrożenia; celowe są eksperymenty z parametrami lokalnych zagłuszcaczy, dymnych i termicznych wabików, a także trybami działania fałszywych punktów elektronicznych. Perspektywiczne jest tworzenie rozproszonych sieci sensorów wczesnego ostrzegania oraz algorytmów automatycznego wykrywania oznak aktywacji/odłączania FPV na podstawie wskaźników optycznych i radiotechnicznych, opracowanie stanowisk symulacyjnych i cyfrowych bliźniaków do doskonalenia SOP z uwzględnieniem czasowych „okien podatności” nosiciela, a także integracja proponowanego modelu z istniejącymi systemami OPL i systemami dowodzenia. Osobny kierunek stanowi ujednolicenie metryk oceny, standardów modułów szkoleniowych dla zwiadowców powietrznych i adaptacja regulaminów do spodziewanej ewolucji środków przeciwnika, w tym wzrostu autonomii i zastosowania sztucznej inteligencji na pokładach platform uderzeniowych.

Bibliografia

1. Institute for the Study of War (2025, October 9). Russian force generation and technological adaptations update. <https://www.understandingwar.org/>.
2. The New Voice of Ukraine (2025, August 22). Ukraine's 118th Brigade destroys Russian Orlan drone carrying two FPV drones. <https://english.nv.ua/>.
3. Center for Strategic and International Studies (2025, May 28). The Russia-Ukraine drone war: Innovation on the frontlines and beyond. <https://www.csis.org/>.
4. Carlstedt, A., & Lyth, M. (2025, March 25). Usage, effectiveness and recent trends of FPV-drones in the Russian invasion of Ukraine based on published combat footage (FOI Memo 8897). Swedish Defence Research Agency (FOI). <https://www.foi.se/>.
5. Joint Air Power Competence Centre (2021). A comprehensive approach to countering unmanned aircraft systems. <https://www.japcc.org/>.
6. Chairman of the Joint Chiefs of Staff (2025, January 24). CJCSM 3320.01D: Joint electromagnetic spectrum operations. Joint Staff. <https://www.jcs.mil/>.
7. Department of the Air Force (2023). Air Force Doctrine Publication 3-85: Electromagnetic spectrum operations. <https://www.doctrine.af.mil/>.
8. U.S. General Services Administration, Office of the Chief Information Security Officer (2025, March 18). IT Security Procedural Guide: Drones/Unmanned Aircraft Systems (UAS) Security (CIO-IT Security-20-104, Rev. 2). <https://www.gsa.gov/>.
9. Ministry of Defence of Ukraine (2024, October 4). DELTA at NATO exercises: Ukraine shares unique counter-drone expertise. <https://mod.gov.ua/>.
10. DJI (2022). How DJI's AeroScope system protects the public interest. <https://enterprise-insights.dji.com/>.