

DOI <https://doi.org/10.32782/2956-333X/2025-3-7>

BEZPIECZEŃSTWO PILOTA DRONÓW W WARUNKACH ZAGROŻEŃ FPV NA DRÓGACH: MODEL PRZECIWDZIAŁANIA ORIENTOWANY NA RYZYKO

AERIAL SURVEILLANCE SAFETY IN THE CONTEXT OF AMBUSHED FPV THREATS ON MOTORWAYS: A RISK-BASED COUNTERMEASURE MODEL

Oleksandr Garasymyuk,

kandydat nauk technicznych, Lwowski Państwowy Uniwersytet Bezpieczeństwa Życia,

Lwów, Ukraina

orcid.org/0000-0001-9708-9862

Summary. The article is devoted to the study of aerial reconnaissance safety in conditions of ambush FPV threats on motorways, when strike UAVs wait for a long time on the roadside and strike targets as vehicles approach. It justifies a risk-based approach to convoy escort planning, shifting the focus from radio jamming to managing environmental vulnerabilities, reducing route predictability, and standardised SOPs. The scientific novelty lies in the integration of EMCON/OPSEC, engineering barriers, and close-range counter-FPV.

Key factors in the effectiveness of ambush FPVs have been identified: exploitation of electronic warfare dead zones in the ground layer, wired or low-emission control, motion sensors for energy conservation and rapid response, and spatial conditions that facilitate concealment of the carrier, cable, and operator position. The limitations of the ‘jamming anything’ paradigm and the advisability of focusing on preventive risk mapping, movement variability, and minimisation of electromagnetic emissions are demonstrated.

The structure of multi-layered countermeasures is investigated, combining organisational solutions (passage windows, time and speed profiling, checklists), engineering and sensor means (‘digital pickets’, roadside and cavity inspections, IR control from a suspension), and tactical escort algorithms with the allocation of close counter-FPV crews and a contour for detecting ambush operators with logistics damage. Effectiveness metrics are proposed for assessing route stability and SOP adaptation.

The application of a risk-oriented model in three environments – open plain, forest belt, urban development – is analysed, taking into account lines of sight, multi-beam and relief screening, which form ‘pockets’ of low electronic warfare effectiveness. The practical value of SOPs with the fixation of emission ‘windows’, attack vector breaking algorithms, and incident analysis is substantiated. The proposed approach reduces the risk of a successful UAV operation and increases the survivability of aerial reconnaissance and transport convoys.

Keywords: UAV, carrier configurations, swarm connections, electronic warfare, electromagnetic silence, camouflage, communication hygiene, operational security, counter-FPV, SOP, situational awareness.

1. Wprowadzenie

Współczesna ewolucja bojowego zastosowania FPV-UAV spowodowała pojawienie się taktyki zasadzki na drogach samochodowych, w ramach której platformy uderzeniowe w trybie uśpienia przez długi czas czekają na poboczach i aktywują się w momencie zbliżania się pojazdów, co znacznie zwiększa ryzyko dla kolumn logistycznych, ekip ewakuacyjnych i grup rozpoznania lotniczego. Kluczowym warunkiem powodzenia takich ataków jest połączenie sterowania przewodowego lub niskiej emisji z wykorzystaniem martwych stref walki radioelektronicznej w warstwie przyziemnej, gdzie skuteczność tłumienia spada z powodu ekranowania przez ukształtowanie terenu i ograniczeń geometrycznych linii widzenia anten, a także wykorzystanie czujników ruchu, co pozwala oszczędzać energię i skracać czas reakcji operatora. W tych warunkach tradycyjna paradygma zagłuszania jako uniwersalnej odpowiedzi okazuje się niewystarczająca, ponieważ nie eliminuje słabych punktów trasy, nie neutralizuje logistyki zasadzki i nie gwarantuje bezpieczeństwa rozpoznawcy lotniczego, który wykonuje rozpoznanie, planowanie i eskortę przejścia kolumn w dynamicznym środowisku o ograniczonej widoczności, fragmentarycznych strefach kontroli i wysokim nasyceniu przeszkód technicznych.

Problem komplikuje brak ujednoliconego modelu przeciwdziałania opartego na ryzyku, zdolnego do integracji rozwiązań organizacyjnych, zabezpieczeń inżynieryjno-sensorowych, dyscypliny emisji elektromagnetycznych i bezpieczeństwa operacyjnego, bliskiego konturu działań przeciwdziałających dronom oraz metrycznej kontroli skuteczności z uwzględnieniem typologii środowisk, sezonowych i dobowych

wahań, różnego poziomu ograniczeń zasobów i wymagań dotyczących współpracy z pokrewnymi jednostkami. Brak standardowych procedur planowania zmiennych tras ruchu, algorytmów wczesnego wykrywania oznak zasadzki, regulaminów tworzenia tymczasowych przeszkód w celu złamania wektora ataku oraz mechanizmów analizy po incydencie prowadzi do fragmentaryczności decyzji i utraty pamięci organizacyjnej. Naukowo uzasadnione tworzenie kompleksowych standardowych procedur operacyjnych i systemu wskaźników efektywności ma na celu zapewnienie systemowego zmniejszenia przewidywalności ruchu, terminowego wykrywania i niszczenia pozycji zasadzek, zwiększenia przeżywalności rozpoznawcy lotniczego oraz zarządzania ryzykiem na wszystkich etapach trasy w terenie otwartym, pasach leśnych i zabudowie miejskiej.

2. Analiza najnowszych badań i publikacji

Aktualny zbiór źródeł odnotowuje przejście przeciwnika do scenariuszy zasadzkowych z wykorzystaniem FPV na drogach samochodowych: „uśpione” urządzenia są rozmieszczane wzdłuż dróg i aktywowane podczas zbliżania się transportu, co potwierdzają dokumenty dotyczące działań bojowych ukraińskich oddziałów związanych z wykrywaniem i niszczeniem „dronów w zasadzce” na przydrożnych odcinkach. W publicznej analizie podkreśla się, że taka taktyka utrudnia przemieszczanie się w najbliższym tyłowym obszarze i zbliża się pod względem efektu do blokady powietrznej, wywierając stałą presję na logistykę. Dodatkowym wymiarem jest pojawienie się sterowanych przewodowo (światłowodowo) FPV, odpornych na REB i mniej zależnych od ukształtowania terenu i wielowiązkowości, co znacznie zmniejsza skuteczność klasycznego tłumienia. Do tego dochodzą dane z badań dotyczące wzrostu importu kluczowych komponentów do takich systemów, w szczególności światłowodów i akumulatorów, co napędza produkcję „niezakłócanych” platform i zwiększa ich zasięg zagrożenia.

Celem badania jest naukowe uzasadnienie i opracowanie modelu przeciwdziałania zagrożeniom FPV na drogach, który integruje rozwiązania organizacyjne, EMCON/OPSEC, środki inżynieryjno-sensorowe i bliski obwód przeciwdziałania FPV w standardowe SOP i system wskaźników efektywności w celu zwiększenia bezpieczeństwa rozpoznawcy lotniczego i stabilności tras.

3. Architektura zagrożenia i podstawy modelu przeciwdziałania

Podstawą proponowanego modelu jest doprecyzowana architektura zagrożenia, w której FPV-UAV są traktowane jako systemy kombinowane składające się z trzech elementów: niewidocznego nośnika, kanału sterowania i logistyki pozycji operatora. Nośnik funkcjonuje w dwóch trybach – pasywnego oczekiwania z minimalną emisją i aktywnego zbliżania się do celu; kanał sterowania może być przewodowy lub radiowy o niskiej emisji, co znacznie ogranicza możliwości klasycznego tłumienia; logistyka pozycji obejmuje schronienie dla operatora, kamuflaż kabla i punkty obserwacyjne. Kluczowymi warunkami fizycznymi powodzenia zasadzek są ekranowanie reliefowe, wielowiązkowość w warstwie przyziemnej, obecność wnęk i elementów konstrukcyjnych infrastruktury, które tworzą „kieszenie” o zmniejszonej skuteczności REB (Department of the Army, 2024). Parametry te tworzą przestrzenno-czasowe okno ataku, co zmusza do przeniesienia punktu ciężkości z czysto elektromagnetycznych oddziaływań na zarządzanie podatnością trasy i niszczenie logistyki zagrożenia.

Model przeciwdziałania oparty na ryzyku jest budowany poprzez cykl identyfikacji, analizy, oceny i przetwarzania ryzyka, a następnie monitorowania, gdzie każdy etap ma swoje własne narzędzia i artefakty dokumentacji. Identyfikacja obejmuje mapowanie „gorących punktów” na podstawie historii incydentów, cech topograficznych, przeglądów saperów i danych wywiadu technicznego; analiza opisuje scenariusze zagrożeń z uwzględnieniem typu kanału sterowania, dostępności schronów dla operatora, możliwości ukrytego ułożenia kabli i linii widoczności; ocena przekształca te scenariusze w ilościowe oceny prawdopodobieństwa i skutków dla różnych kategorii celów; przetwarzanie określa kombinację działań organizacyjnych, inżynieryjno-sensorycznych i taktycznych; monitorowanie zapewnia sprzężenie zwrotne poprzez metryki, dzienniki SOP i analizę po incydencie (Joint Chiefs of Staff, 2022). Taki schemat pozwala racjonalnie rozdzielać ograniczone zasoby na najbardziej wrażliwe węzły trasy.

Kontur organizacyjny modelu ma na celu zmniejszenie przewidywalności ruchu i dyscyplinę emisji. Planowanie marszów przewiduje dwie-trzy alternatywne trasy o różnej geometrii i oknach czasowych,

ograniczenia dotyczące powtarzania rozkładów, regulamin korzystania z kanałów satelitarnych i radiowych w krótkich sesjach, przeniesienie punktów rozmieszczenia środków łączności poza główny strumień techniki, a także uzgadnianie tylko krytycznie niezbędnych danych z sąsiednimi jednostkami. Dla rozpoznawcy lotniczego sporządza się listę kontrolną przygotowań przed marszem, która ujednolica sprawdzanie kanałów, kalibrację optyki, ustawianie trybów niskiej emisji, przygotowanie „cichych” kart łączności, tworzenie zestawu fraz sygnałowych i procedur natychmiastowej zmiany tempa ruchu (Department of the Navy, 2017). Standardy procedur operacyjnych eliminują zależność od indywidualnego doświadczenia i zapewniają powtarzalność decyzji w dynamicznych warunkach.

Obwód inżynieryjno-sensorowy ma na celu uczynienie drogi „chłodną” i poinformowaną. Na niebezpiecznych odcinkach rozmieszczane są „cyfrowe piktety” z tanich czujników optycznych i pasywnych czujników podczerwieni, rozmieszczonych na różnych wysokościach w celu wyeliminowania fałszywych alarmów; w węzłach infrastruktury okresowo przeprowadzane są przeglądy z zawieszenia quadkoptera w zakresie podczerwieni i widzialnym o różnych porach dnia; ustanawiane są punkty do szybkiego ustawiania zasłon dymnych i termicznych, jeśli geometria odcinka pozwala na złamanie wektora naprowadzania. Przenośne środki rozpoznania radiotechnicznego są wykorzystywane nie jako samodzielne środki wykrywania nośnika, ale jako wskaźnik wtórnych przejawów aktywności – towarzyszących kanałom, latarni, urządzeń pomocniczych operatora (International Organization for Standardization, 2018). Zaangażowanie grup saperów do skanowania wnęk, poboczy i kanałów przydrożnych zapewnia wykrywanie tras kablowych w scenariuszach przewodowych, co otwiera możliwości fizycznego przerwania sterowania.

Kontur taktyczny koncentruje się na bezpośrednim odparciu ataku i odparciu operatora. Formacja marszowa obejmuje główny pojazd o zmiennej prędkości ruchu w celu zniszczenia stabilnych trybów, pojazd zamykający wyposażony w środki bezpośredniego kontr-FPV, a także wyodrębnioną załogę rozpoznania lotniczego do dalszego rozpoznania z przodu i na flankach. Kluczowym elementem jest dopracowany algorytm ostatnich sekund: krótka zasłona dymna w celu zmniejszenia kontrastu, gwałtowny manewr z wyjściem na inny kontur, lokalne tłumienie w wąskim paśmie częstotliwości, zastosowanie przechwytyującego lub zniszczenia nośnika standardowym środkiem walki bezpośredniej w wcześniej określonym sektorze (NATO Allied Command Transformation, 2024). Równolegle tworzony jest kontur przeciwko operatorowi: wykrywanie nowych podejść do pozycji, śladów ukrycia, miejsc możliwego przeglądu, przechwytywanie kanałów pomocniczych i niszczenie punktu sterowania, ponieważ to właśnie logistyka zasadzki jest bardziej podatna na atak niż „cichy” nośnik.

Weryfikacja modelu odbywa się w trzech podstawowych środowiskach. Na otwartej równinie dominuje problem linii widzenia, dlatego manewry i rozwiązania dymne są bardziej skuteczne, a „cyfrowe pikiety” rozprzestrzeniają się na większe odległości z obowiązkowym powielaniem kierunków obserwacji. W pasach leśnych i na terenie pagórkowatym główne ryzyko stwarza ekranowanie reliefowe, które wymaga zwiększenia gęstości czujników, zwiększenia częstotliwości obserwacji z powietrza i bardziej agresywnej taktyki poszukiwania tras kablowych wzdłuż naturalnych osłon (Joint Air Power Competence Centre, 2024). W zabudowie miejskiej priorytetem są trasy z minimalną liczbą „kieszeni” i zamkniętych podwórek, ściśle regulowana jest prędkość i zabronione są postoje w strefach wielokrotnych odbić sygnałów; rozpoznawanie lotnicze działa krótkimi seriami z bezpiecznych pozycji dachowych, wykorzystując przeglądy w podczerwieni w przejściowych okresach doby, kiedy kontrast śladów cieplnych jest maksymalny.

Kontur metryczny zapewnia sterowalność i szkolenie organizacji. Do podstawowych wskaźników zalicza się odsetek udaremnionych ataków w stosunku do zarejestrowanych zdarzeń, średni czas wykrycia zagrożenia od momentu wejścia w „gorący” segment, częstotliwość rotacji wątków trasy, odsetek segmentów z aktywnymi „cyfrowymi pikietami” i dokumentacją przeglądów, czas trwania i częstotliwość „cichych” sesji łączności, czas rozłożenia zasłony dymnej/cieplnej, liczba wykrytych lub zneutralizowanych pozycji operatora na 100 km przejścia (Department of the Army, 1996/2002). Analiza po incydencie w odniesieniu do tych wskaźników pozwala skorygować SOP, wykryć nadmierne lub niewystarczające procedury, realokować zasoby i standaryzować skuteczne praktyki.

Wdrożenie modelu wymaga uzgodnienia komponentów kadrowych i szkoleniowych. Dla lotniczego zwiadowcy ustalane są scenariusze ról – planista ryzyka, operator rozpoznania, oficer SOP i analityk incydentów – wraz z odpowiednimi programami szkoleniowymi, obejmującymi analizę kartograficzną,

pracę z czujnikami podczerwieni, dyscyplinę EMCON/OPSEC oraz umiejętności bliskiego kontr-FPV. Obieg dokumentów jest przekształcany w standardowe formularze map ryzyka, listy kontrolne, dzienniki emisji i raporty po przejściu, które gromadzą pamięć organizacyjną i skracają czas adaptacji jednostki do nowych taktyk przeciwnika (Watling, J., & Reynolds, N., 2025). W rezultacie integracja rozwiązań organizacyjnych, inżynieryjno-sensorowych i taktycznych w ramach jednego cyklu zorientowanego na ryzyko zwiększa żywotność rozpoznawcy lotniczego i stabilność tras, przenosząc środowisko drogowe z kategorii trudno kontrolowanego zagrożenia do kategorii kontrolowanego ryzyka z mierzalną skutecznością przeciwdziałania.

4. Formalizacja modelu ryzyka i jednolite procedury EMCON/OPSEC

Rozszerzenie proponowanego modelu wymaga sformalizowania taksonomii zagrożeń i rozwiązań trasowych, które zapewniają spójność działań pododdziałów w różnych konfiguracjach przestrzennych i czasowych. FPV z zasadzką należy opisywać według cech kanału sterowania (przewodowy, kanał radiowy o niskiej emisji, opóźniona aktywacja z czujnikami ruchu), trybu oczekiwania (całkowicie pasywny lub z okresowymi krótkimi sesjami autodiagnostyki), typu nośnika (klasyczny FPV, przerobione platformy cywilne ze wzmocnionym podwoziem, miniaturowe modyfikacje „pełzające”) oraz logistyki pozycji operatora (stacjonarna, mobilna, rozproszona). Taka klasyfikacja pozwala jeszcze na etapie wstępnej analizy zbudować matrycę podatności trasy, gdzie każdemu odcinkowi drogi przypisuje się oczekiwany profil zagrożeń i listę preferowanych środków zaradczych (Bronk, J., 2025). Z praktycznego punktu widzenia oznacza to, że zamiast uniwersalnych, ale mało skutecznych „parasoli” REB stosuje się modułowe połączenie czujników, procedur i trybów ruchu, gdy na prostych odcinkach z otwartą linią widzenia nacisk kładzie się na manewr i degradację kontrastu celu przez dym, w pasach leśnych – na gęstsze „cyfrowe pikiety” i rozpoznanie kablowe, a w zabudowie miejskiej – na dokładną geometrię przejścia z minimalizacją „kieszeni” do zasadzki i utrzymaniem tempa.

Ważnym elementem jest stworzenie procesu zarządzania ryzykiem jako kontrolowanego obiegu dokumentów. Faza przedmarszowa tworzy „mapę ciepłą” zagrożeń na podstawie historii incydentów, inspekcji inżynieryjnej wrażliwych miejsc, danych z rozpoznania lotniczego i rozpoznania technicznego (Epstein, J., 2025). Dla każdego segmentu określa się prawdopodobieństwo pojawienia się zasadzki, stopień trudności jej ukrycia, przewidywany czas wykrycia oraz potencjalne skutki uderzenia dla konkretnego składu kolumny. Otrzymane oceny przekształcane są w reguły progowe: w segmentach wysokiego ryzyka ruch odbywa się wyłącznie z aktywowanym obwodem bliskiego kontr-FPV i rezerwową trasą odwrotu; w segmentach średniego ryzyka dopuszcza się skrócony zestaw procedur pod warunkiem zachowania „cichych” okien komunikacyjnych; w segmentach niskiego ryzyka utrzymuje się podstawowa dyscyplina emisji i routingu bez obniżania czujności. Taka stratyfikacja eliminuje pokusę przekształcania SOP w formalność i pozwala oszczędzać zasoby tam, gdzie dają one największy efekt graniczny.

Szczegółowe informacje EMCON/OPSEC przekładają ogólne hasła dotyczące „minimalizacji promieniowania” na konkretne procedury. Terminale satelitarne i stacje radiowe działają w krótkich, z góry określonych „oknach”, z antenami umieszczonymi w bezpiecznej odległości od głównego strumienia sprzętu, a dzienniki sesji są przechowywane lokalnie z opóźnioną transmisją, aby uniknąć demaskujących wzorców. Urządzenia mobilne załóg są przełączane w tryby uniemożliwiające sporadyczne połączenia w tle; interfejsy bliskiego zasięgu pozostają domyślnie wyłączone; lokalne punkty dostępu, jeśli są krytycznie potrzebne, są używane z minimalną mocą i tylko w ściśle regulowanych przedziałach czasowych. Marszowe „siatki cisy” są uzgadniane między pododdziałami, aby uniknąć nakładania się emisji, a każda nieplanowana transmisja podczas przejścia „gorącego” segmentu jest rejestrowana jako incydent z późniejszym rozpatrzeniem przyczyn (Ukrainian forces report ‘wired’ drones being used by Russia to evade jamming, 2025). Bezpieczeństwo operacyjne uzupełnia dyscyplina danych: ograniczenie szczegółowości tras w kanałach tekstowych, wykorzystanie map o obniżonej dokładności do wymiany taktycznej, ścisła rotacja haseł i kluczy do urządzeń terenowych.

Obwód inżynieryjno-sensorowy, oprócz środków optycznych i podczerwieni, należy racjonalnie wzmacniać prostymi, ale skutecznymi metodami wykrywania tras przewodowych i ukrytych pozycji. Okresowe „zimne” przejścia w małych grupach z magnetometrycznymi i indukcyjnymi wskaźnikami

pozwalają określić miejsca, w których kabel przecina elementy przydrożne; próby wibroakustyczne w godzinach porannych zmniejszają poziom szumów tła i zwiększają czułość na nietypowe źródła. Na trudnych odcinkach stosuje się pomiary pola cieplnego w przejściowych porach dnia, kiedy cienkie kable, rozgrzane w glebie lub na powierzchni, kontrastują z otoczeniem; rozpoznanie lotnicze stosuje niskie przeloty pod różnymi kątami widzenia w celu wykrycia deformacji trawy i drobnych cieni. W miarę gromadzenia danych tworzona jest biblioteka „drobnych anomalii” charakterystycznych dla konkretnych dróg, co skraca czas podejmowania decyzji i zmniejsza liczbę fałszywych alarmów.

5. Taktyka, szkolenie i instytucjonalizacja modelu

Kontur taktyczny ujawnia się poprzez scenariusze działań w ostatnich sekundach i poprzez strukturę prowadzenia trasy. Zasada zmiennej prędkości wyklucza ustalone rytmy, które ułatwiają namierzanie; mikromanewr w granicach pasa z okresowymi odchyleniami od idealnej trajektorii utrudnia korektę kursu drona; krótka zasłona dymna rozmywa kontrasty wizualne i utrudnia działanie prostych algorytmów widzenia komputerowego. Załoga bliskiego kontr-FPV działa nie jako „uniwersalny tarcza”, ale jako wyspecjalizowany przechwytyjący, aktywowany przy wejściu nośnika do wcześniej określonego sektora rażenia, przy czym sektor jest planowany z uwzględnieniem ukształtowania terenu, wiatru i typowych działań dronów. Równolegle toczy się walka z operatorem: rozpoznanie wykrywa świeże ślady zbliżania się do pozycji, miejsca możliwego obserwacji i ukrycia, rejestruje „logikę wygody” dla podłączenia kabla; w przypadku potwierdzenia oznak zasadzki grupa neutralizacyjna pozbawia przeciwnika kontroli lub niszczy punkt dowodzenia. Ważne jest, że taktyka ta nie sprowadza się do „pojedyńku platforma kontra platforma”, ale systematycznie niszczy łańcuch podejmowania decyzji przez przeciwnika.

Istotnym wzmocnieniem modelu są treningi symulacyjne i „czerwone komendy”, które odtwarzają sposób myślenia przeciwnika w konkretnych warunkach terenowych. Tworzenie cyfrowych makiet trasy z zaznaczeniem potencjalnych punktów zasadzek, linii widoczności, „kieszeni” o niskiej skuteczności REB i miejsc do ukrytego układania kabli zapewnia zupełnie nowy poziom przygotowania załóg. Rozpoznawca lotniczy otrzymuje możliwość wcześniejszego przetestowania „scenariusza ostatnich sekund”, obliczenia czasu ustawienia zasłony dymnej, wybrania miejsc do krótkiego rozłożenia się i zaplanowania, gdzie dokładnie należy spodziewać się próby wykorzystania przez przeciwnika ukształtowania terenu (Ling, J., 2024). Wyniki symulacji są rejestrowane w postaci map ryzyka, które podlegają regularnej aktualizacji na podstawie wyników rzeczywistych przejść i analiz po incydentach, dzięki czemu pamięć organizacyjna jednostki nie rozplywa się w rotacjach personelu.

Szczególny nacisk kładzie się na standaryzację komunikacji o niskiej emisji i kompatybilność jednostek. Krótkie frazy kodowe pozwalają przekazywać niezbędne informacje bez szczegółowego opisu; mapy o obniżonej dokładności na poziomie taktycznym zmniejszają ryzyko wycieków; ujednoliconą symboliką topograficzną i „linią decyzji” w SOP upraszczają interakcję na styku, gdzie zwykle pojawiają się błędy. Ważne jest, że dyscyplina emisji nie ogranicza się do techniki: trasy są uzgadniane w minimalnym niezbędnym zakresie, aby zapewnić dekonfliktowość operacji, a jednocześnie nie tworzyć demaskujących szablonów dla zewnętrznych obserwatorów.

W celu zwiększenia powtarzalności i kontroli jakości wprowadza się rozszerzony obwód metryczny. Oprócz odsetka udaremnionych ataków i średniego czasu wykrycia zagrożenia śledzone są wskaźniki „chłodu trasy” jako stosunek czasu „ciszy” do całkowitego czasu przejścia z uwzględnieniem planowanych okien, wskaźniki sprawności korytarza sensorycznego, częstotliwość odchyień od podstawowych SOP i ich wpływ na profil ryzyka, wyniki „czerwonych” ćwiczeń, podczas których zespoły przeciwnika próbują przełamać obronę trasy (Center for Strategic and International Studies, 2025). Analizy po incydentach mają ujednoliconą strukturę, co zmusza do analizowania nie tylko działań taktycznych załóg, ale także błędów planistycznych, ograniczeń logistycznych i niedociągnięć EMCON/OPSEC. Gromadzenie i analiza tych wskaźników w dynamice tworzy podstawy do kontrolowanych korekt SOP, zmian konfiguracji czujników i redystrybucji zasobów.

Czynnik ludzki i przygotowanie personelu są kluczowymi elementami przetrwania. Dla obserwatora lotniczego określa się role – planista ryzyka, operator rozpoznania, analityk incydentów i oficer SOP – wraz z jasnym wykazem kompetencji, obejmujących analitykę kartograficzną, pracę w zakresie

podczerwieni, dyscyplinę emisji, umiejętności bliskiego kontr-FPV i algorytmy działania w ostatnich sekundach ataku. Moduły szkoleniowe są skonstruowane w taki sposób, aby każda kompetencja była testowana w warunkach zbliżonych do rzeczywistych, a wyniki były zapisywane w indywidualnych profilach rozwoju. Stwarza to podstawę do obiektywnego zarządzania szkoleniem i szybkiego wprowadzania nowych członków jednostki do standardowych procedur.

Wreszcie, integracja modelu w szerszym kontekście zabezpieczania tras wymaga zrównoważenia rozwiązań technicznych i organizacyjnych z ograniczeniami zasobów. Nie każdy oddział ma dostęp do drogich czujników lub pełnoprawnych środków przechwytywania, jednak właśnie podejście oparte na ryzyku pozwala skierować ograniczone zasoby tam, gdzie w największym stopniu zmniejszają one prawdopodobieństwo udanego działania drona lub minimalizują skutki. W tym sensie model nie jest zbiorem rozproszonych „funkcji”, ale spójnym systemem, który przekształca teatr działań drogowych z trudnej do kontrolowania strefy zagrożenia w środowisko o przewidywalnych ryzykach, zrozumiałych granicach odpowiedzialności i mierzalnych wynikach dla bezpieczeństwa lotniczego zwiadowcy i stabilności operacji logistycznych.

Aby przekształcić ogólne podejścia w praktykę, warto sformalizować model oceny ryzyka, który odzwierciedla specyfikę zasadzek FPV w warstwie przyziemnej. Całkowite ryzyko trafienia na danym odcinku trasy warto traktować jako iloczyn prawdopodobieństwa realizacji zagrożenia i oczekiwanych szkód dla określonej kategorii celów, gdzie prawdopodobieństwo rozkłada się na czynniki widoczności i dostępności celu, przestrzennej przydatności terenu do ukrycia nośnika i logistyki operatora, widoczności elektromagnetycznej, powtarzalności czasowych i kinematycznych wzorców ruchu, a także wcześniejszej historii incydentów. Taka dekompozycja pozwala na parametryzację środowiska: na otwartych terenach kluczowe znaczenie ma kontrola linii widoczności i degradacja kontrastu optycznego, w pasach leśnych – diagnostyka kryjówek i przebiegających tras kablowych, w miastach – minimalizacja „kieszeni” i stref, w których możliwe jest umieszczenie operatora z uprzywilejowaną obserwacją. Ważne jest, że ocena nie jest przeprowadzana jednorazowo, ale w cyklicznym obiegu z ciągłym doprecyzowywaniem współczynników wagowych na podstawie analizy po incydencie i przejazdów szkoleniowych, dzięki czemu model dostosowuje się do konkretnego teatru działań, lokalnej topografii i kultury taktycznej jednostki.

Kluczowym elementem praktycznej realizacji staje się synchronizacja sensoryczno-rozpoznawcza „na czele kolumny – na flankach – na końcu”, która tworzy korytarz informacyjny i wykrywa oznaki zasadzki przed wejściem w „okno ataku”. Przedni element rozpoznania lotniczego działa krótkimi seriami, zaznaczając podejrzane punkty z uwzględnieniem anomalii termicznych, geometrycznych i teksturalnych, grupy flankujące sprawdzają pobocza i zagłębienia, koncentrując się na miejscach dogodnych do ukrytego poprowadzenia kabla, element zamykający utrzymuje „czystość” pola informacyjnego i gotowość do bliskiego przechwycenia. Aby zmniejszyć liczbę fałszywych alarmów, czujniki „pikietowe” są budowane na zasadzie wielokanałowej korelacji: słaby sygnał termiczny nabiera znaczenia tylko w przypadku obecności odpowiednich cech geometrycznych i śladów logistyki, a pojedyncze wykrycie na kamerze o niskiej rozdzielczości jest potwierdzane alternatywnym kątem widzenia lub przejściem IR w godzinach przejściowych, kiedy kontrast środowiska jest maksymalny. Takie podejście przenosi wykrywanie z kategorii intuicyjnej „sztuki” do zdyscyplinowanej procedury o przewidywalnej dokładności.

Dalszy rozwój modelu wymaga wprowadzenia kontrolowanych „fałszywych” scenariuszy, które zmuszają przeciwnika do ujawnienia zasadzek poza pożądanym dla niego przedziałem czasowym. Zastosowanie niewielkich rozmiarów pułapek termicznych i świetlnych o kontrolowanym profilu promieniowania, zdalne wypuszczanie mało widocznych technicznych „sond” przed głównym sprzętem, tworzenie krótkotrwałych elektromagnetycznych „błysków” w bezpiecznych punktach trasy pozwala wywołać przedwczesną aktywację „leżących” FPV lub uruchomienie ich czujników ruchu, po czym rozpoznanie lotnicze rejestruje reakcję środowiska i lokalizuje miejsca potencjalnego umiejscowienia operatora. Ważnym warunkiem skuteczności oszustwa jest jego nieregularność i niepowtarzalność, aby przynęty same nie stały się nowym szablonem, który przeciwnik będzie mógł wykorzystać do kontrplanowania.

Osobnego omówienia wymaga profil kinematyczny ruchu jako narzędzie przełamania naprowadzania w ostatnich sekundach ataku. Zasada zmiennej prędkości i mikromanewru w granicach pasa tworzy nieliniowy wektor, co utrudnia korektę kursu dla operatora lub prostych algorytmów widzenia komputerowego

po stronie nośnika; krótka zasłona dymna w momencie wejścia nośnika do wcześniej określonego sektora „końcowego” kontaktu zmniejsza kontrast optyczny i pozwala zyskać krytyczne ułamki sekundy na przechwycenie lub zniszczenie; lokalne tłumienie w wąskim paśmie częstotliwości, zsynchronizowane z dymem i manewrem, obniża jakość sprzężenia zwrotnego i zwiększa prawdopodobieństwo chybień. Wszystko to należy przełożyć na scenariusze szkoleniowe, w których załogi doprowadzają sekwencje „dym – manewr – lokalne tłumienie – przechwycenie” do automatyzmu i opanowują normy czasowe odpowiadające rzeczywistej bezwładności pojazdów i aerodynamice typowych nośników przeciwnika.

Dyscyplina emisji i bezpieczeństwo operacyjne nie są kształtowane „odgórnie”, ale poprzez rutynowy obieg dokumentów w dziale. Dzienniki „okien ciszy”, mapy ryzyka i listy kontrolne przygotowań mają ujednoliconą strukturę, która pozwala na szybkie przenoszenie najlepszych praktyk między zmianami i pokrewnymi działami. Dla każdego „gorącego” segmentu rejestruje się dozwolone i zabronione typy transmisji, miejsca umieszczenia anten, maksymalny czas trwania sesji i punkty awaryjnego opuszczenia. Analiza po incydencie jest sporządzana według szablonu, który zmusza do analizy nie tylko działań taktycznych załóg, ale także decyzji planistycznych, ograniczeń logistycznych, odchyłeń od EMCON/OPSEC oraz skuteczności konfiguracji czujników (Kallenborn, Z., 2022); na podstawie jego wyników automatycznie aktualizowane są współczynniki wagowe modelu ryzyka i lista procedur zapobiegawczych dla podobnych segmentów.

Znaczne oszczędności zasobów zapewnia priorytetowe traktowanie obecności czujników „według ryzyka” w połączeniu z niskokosztowymi metodami rozpoznania. Na obszarach o wysokim prawdopodobieństwie scenariuszy przewodowych preferowane są częstsze oglądziny wizualne i podczerwone pobo- czy i wnek oraz stosowanie prostych wskaźników indukcyjnych w godzinach porannych; na otwartych prostych odcinkach – rozproszonym punktom obserwacyjnym z alternatywnymi kątami widzenia i kontrolowanymi zasłonami dymnymi; w środowisku miejskim – starannie zaplanowanym trasom z wyłączeniem podwórek-„kieszeni” i regularnym przejazdem „próbników”, które sprawdzają reakcję środowiska bez zbędnego ujawniania kolumn. Takie „stratyfikowane” rozmieszczenie pozwala utrzymać wystarczającą gęstość kontroli w krytycznych węzłach, nie rozpraszać środków na segmenty o niskim efekcie granicznym.

W kontekście walki nie tylko z nośnikiem, ale także z operatorem ważne jest modelowanie „logiki wygody” przeciwnika. Mapa potencjalnych pozycji dowodzenia jest tworzona z uwzględnieniem wymagań dotyczących widoczności drogi, osłony przed obserwatorami, możliwości bezgłośnego doprowadzenia kabla oraz obecności naturalnych lub sztucznych ekranów; rozpoznanie lotnicze oznacza prawdopodobne punkty obserwacyjne, rejestruje świeże ślady podejścia, oznaki niedawnej aktywności i „ślady” cieplne sprzętu. Po zlokalizowaniu obszaru dowodzenia włącza się obwód neutralizacji: przerywanie kabla, tłumienie kanałów pomocniczych i bezpośrednie uderzenie w pozycję, co często okazuje się skuteczniejsze niż długotrwała walka z „milczącym” nośnikiem w warstwie przyziemnej.

Praktyczna powtarzalność decyzji jest zapewniona dzięki symulacyjnym szkoleniom i pracy „czerwonych drużyn”, które w imieniu przeciwnika planują zasadzki na konkretnych trasach jednostki. Cyfrowe makiety z naniesionymi liniami widoczności, „kieszeniami” niskiej skuteczności REB, obszarami możliwego ułożenia kabli i ukrytymi podstępami pozwalają testować warianty przejścia, sprawdzać skuteczność rozwiązań dymnych i manewrowych, kalibrować progi wyzwalania czujników i precyzować normy czasowe „ostatniej sekundy”. Regularne porównywanie wyników symulacji z rzeczywistymi danymi dotyczącymi przejść i incydentów wypełnia lukę między „laboratoryjnymi” założeniami a praktyką terenową.

Wreszcie, aby zinstytucjonalizować model, potrzebne są ramy edukacyjne i kadrowe, w ramach których funkcje rozpoznawcy lotniczego zostaną sformalizowane jako wzajemnie uzupełniające się role: planista ryzyka, operator rozpoznania, oficer SOP i analityk incydentów. Każda rola ma ustrukturyzowaną listę kompetencji i zadań kontrolnych: od analizy topograficznej i przeglądów IR do dyscypliny emisji i bliskiego kontr-FPV. Takie podejście zapewnia ciągłość wiedzy, szybką adaptację nowych specjalistów, minimalizuje zależność od poszczególnych „gwiazdorskich” operatorów i zwiększa żywotność organizacyjną jednostki. W rezultacie model zorientowany na ryzyko, wspierany przez synchronizację sensoryczną, kontrolowane scenariusze oszukiwacze, znormalizowany obieg dokumentów, szkolenia symulacyjne i ramy kadrowe, przenosi ochronę tras z płaszczyzny reaktywnej obrony do stanu proaktywnego

zarządzania, gdzie „okna ataku” zawężają się, a obserwator lotniczy otrzymuje niezbędny zapas czasu na bezpieczne podejmowanie decyzji.

6. Wnioski

Zaproponowana w badaniu model przeciwdziałania zagrożeniom FPV na drogach samochodowych, oparty na ryzyku, pokazuje, że zwiększenie bezpieczeństwa rozpoznania powietrznego osiąga się nie tyle poprzez zwiększenie mocy tłumienia radioelektronicznego, ile poprzez zarządzanie słabościami trasy i logistyką przeciwnika. Fizyka warstwy przyziemnej, wielowiązkowość i ekranowanie reliefowe tworzą stabilne strefy niskiej skuteczności tradycyjnej elektronicznej walki, co rekompensuje przejście na kompleksową architekturę ochrony, w której bezpieczeństwo operacyjne i dyscyplina emisji tworzą podstawową warstwę przetrwania, a nasycenie sensoryczne i bliski kontur działań przeciwdronowych zapewniają terminowe wykrywanie i udaremnianie ataku w końcowym oknie.

Praktyczna implementacja modelu wymaga standaryzacji planowania marszów o zmiennej geometrii i oknach czasowych, wyniesienia i maskowania anten, regulacji krótkich sesji łączności, rozmieszczenia cyfrowych pikiet na niebezpiecznych segmentach, rutynizacji inspekcji saperskich i podczerwieni, a także gotowości załóg do skoordynowanej sekwencji dym, manewr, lokalne tłumienie, przechwycenie. Krytycznym elementem staje się kontur przeciwdziałania operatorowi, który kieruje wysiłki na wykrywanie i niszczenie punktów sterowania i tras kablowych, pozbawiając przeciwnika głównej przewagi w trybach niskiej emisji.

Bibliografia

1. Department of the Army (2024, December 13). ATP 3-01.81: Counter-Unmanned Aircraft System Techniques. Headquarters, Department of the Army.
2. Joint Chiefs of Staff (2022). JP 3-13.3, Operations Security. Joint Staff. https://irp.fas.org/doddir/dod/jp3_13_3.pdf.
3. Department of the Navy (2017). NTP 3-13.3M(A), Navy Operations Security. Navy Warfare Development Command. <https://irp.fas.org/doddir/navy/ntp3-13-3.pdf>.
4. International Organization for Standardization (2018). ISO 31000:2018 Risk management – Guidelines. <https://www.iso.org/standard/65694.html>.
5. NATO Allied Command Transformation (2024, October 16). Countering Class I UAS – A Handbook (Fact Sheet). <https://www.act.nato.int/article/countering-class-i-uas-handbook/>.
6. Joint Air Power Competence Centre (2024, June 28). A Comprehensive Approach to Countering Unmanned Aircraft Systems (C-UAS) (Book). <https://www.japcc.org/cuas/>.
7. Department of the Army (1996/2002). FM 3-50: Smoke Operations (incl. Change pages). U.S. Army. <https://www.bits.de/NRANEU/others/amd-us-archive/fm3-50%2890%29.pdf>.
8. Watling, J., & Reynolds, N. (2025, February). Tactical Developments During the Third Year of the Russo–Ukrainian War. Royal United Services Institute. <https://static.rusi.org/tactical-developments-third-year-russo-ukrainian-war-february-2205.pdf>.
9. Bronk, J. (2025, August 4). NATO Should Not Replace Traditional Firepower with “Drones”. Royal United Services Institute. <https://www.rusi.org/explore-our-research/publications/rusi-defence-systems/nato-should-not-replace-traditional-firepower-drones>.
10. Epstein, J. (2025, September 16). Ukraine’s front-line road nets are catching Russian drones, but gaps leave vehicles exposed to ambush. Business Insider. <https://www.businessinsider.com/ukraine-anti-drone-road-nets-effective-russian-pilots-finding-holes-2025-9>.
11. Ukrainian forces report ‘wired’ drones being used by Russia to evade jamming (2025, August 8). The Guardian. <https://www.theguardian.com/world/2025/aug/08/ukraine-russia-wired-drones-evade-jamming>.
12. Ling, J. (2024, December 23). The invisible Russia–Ukraine battlefield. WIRED. <https://www.wired.com/story/electronic-warfare-russia-ukraine/>.
13. Center for Strategic and International Studies (2025, May 28). The Russia-Ukraine Drone War: Innovation on the Frontlines and Beyond (Event transcript). <https://www.csis.org/analysis/russia-ukraine-drone-war-innovation-frontlines-and-beyond>.
14. Kallenborn, Z. (2022, July 26). How to Counter Drone Swarms (Issue Brief No. 5315). The Heritage Foundation. <https://www.heritage.org/defense/report/how-counter-drone-swarms>.