2025

Zagrożenia związane z użyciem dronów DJI

FUNDACA ZELAZNY
TOMASZ DARMOLINSKI

SPIS TREŚCI

WOJSKOWE SYSTEMY RADIOELEKTRONICZNE DO WYKRYWANIA DRONÓW DJI

SHIPOVNIK-AERO (ШИПОВНИК-АЭРО)

Rosyjski mobilny system walki elektronicznej opracowany przez instytut „Etalon”. Jego zadaniem jest monitorowanie widma radiowego i automatyczne wykrywanie sygnałów używanych do zdalnego sterowania dronami. Działa w bardzo szerokim zakresie częstotliwości (25 MHz–2500 MHz), obejmując pasma wykorzystywane przez łączność DJI (2,4 GHz i 5,8 GHz). System potrafi przechwycić i analizować wykryte transmisje, a następnie je zakłócić lub nawet przejąć kontrolę nad dronem. Zainstalowany jest na ciężarówce KAMAZ i ma zasięg działania rzędu ok. 10 km. Shipovnik-Aero był obserwowany przez OBWE na wschodzie Ukrainy już w 2016 r. i ponownie w 2021 r., co potwierdza jego użycie w warunkach bojowych. Dzięki pasywnemu nasłuchowi potrafi namierzyć zarówno drona, jak i źródło emisji (kontroler/operator). Po identyfikacji sygnału może prowadzić triangulację i kierunkowe zakłócanie w stronę operatora. System uchodzi za trudny do wykrycia i potrafi nawet generować fałszywe sygnały, by zmylić przeciwnika.

REPELLENT-1

Ciężki rosyjski kompleks antydronowy opracowany przez Naukowo-Techniczne Centrum Walki Radioelektronicznej. Zestaw na podwoziu MAZ/KAMAZ (ponad 20 ton) wykrywa i zakłóca pracę UAV. Charakteryzuje się bardzo dużym zasięgiem detekcji — potrafi pasywnie wykrywać sygnały sterowania małych dronów (np. DJI) z dystansu ponad 35 km. W praktyce używa czułych anten do nasłuchu pasm 2,4/5,8 GHz, co pozwala namierzyć zarówno drona, jak i operatora. Zasięg neutralizacji (zakłócania) jest mniejszy — skuteczne zagłuszanie do ok. 2,5 km. Oznacza to, że Repellent-1 wykrywa cel dużo wcześniej, niż jest w stanie go unieszkodliwić, dając czas na reakcję. System został odnotowany na Donbasie (raport OBWE z lipca 2018 r.). Używano go także podczas obecnej inwazji; był m.in. przechwycony przez siły Azerbejdżanu w Górskim Karabachu w 2020 r., co wskazuje na eksport. Kabina jest osłonięta przed ostrzałem i skażeniami NBC.

SILOK-01 (СИЛОК-01)

Nowszy rosyjski system przeciwdronowy średniego zasięgu, zaliczany do środków WRE szczebla frontowego. Automatycznie wykrywa i zagłusza łącza dron–operator w pasmach 2,4 i 5,8 GHz (typowych dla DJI). Według dostępnych danych pojedynczy Silok może jednocześnie obsłużyć do 10 celów i tworzy „bańkę” ochronną o promieniu ok. 4 km. W obronie statycznej używa się go na trójnogu, istnieje też wersja mobilna. Siloki rozlokowywano gęsto wzdłuż linii frontu (co ~10 km, ok. 7 km za frontem), by zagłuszać kanały RC i GPS używane przez ukraińskie drony rozpoznawcze oraz amunicję krążącą. Utrudniło to operacje UAV i przyczyniło się do dużych strat dronów, choć skuteczność Siloka okazała się ograniczona — ukraińscy operatorzy zaczęli używać innych częstotliwości i trybów autonomicznych. Część systemów zniszczono po przeniknięciu dronów przez ich „bańkę”. Analitycy oceniali, że Silok cierpi na niewystarczającą czułość i moc, co ogranicza jego realną skuteczność.

R-330Ż „ŻYTIEL”

Zestaw zakłóceń radiowych starszej generacji, używany przez Rosję już od wojny w Donbasie. Jego podstawowa funkcja to zagłuszanie GPS/GSM na szerokim obszarze, co unieruchamia wiele dronów polegających na nawigacji satelitarnej lub sieci komórkowej. System ma też stację radio-rozpoznawczą do wykrywania źródeł emisji w pasmach VHF/UHF. W praktyce może służyć do wykrywania aktywności dronów (telemetria, kontrola), choć mniej precyzyjnie niż Silok. Według analiz Rosjanie łączą Żytiele z Silokami i Shipovnikiem, tworząc warstwową obronę WRE przeciw dronom.

INNE SYSTEMY

Rosja pozyskuje i rozwija także inne technologie do wykrywania UAV. W 2023 r., mimo sankcji, instytut MIREA zakupił kanadyjski system SkyEye firmy Skycope Technologies — przenośny radar (~10 kg) zdolny wykryć drona z odległości do 35 km w terenie otwartym (ok. 10 km w mieście). Jednocześnie śledzi do 14 celów i ma bazę wzorców dla ponad 330 modeli (AI rozpoznaje także nieznane typy). Radar wykrywa statek powietrzny, nie lokalizuje bezpośrednio operatora, ale zwiększa świadomość sytuacyjną (np. ostrzega przed nadlatującymi Mavicami, nawet nisko i cicho). Stosowane są też improwizowane czujniki akustyczne — skuteczne głównie na większe, głośne UAV (np. Shahed-136), mniej na ciche quadcoptery DJI.

WYKRYWANIE SYGNAŁÓW DJI AEROSCOPE I IDENTYFIKATORÓW RADIOWYCH

DJI AEROSCOPE

Specjalny system producenta do wykrywania dronów DJI przez służby. Drony DJI (od 2017 r.) emitują sygnał DroneID (Remote ID) zawierający m.in. pozycję drona, wysokość, prędkość, numer identyfikacyjny, a także pozycję pilota (jeśli kontroler ma GPS) i punkt startu (home point). Sygnał nadawany jest w kanale łączności drona (np. OcuSync) i bywa odbierany przez stacje AeroScope nawet do ok. 50 km (w zależności od anten). Odbiornik dekoduje dane w czasie rzeczywistym i pokazuje model, położenie i trajektorię drona oraz lokalizację operatora.

W realiach wojny AeroScope zyskał inne znaczenie. Rosja pozyskała i wykorzystuje stacje AeroScope do namierzania ukraińskich dronów; pojawiały się twierdzenia o „rozszerzonych" wersjach o większym zasięgu. Według ukraińskich źródeł Rosjanie dysponowali stacjonarnymi AeroScope'ami z Syrii (zasięg do 40 km). Dzięki temu mogli lokalizować załogi dronów DJI, a następnie kierować w ich pozycję ogień. W marcu 2022 r. wicepremier Ukrainy Mychajło Fedorow alarmował, że AeroScope służy Rosji do zabijania ukraińskich operatorów, i apelował do DJI o blokadę. DJI początkowo tłumaczyło problemy techniczne po stronie ukraińskiej, a następnie ogłosiło wstrzymanie sprzedaży sprzętu w Rosji i na Ukrainie oraz wyłączenie wsparcia dla AeroScope w tych rejonach. Mimo to Rosjanie korzystali z posiadanych urządzeń; według dystrybutora DJI na Ukrainie kilku operatorów zostało namierzonych i zabitych z powodu emisji DroneID.

Co ważne, DJI twierdziło początkowo, że DroneID/AeroScope są szyfrowane. Okazało się jednak, że transmisja nie jest szyfrowana i może być przechwycona także przez osoby postronne.

ANALIZA SDR I TRIANGULACJA

Dzięki SDR społeczność zbudowała otwarte odbiorniki DroneID. Już w 2022 r. pojawiły się projekty dekodujące DroneID DJI. Rosyjskojęzyczni programiści opublikowali skrypt JeepDoors, który pozwala wyłączyć nadawanie DroneID lub wstawić dane fałszywe. Naukowcy zaprezentowali oprogramowanie do odbioru DroneID przy użyciu tanich SDR-ów. W praktyce Rosjanie mogą stworzyć improwizowane „mini-AeroScope". Triangulacja takich emisji jest możliwa przy użyciu co najmniej dwóch odbiorników; w polu działa też prosta metoda „foxhuntingu" z anteną kierunkową. Nawet jeśli operator wyłączy DroneID, sam sygnał kontrolera (np. 2,4 GHz) może zdradzić jego pozycję.

PRZYKŁADY UŻYCIA NA UKRAINIE

W pierwszych miesiącach wojny zdarzało się, że operatorzy ukraińskich DJI byli wykrywani i atakowani niemal natychmiast po starcie — wskazywało to na użycie AeroScope lub podobnych środków. Ukraińcy wdrożyli środki zaradcze: w maju 2022 r. opublikowano open-source'owe narzędzie do „maskowania" przed AeroScope (JeepDoors). Wprowadzono też zalecenia taktyczne: wyłączać GPS w urządzeniu mobilnym podłączonym do kontrolera, startować dronem z innego miejsca niż pozycja operatora i nie wracać bezpośrednio w punkt startu. Na masową skalę modyfikowano też oprogramowanie DJI — po obu stronach.

Po stronie rosyjskiej powstała inicjatywa „Russian Hackers for the Front", która przygotowała firmware „1001" dla DJI Mavic 3 i pokrewnych. Modyfikacja usuwa ograniczenia producenta (wyłącza DroneID, omija geofencing i strefy No-Fly, pozwala latać bez sygnału GPS, znosi limity wysokości i zasięgu). Instalację prowadzono w sieci kilkuset punktów serwisowych na terytorium Rosji i obszarach okupowanych, by kontrolować dystrybucję. Według deklaracji liczba zaktualizowanych dronów liczona jest w dziesiątkach, a nawet setkach tysięcy (dane mogą być zawyżone). Po wgraniu „1001" powrót do oryginalnego firmware'u jest utrudniony, co zabezpiecza drona przed zdalnym „wyłączeniem" lub cofnięciem zmian.

ZAGROŻENIA ZWIĄZANE Z UŻYCIEM DRONÓW DJI MATRICE 350 RTK PRZEZ STRAŻ GRANICZNĄ

WPROWADZENIE

DJI Matrice 350 RTK (M350 RTK) to zaawansowana platforma stosowana m.in. do obserwacji granic, poszukiwań i nadzoru infrastruktury. Atuty: długi czas lotu (do 55 min), odporność IP55 (pył/deszcz), nowoczesne sensory (np. termowizja). Jednocześnie użycie sprzętu DJI niesie istotne ryzyka — cyber, operacyjne i logistyczne.

RYZYKA CYBERBEZPIECZEŃSTWA I TRANSMISJI DANYCH

1) Przechwycenie i wyciek danych

Dron generuje duże ilości danych (wideo, zdjęcia, GPS), które domyślnie mogą synchronizować się z chmurą DJI przy użyciu aplikacji sterującej. Nowa maszyna wymaga konta DJI i okresowego połączenia z internetem (aktualizacje NFZ/firmware), w przeciwnym razie nakładane są ograniczenia działania. To budzi obawy, że wrażliwe dane SG (nagrania z granicy, trasy patroli) trafią poza własną infrastruktūrę. Eksperci zwracają uwagę, że bez dogłębnej analizy sprzętowej nie ma pewności, czy urządzenie nie przesyła obrazu lub innych krytycznych danych na zewnątrz.

2) Ingerencja w oprogramowanie (firmware)

M350 RTK ma mechanizmy bezpiecznego rozruchu i podpisu cyfrowego (aktualizacje podpisywane kluczem, akceptowane tylko autoryzowane obrazy), co utrudnia nieuprawnione modyfikacje. Mimo to luki się zdarzają: ujawniano podatności m.in. w protokole Wi-Fi QuickTransfer (M300/M30), pozwalające na nieuprawniony dostęp do zdjęć/wideo lub ataki DoS. Producent wydawał poprawki, ale to pokazuje, że trzeba stale reagować na nowe zagrożenia. Zdarzały się też przypadki nagłego rozszerzania stref zakazu lotów po stronie jednego użytkownika, gdy po drugiej identyczny model działał normalnie — formalnych dowodów na celowe działania nie przedstawiono, ale zależność od baz danych i geofencingu może w praktyce zadziałać przeciw użytkownikowi.

3) Łączność z serwerami producenta

Siedziba w Chinach rodzi pytania o bezpieczeństwo komunikacji dron/kontroler ↔ infrastruktura dostawcy. Pojawiały się oskarżenia i ograniczenia w niektórych krajach, ale są też audyty wskazujące na możliwość pracy w trybie całkowicie offline (Local Data Mode) bez ruchu wychodzącego. Niezależnie od deklaracji producenta służby powinny opierać się na własnej weryfikacji.

MOŻLIWOŚĆ LOKALIZACJI OPERATORA PRZEZ OSOBY TRZECIE

Najpoważniejsze ryzyko: drony DJI ujawniają pozycję operatora. System DroneID/AeroScope nadaje pakiety z pozycją drona i kontrolera; transmisja nie jest szyfrowana i może być przechwycona przez posiadaczy odpowiednich odbiorników. W warunkach wojny Rosjanie wykorzystywali AeroScope do namierzania operatorów i kierowania ognia. Istnieją narzędzia pozwalające wyłączyć lub maskować Remote ID, ale producent usiłuje je blokować aktualizacjami. Dostępne są też otwarte narzędzia do budowy własnych odbiorników DroneID (SDR) lub imitowania sygnałów Remote ID. Wniosek: nie tylko służby, także przestępcy mogą namierzyć operatora M350 RTK, jeśli dron działa „fabrycznie”. Potwierdzono, że DroneID nadaje dokładne współrzędne pilota w czasie rzeczywistym i transmisja nie jest szyfrowana — operator nie powinien zakładać anonimowości w terenie.

SCENARIUSZE PRZEJĘCIA KONTROLI NAD DRONEM

Jamming (zagłuszanie)

Najczęstszy atak to zagłuszanie łączy sterowania (2,4/5,8 GHz) lub GNSS. Skutki: utrata łączności, RTH, lądowanie awaryjne, a w skrajnym wypadku rozbicie. Szacunki z frontu wskazują, że znaczna część utraconych dronów pada ofiarą zakłócania, czasem także „własnego". M350 RTK ma algorytmy anty-zakłóceniowe i cztery anteny, ale przy silnym WRE to nie zawsze wystarcza.

Spoofing GPS

Fałszywy sygnał GNSS może oszukać autopilota i zmienić trasę lub wymusić lądowanie w wybranym miejscu. Cywilne GNSS oznacza podatność. Objawy: krążenie po okręgu, „ucieczka", lądowanie w złym punkcie. W rejonach przygranicznych dobrze przygotowane grupy mogą zastosować spoofing.

Przejęcie łącza radiowego (kontroli)

M350 RTK korzysta z szyfrowania AES-256 (OcuSync 3.0) z kluczem sesji, co utrudnia podsłuch i wstrzyknięcie komend. W praktyce częstsze są inne wektory: ataki na usługi pomocnicze (QuickTransfer/Enhanced Wi-Fi), infekcja tabletu sterującego, a przede wszystkim wymuszony RTH/lądowanie przez jamming. W efekcie dron bywa fizycznie przejmowany na ziemi — z perspektywy operatora to również „utrata kontroli".

OGRANICZENIA TECHNICZNE M350 RTK W DZIAŁANIACH STRAŻY GRANICZNEJ

Warunki terenowe i pogodowe

Mimo IP55 i zakresu pracy od -20°C do +50°C, w gęstym lesie czy górach zasięg łączności spada. Wymagana jest możliwie bezpośrednia LOS; większa wysokość zwiększa ryzyko wykrycia. Silny wiatr i opady ograniczają stabilność; zimą problemem jest oblodzenie, latem — przegrzewanie. Dron nie zawsze zastąpi patrol pieszy.

Silne zakłócenia elektromagnetyczne

W pobliżu silnych emiterów (radary, nadajniki) kompas/GNSS mogą się mylić, dron przechodzi w tryby ograniczone (ATTI). Redundancja czujników pomaga w środowisku zurbanizowanym, ale w skrajnych warunkach możliwe są resety i anomalie. Doświetlacze IR/reflektory oraz sygnatura akustyczno-świetlna zdradzają obecność. M350 RTK to duży, słyszalny quadcopter.

LOGISTYKA I EKSPLOATACJA

TB65 są „hot-swap", ale jedna para to zwykle ok. 45–50 min lotu z ładunkiem; potrzebne są liczne zestawy i stacje ładujące. Masa zestawu i akcesoria wymuszają użycie pojazdu. Czas rozłożenia/kalibracji to kolejne minuty — w nagłych interwencjach często lepsze są mniejsze platformy.

Geofencing i ograniczenia przestrzeni

System GEO może blokować loty bez wcześniejszego odblokowania, co przy lotniskach czy strefach zakazanych może opóźnić akcję. Wersje „Government" ograniczają te bariery, ale w konfiguracji standardowej trzeba pamiętać o zależności od internetu do odblokowań.

ZALEŻNOŚĆ OD INFRASTRUKTURY DJI (CHMURA, AKTUALIZACJE, REMOTE ID)

Aktualizacje firmware i bazy

Brak aktualizacji to ryzyko pozostawienia znanych luk; aktualizacja — ryzyko niepożądanych zmian (np. twardszy Remote ID). Aktualizacje zwykle wymagają łączności z serwerem producenta; możliwe są tryby offline, ale to dodatkowa logistyka. W razie eskalacji konfliktu wsparcie i części mogą być ograniczone.

Chmura i usługi online

FlightHub 2 ma wariant on-prem, ale użycie chmury producenta to ryzyko nieautoryzowanego dostępu. W służbach bezpieczniej przechowywać i przetwarzać dane wyłącznie on-prem. W przeszłości wykazywano podatności kont i usług.

AeroScope/Remote ID w ekosystemie

Funkcję Remote ID trudno oficjalnie wyłączyć (często wymóg prawny). Służby muszą liczyć się z emisją wrażliwych danych o pozycji, chyba że użyją modyfikacji nieoficjalnych. Zmiany regulacyjne trzeba śledzić, by zachować zgodność z prawem.

Kompatybilność i zamknięty ekosystem

DJI używa własnych standardów transmisji, akcesoriów i baterii. Utrzymanie M350 RTK wymaga oryginalnych komponentów (TB65, BS65, Zenmuse H20/H30 itd.). Sankcje lub przerwy w dostawach mogą wstrzymać serwis. Dane na kartach/pamięci są szyfrowane (AES-256-XTS z kluczem użytkownika), więc odzysk bez klucza w razie awarii bywa trudny.