*Radosław BIELAWSKI*
*Akademia Sztuki Wojennej*[1]
*Wydział Bezpieczeństwa Narodowego*
*Instytut Podstaw Bezpieczeństwa*
*r.bielawski@akademia.mil.pl*
*ORCID0000-0002-5701-4476*
*https://doi.org/10.34739/dsd.2019.02.12*

# BEZPIECZEŃSTWO BEZZAŁOGOWYCH SYSTEMÓW POWIETRZNYCH W ŚRODOWISKU ZAKŁÓCEŃ

**ABSTRAKT:** Przedmiotem badań tego opracowania są zakłócenia jako forma niekinetycznej walki z bezzałogowymi systemami powietrznymi. Celem praktycznym artykułu jest uporządkowanie teoretycznej wiedzy i terminologii dotyczącej zakłóceń, celem poznawczym natomiast jest wykazanie, że zakłócenia stanowią realny i nowy problemem, dotyczący bezpieczeństwa użytkowania bezzałogowych systemów powietrznych. W pracy użyto teoretycznych metod badawczych, takich jak: analiza, synteza, abstrahowanie i uogólnienie. Rezultatem badań jest określenie rodzajów zakłóceń (głównie *jamming* oraz *spoofing*) oraz ich charakterystyki w stosunku do bezzałogowych aparatów latających. Dokonano uporządkowania wiedzy teoretycznej, wyjaśniając techniki zakłóceń, wskazując na cele ataków oraz obiekty ich oddziaływania. W pracy dokonano analizy możliwości dostępnych, niekinetycznych systemów neutralizacji BSP wraz z ich możliwościami oraz charakterystyką taktyczno-techniczną. Przewidując dalszy rozwój bezzałogowych systemów powietrznych wskazano na problem bezpieczeństwa w kontekście autonomizacji tych systemów. Drugim ważnym wnioskiem jest brak norm prawnych regulujących używanie urządzeń do zakłócania. Stwarza to realny problem, pozwalając na ich użytkowanie np. w stosunku do urządzeń satelitarnych systemów nawigacyjnych, stosowanych powszechnie w lotnictwie.

**SŁOWA KLUCZOWE:** bezpieczeństwo, bezzałogowe statki powietrzne, zakłócenia

# SAFETY OF THE UNMANNED AIRCRAFT SYSTEMS IN A HARSH INTERFERENCE ENVIRONMENT

**ABSTRACT:** This study considers signal interference as a form of non-kinetic warfare against unmanned aircraft systems (UAS). The practical purpose of this paper is to organize the theoretical knowledge and terminology concerning interference, while its cognitive purpose is to demonstrate that this recently recognized problem is a real threat to the safe use of unmanned aircraft systems. The research methods employed in this work – analysis, synthesis, abstracting and generalization – serve to determine the types of interference (i.e. primarily *jamming* and spoofing) and their characteristics in relation to unmanned aircraft. The paper organizes

[1] War Studies Academy; Poland.

the theoretical knowledge by explaining the signal interference techniques and indicating the targets of attacks or objects of interest. Therefore, available non-kinetic energy UAS neutralization systems are analyzed with respect to their capabilities, tactical characteristics and technical specifications. Given the anticipated further development of unmanned aircraft systems technologies, signal interference carries serious implications for the safety of autonomous operation of these systems. The second important conclusion highlighted in this analysis is the absence of a legislative framework that would regulate the use of interference facilities. This gap in legal regulations implicitly permits their engagement against such crucial infrastructure as e.g. satellite devices for navigation systems – standard and critical equipment in the aviation.

**KEYWORDS:** safety, unmanned aircraft system – UAS, interference

## WSTĘP

Jednym z niekinetycznych[2] sposobów walki z bezzałogowymi systemami powietrznymi są zakłócenia. Można rozumieć je jako zewnętrzne sygnały powodujące naruszenie porządku lub równowagi – w tym przypadku urządzenia radio- i nawigacyjnych. Z uwagi na ich charakter można podzielić je na niezamierzone (ang. *unintentional interferences*)[3], czyli inne urządzenia emitujące fale, np. nadajniki radiowe, oraz zakłócenia zamierzone (ang. *intentional interferences*)[4] – będące przedmiotem badań tego opracowania.

Chcąc zobrazować wpływ zakłóceń na bezpieczeństwo ruchu lotniczego można posłużyć się przykładem ataku na system nawigacyjny, który miał miejsce w lipcu 2019 r. w przestrzeni powietrznej głównego, izraelskiego lotniska – Ben Guriona, położonego w pobliżu Tel Awiwu. Prawdopodobnie źródłem tego zakłócenia są rosyjskie działania wojskowe w sąsiedniej Syrii. Sytuacja ta wywołała zaniepokojenie Międzynarodowej Federacji Stowarzyszeń Pilotów Linii Lotniczych (ang. *The International Federation of Air Line Pilots' Associations* – IFALPA) z uwagi na to, że podczas wykonywania operacji startu i lądowania w strefie izraelskiego portu lotniczego kilku pilotów straciło łączność z sygnałem systemu GPS. Taka sytuacja ma decydujący wpływ na bezpieczeństwo ruchu lotniczego.

Celem praktycznym artykułu jest uporządkowanie teoretycznej wiedzy dotyczącej zakłóceń, celem poznawczym natomiast jest wykazanie, że zakłócenia są realnym i nowym problemem dotyczącym bezpieczeństwa użytkowania bezzałogowych systemów powietrznych zarówno w zastosowaniach cywilnych, jak i wojskowych.

## METODY I TECHNIKI ZAKŁÓCAJĄCE BEZZAŁOGOWE SYSTEMY POWIETRZNE – PRÓBA UPORZĄDKOWANIA TERMINOLOGII

W literaturze przedmiotu możemy wyróżnić dwie podstawowe techniki (sposoby) zamierzonego zakłócania urządzeń radioelektronicznych, w tym tych zaimplementowanych na

[2] Rozumianymi jako działania/ oddziaływania bez udziału energii kinetycznej.
[3] N.G. Ferrara i in., *A new implementation of narrowband interference detection, characterization, and mitigation technique for a software-defined multi-GNSS receiver*, „GPS Solutions" t. 22 nr 4 (2018).
[4] F. Bazzano i in., *Mental Workload Assessment for UAV Traffic Control Using Consumer-Grade BCI Equipment*, 2017.

pokładach bezzałogowych statków powietrznych. Należą do nich *jamming*[5] oraz *spoofing*[6]. Niektóre opracowania rozróżniają także technikę *meaconingu*[7]. Opracowania traktujące o zakłóceniach systemów radioelektronicznych zawierają także akronim – MIJI, pochodzący od kompilacji anglojęzycznych słów: *Meaconing*, *Intrusion*, *Jamming* i *Interference*[8].

Najpopularniejszym terminem stosowanym w odniesieniu do zakłóceń jest *jamming* (zagłuszanie). Można rozumieć go jako emitowanie fal elektromagnetycznych w kierunku odbiornika sygnału (np. nawigacyjnego) w celu przerwania jego dostępności. Kolejna definicja opisuje *jamming* jako świadomy akt transmisji, generowanie sygnału w tym samym paśmie co prawidłowy sygnał[9] skierowany w kierunku urządzenia (np. odbiornika GPS).

Następnym, zamierzonym sposobem celowego zakłócania jest *spoofing* (fałszowanie sygnału i podszywanie się pod niego). W odniesieniu do przedmiotu badań w tym artykule wiąże się on z transmisją, wydawałoby się, legalnego sygnału, który jednak jest sygnałem fałszywym. Definicja *spoofingu* traktuje go jako atak polegający na podszywaniu się pod inny element systemu. Etymologia tego słowa pochodzi od anglojęzycznego *spoof* tłumaczonego jako naciąganie, szachrajstwo. Inna literaturowa definicja przedstawia *spoofing* jako „transmisję fałszywych sygnałów systemu nawigacji satelitarnej, która ma na celu doprowadzenie do wyznaczenia, przez odbiornik tych sygnałów, nieprawidłowych informacji o jego położeniu, prędkości i aktualnym czasie”[10].

*Spoofing* jest rodzajem elektronicznego ataku, którego działanie polega na emisji fałszywych sygnałów nawigacyjnych (np. GSP), imitujących prawdziwe sygnały docierające do użytkownika z satelitów tego systemu. Jego celem jest dostarczenie użytkownikowi nieprawidłowych informacji dotyczących pozycjonowania, prędkości i czasu, niezbędnych do prowadzenia statku powietrznego.

W literaturze przedmiotu wyróżnia się dwie techniki prób „oszukania” odbiornika: fałszowanie sygnału, który odbierany jest przez odbiornik jako rzeczywisty i na jego podstawie wyznaczana jest błędna pozycja (np. w systemie GPS), oraz drugi, którego działanie polega na przesyłaniu informacji, że prawidłowy sygnał jest rzekomo fałszywy, co powoduje, iż odbiornik interpretuje rzeczywisty sygnał jako błędny[11].

---

[5] Vide: J.C. Price, J.S. Forrest, *Commercial Aviation Airport Security* [w:] *Practical Aviation Security*, Elsevier 2013; R. Sabatini, T. Moore, S. Ramasamy, *Global navigation satellite systems performance analysis and augmentation strategies in aviation*, „Progress in Aerospace Sciences” t. 95 (2017); M.G. Stewart, J. Mueller, *Evaluating Aviation Security* [w:] *Are We Safe Enough?*, Elsevier 2018.

[6] Vide: G. Buesnel, *Threats to satellite navigation systems*, „Network Security” t. 2015 nr 3 (2015); J. Magiera, R. Katulski, *Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing*, „Journal of Applied Research and Technology” t. 13 nr 1 (2015); M. Riahi Manesh, N. Kaabouch, *Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions*, „Computers & Security” t. 85 (2019).

[7] R.F. Graf, *M* [w:] *Modern Dictionary of Electronics*, Elsevier 1999; D. Marnach i in., *Detecting Meaconing Attacks by Analysing the Clock Bias of Gnss Receivers*, „Artificial Satellites” t. 48 nr 2 (2013); R. Sabatini, T. Moore, S. Ramasamy, *Global navigation satellite systems performance analysis and augmentation strategies in aviation*...

[8] G. Loukas, *Cyber-Physical Attack Steps* [w:] *Cyber-Physical Attacks*, Elsevier 2015.

[9] M. Figurski i in., *Wpływ zakłóceń na pomiary GPS. GPS kontra zagłuszanie*, „Geodeta” t. 1 nr 188 (2011), s. 47.

[10] J. Magiera, *Analiza i badania systemu antyspoofingowego GPS* [w:] Politechnika Gdańska 2015, s. 1.

[11] M. Figurski i in., *Wpływ zakłóceń na pomiary GPS. GPS kontra zagłuszanie*..., s. 47.

Innym sposobem zamierzonego zakłócenia sygnału jest *meaconing* polegający na zakłócaniu i ponownym nadawaniu sygnału lub zakłócaniu i opóźnieniu nadawania sygnału na tej samej częstotliwości[12]. *Meaconing* można zdefiniować następująco – jest to zakłócenie i wyciszenie odbieranych sygnałów radiowych powiązane z opóźnionym nadawaniem obcych sygnałów nawigacyjnych, przekazywanych w celu zmylenia wrogiego nawigatora. Wynikiem takich działań jest niedokładne lub nieadekwatne określenie położenia. Efektem stosowania techniki *meaconingu* jest zwabienie obcego statku powietrznego, lądowanie w innym niż planowane miejscu, zboczenie z kierunku, użycie uzbrojenia w innym niż planowano miejscu (np. zrzucenie klasycznych bomb). Zgodnie ze słownikiem terminów NATO[13] *meaconing* interpretuje się jako mylenie nawigacyjne i definiuje w sposób następujący: *meaconing* to system otrzymywania sygnałów z radiolatarni i powtórne ich przesyłanie na tej samej częstotliwości w celu zakłócenia nawigacji. Stacje zakłócające powodują, że statki powietrzne oraz stacje naziemne uzyskują niedokładny namiar.

Zintegrowaną techniką zamierzonego zakłócania jest MIJI. W nomenklaturze wojskowej termin ten (akronim) opisywany jest już od 1986 roku. Jeden z dokumentów traktujących o tego typu zdarzeniach[14] określa znaczenie zawartych w akronimie terminów oraz sposób postępowania w przypadku ich wystąpienia lub podejrzenia o możliwościach ich zastosowania. Zgodnie z jego treścią za *meaconing* uważa się taki rodzaj zakłóceń, który dotyczy wysyłanych i retransmitowanych sygnałów do radiolatarni (ang. *radio beacon*) o tej samej częstotliwości w celu zmylenia systemów radionawigacji. Urządzenia wywołujące zjawisko *meaconingu* powodują niepoprawne dane na temat przemieszczenia się statku powietrznego. Za intruzje, czyli wtargnięcie (ang. *Intrusion*) uważa się działanie, którego wynikiem jest zamierzone oddziaływanie energią elektromagnetyczną na jedną ze ścieżek transmisyjnych, a w efekcie nieprawidłowy i nieautoryzowany (nieupoważniony) odczyt transmisji radiowej (nieprawidłowe instrukcje) przez kontrolera ruchu lotniczego lub pilota. Za *jamming* uważa się tutaj celowe działanie polegające na wysyłaniu promieniowania lub odbiciu promieniowania w taki sposób, aby zakłócić działanie urządzeń elektronicznych, elementów wyposażenia lub systemów nieprzyjaciela. Przykładem może być nadawanie szumu blokującego odbiór informacji nadawanej na danej częstotliwości. Za interferencję (ang. *Interference*) przyjmuje się każdą aktywność elektromagnetyczną powodującą zakłócenia lub ograniczenia efektywnego działania urządzeń elektrycznych lub elektronicznych. Ten rodzaj zakłóceń może być wywołany celowo, jak w niektórych formach wojny radioelektronicznej, lub nieumyślnie – w wyniku fałszywych emisji i reakcji na skutek intermodulacji[15], itp. Za przykład takiego działania można podać przerwę w transmisji wojskowej wywołaną przez cywilną transmisję radiową.

[12] Ibidem.
[13] NATO Standardization Agency (NSA), *AAP-6. Słownik terminów i definicji NATO*, 2005, s. 224.
[14] *Operations Reporting Meaconing, Intrusion, Jamming and Interference of Electromagnetic Systems, RCS: JCS-1066(MIN)*, 1986.
[15] Intermodulacja – to zakłócenia spowodowane przenikaniem pojedynczych kanałów, co skutkuje ich zajętością. Charakteryzuje się ona pojawianiem się na wyjściu toru transmisyjnego nowych składowych (częstotliwości)

Zintegrowana technika MIJI stosowana jest najczęściej w ramach walki radioelektronicznej.

W celu uporządkowania terminologii wyżej określone metody zakłóceń zamierzonych, skierowanych w stosunku do bezzałogowych statków powietrznych oraz ich anglojęzyczne tłumaczenia i znaczenia zestawiono w tabeli poniżej (Tabela 2).

| Metoda zakłócenia | Polskojęzyczne znaczenie | Cel oddziaływania/ataku | Obiekt oddziaływania/ataku |
|---|---|---|---|
| ***jamming*** | Zagłuszanie | przerwanie dostępności sygnału | odbiornik satelitarnego systemu nawigacji satelitarnej GPS |
| ***spoofing*** | fałszowanie i podszywanie | przekazanie nieprawidłowych informacji o parametrach statku powietrznego – współrzędnych geograficznych (położenie SP), prędkości i aktualnym czasie | systemy nawigacji satelitarnej – w szczególności komponent naziemny systemu |
| ***meaconing**** | zakłócenie i opóźnienie | przekazanie niepoprawnych i opóźnionych sygnałów – niepoprawny namiar | radiolatarnia |
| **MIJI** | wysyłanie retransmitowanych sygnałów, intruzja, zakłócenie i interferencja | zmylenia systemów radionawigacji poprzez błędne przekazywanie sygnałów, nieprawidłowy i nieautoryzowany odczyt transmisji radiowej przez kontrolera ruchu lotniczego/pilota, wysyłanie promieniowania elektromagnetycznego w celu zakłócania urządzeń elektronicznych | radiolatarnia<br><br>systemy nawigacji i radionawigacji<br><br>urządzenia elektryczne i elektroniczne |

* w nomenklaturze NATO określa się *meaconing* jako – **mylenie nawigacyjne**

**Tabela 2.** Metody zakłóceń zamierzonych, skierowanych w stosunku do bezzałogowych statków powietrznych
Źródło: opracowanie własne.

## CHARAKTERYSTYKA I MOŻLIWOŚCI URZĄDZEŃ ZAKŁÓCAJĄCYCH, STOSOWANYCH PRZECIWKO BEZZAŁOGOWYM SYSTEMOM POWIETRZNYM

### JAMMERY

Bazując na powyższej typologii na potrzeby tego (i nie tylko) opracowania, urządzenia do zamierzonych zakłóceń, których celem jest zagłuszanie, nazwać możemy jammerami lub zagłuszaczami.

Sposób działania jammera polega na tym, iż wysyła on sygnał interferencyjny[16] w paśmie wykorzystywanym przez urządzenia zaimplementowane na pokładzie bezzałogowego statku powietrznego (np. sygnału z systemu nawigacji satelitarnej). W efekcie sygnał satelitarny będzie nadal wykrywalny, ale wysyłany sygnał użyteczny zostanie „przykryty" przez moc sygnału wysłanego z jammera. Najprostszą i najczęściej stosowaną metodą przez tego typu urządzenia jest emisja w kierunku odbiornika GPS fali elektromagnetycznej na częstotliwości nośnej wynoszącej

będących kombinacją składowych zawartych w sygnale wejściowym oraz ich harmonicznych; R. Strużak, J. Sobolewski, *Wirtualna zajętość widma w sieciach radia kognitywnego – algorytmy oceny*, „Telekomunikacja i Techniki Infomacyjne" t. 1–2 (2014), s. 34.

[16] Sygnał interferencyjny polega na nakładaniu się dwóch lub więcej fal powodujących wzmocnienie lub natężenie fali wypadkowej.

1575,42 MHz. Dzięki temu sygnał może mieć charakter: ciągły z niezmienną częstotliwością, impulsowy z niezmienną częstotliwością lub impulsowy ze zmienną częstotliwością[17]. Sygnał nawigacyjny docierający do odbiornika użytkownika jest stosunkowo słaby (np. w systemie GPS poziom mocy sygnału wynosi około 160 dBW, co stanowi 10÷16W), a w konsekwencji czyni go podatnym na zakłócenia. Zważywszy na fakt łatwości dokonania zakłóceń urządzeniami typu jammer należy także podkreślić, że pomimo iż celem zagłuszenia jest przerwanie dostępności sygnału docierającego do odbiornika, to zakłócenia mogą spowodować również jego fizyczne uszkodzenie.

Niektóre opracowania dostępne w literaturze przedmiotu zawierają typologię jammerów. Dzieli się je na dwie grupy – jammery podstawowe oraz zaawansowane. Do jammerów podstawowych należą zagłuszacze aktywne i proaktywne. Jammery aktywne wysyłają sygnały zakłócające niezależnie od tego, czy istnieje komunikacja zakłócającego obiektu czy nie, aktywne natomiast pracują wówczas, gdy emitowana jest aktywność obiektu na określonym kanale. W tym celu posiadają one moduły odpowiadające za wykrywanie aktywności sieci. Zagłuszacze zaawansowane natomiast dzielimy na dwie grupy: funkcjonalne (ang. *Function-Specific*) oraz hybrydowe (ang. *Smart-Hybrid*). Zagłuszacze funkcjonalne wyposażone są we wstępnie ustalone funkcje oraz mogą pracować, wykorzystując pojedynczy kanał w celu oszczędności energii oraz maksymalizacji przepustowości. Charakterystyczną cechą jammerów hybrydowych jest energooszczędność połączona z dużą skutecznością działania. Ponadto mogą one pracować zarówno w trybie aktywnym, jak i proaktywnym [18].

Analizując zagłuszacze należy podkreślić fakt, że w ostatnim czasie – z uwagi na niską cenę – popularne stały się urządzenia komercyjne, nazywane także urządzeniami ochrony osobistej lub ochrony prywatności (ang. *Personal or Privacy Protection Devices* – PPDs). Są to niewielkiej masy (do ok. 1 kg) oraz rozmiarów jammery, których zasięg wynosić może do ok. 10 m emitując moc sygnału do wartości ok. 1,5÷2,5W. W zależności od lokalizacji pionowej tych urządzeń charakteryzują się one następującymi, przykładowymi możliwościami: na wysokości 3 m, 30 m i 100 m zasięgi odpowiednio do wysokości – 20 km, 50 km oraz 100 km[19]. Takie parametry, ogólna dostępność oraz niska cena (ok. 30 Euro), pomimo barier prawnych zakazujących użytkowania, spowodowały ich dużą popularność. Jednakże ich wykorzystywanie jest niebezpieczne, szczególnie dla żeglugi powietrznej statków powietrznych, w tym bezzałogowych aparatów latających. Zakłócenie sygnału nadawanego przez infrastrukturę techniczną pomocy radionawigacyjnych lub lotniczych globalnych systemów nawigacji satelitarnej może spowodować zniekształcenie integralności tych systemów, a w efekcie doprowadzić do wygenerowania zafałszowanej informacji na temat położenia statków

[17] P. Kowaleczko, J. Sulkowski, *Podatność systemu nawigacji satelitarnej GPS na zakłócenia i wynikające z niej zagrożenia dla transportu*, „Logistyka" t. 3 (2012), s. 1117.
[18] K. Grover, A. Lim, Q. Yang, *Jamming and anti-jamming techniques in wireless networks: a survey*, „International Journal of Ad Hoc and Ubiquitous Computing" t. 17 nr 4 (2014), ss. 199–201.
[19] Z. Trzaskowski, *Bezpieczeństwo globalnych systemów nawigacji satelitarnej a możliwości ich zakłócenia – jamming* [w:] *Bezpieczeństwo w środowisku lotniczym i kosmicznym*, Warszawa 2018, s. 166.

powietrznych. Uniemożliwi to nawigację na trasie przelotu lub podejście do lądowania. Prawie wszystkie dostępne w handlu jammery przesyłają sygnały świergotowe (ang. *chirp signals*), czyli ciągły sygnał falowy (ang. *Continuous Wave* – CW), z nieustannie zmieniającą się częstotliwością w czasie trwania impulsu. Ich przepustowość często dotyczy również wojskowej częstotliwości GPS. Skutki ich użytkowania nie są łatwe do złagodzenia, a w przypadku zakłóceń impulsowych sygnał interferencji może zostać całkowicie wygaszony. Jammery CW można skutecznie zneutralizować, stosując filtr wycinający. Nie ma jednak praktycznego podejścia do przetwarzania sygnału świergotowego[20].

Badania nad problematyką jammerów, w kontekście zagłuszania przez nie systemów GPS prowadzi między innymi National Physical Laboratory w Wielkiej Brytanii. Koordynowany tutaj projekt o nazwie SENTINEL[21] zakładał zamontowanie 20 urządzeń na terenie kraju, których celem było wykrywanie incydentów zakłócenia sygnału satelitarnego. W wyniku badań od września 2011 roku do lutego 2012 (6 miesięcy) jeden z czujników odnotował ponad 60 takich epizodów[22]. Taki stan rzeczy zmusił do powołania specjalnego oddziału – GPS Jammer LOCATION System (JLOC) Master Station. System ten przy wykorzystaniu czujników i różnych schematów raportowania zbiera informacje o możliwych zakłóceniach i zgłuszeniach sygnału, analizuje wpływ tych danych na odmowę nawigacji oraz centralizuje zagłuszanie. W tym samym czasie użytkownik systemu może generować raporty, statystyki niezbędne do planowania misji (np. bojowych), które są zależne od działania systemu GPS. Zważywszy na prawidłowe działanie odbiorników GPS przeznaczonych do celów wojskowych, tworzone są specjalne sygnały, które nie są dostępne dla cywilnych użytkowników oraz są dużo bardziej odporne na zakłócenia typu *jamming*.

## SPOOFERY

Zgodnie z wcześniej określoną definicją fałszowanie i podszywanie mające na celu przekazanie nieprawidłowych informacji o parametrach statku powietrznego – współrzędnych geograficznych (położenie SP), prędkości i aktualnym czasie – skierowane przeciwko systemom nawigacji satelitarnej nazywamy *spoofingiem*. Zatem urządzenia do tego typu zamierzonych zakłóceń nazwać możemy spooferami.

Zważywszy na to, że celem ataków są systemy GPS, to skuteczność podszywania się zależna jest od mocy sygnałów satelitarnych. Zatem, aby atak *spoofingowy* był skuteczny, moc fałszywych sygnałów na wejściu odbiornika musi być znacznie większa od normalnych sygnałów satelitarnych. Dlatego też sygnały nadawane w trakcie ataku z jednej strony zagłuszają sygnały pożądane, z drugiej zaś stanowią nośnik nieprawidłowych danych dla

[20] A. Rügamer, D. Kowalewski, *Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!*[w:] *FIG Working Week - From the Wisdom of the Ages to the Challenges of the Modern World, 2015*, Sofia 2015, s. 4.
[21] T. Kattenborn i in., *UAV data as alternative to field sampling to map woody invasive species based on combined Sentinel-1 and Sentinel-2 data*, „Remote Sensing of Environment" t. 227 (2019).
[22] *Jamming GPS*, https://www.dlp-expert.pl/blog/id,194/geoforum.pl/upload/review/file/188_s46_51_z.pdf.(06.06.2019)

odbiornika, który znajduje się w zasięgu spoofera. Możliwość wytworzenia sygnałów imitujących odbieranie z satelitów jest spowodowana ogólnodostępnością informacji, które dotyczą sygnałów cywilnych. Dodatkowo dane nawigacyjne nie podlegają szyfrowaniu, co istotnie ułatwia sfałszowanie sygnałów[23].

Spoofer może występować w postaci naziemnej albo w formie przystosowanej do przemieszczania się w celu ataku – znajduje się na pokładzie statku powietrznego (również bezzałogowego), statku morskiego lub pojazdu naziemnego. Dodatkowo z uwagi na budowę elementu nadającego rozróżnia się trzy klasy tego typu urządzeń:

1. komercyjny symulator konstelacji satelitów – urządzenia tego rodzaju są wykorzystywane w laboratoriach testowych odbiorników sygnału w celu zapewnienia stabilności i powtarzalności warunków badawczych. Tego typu urządzenie posiada zaimplementowany wzmacniacz mocy oraz antenę nadawczą rozlokowaną na wyjściu generatora. Taka budowa pozwala na transmisje sygnałów o ściśle zdefiniowanej postaci do urządzeń odbierających sygnał w promieniu do kilku kilometrów. Pierwszym, podstawowym problemem wynikającym z chęci posiadania tego typu urządzenia jest jego cena – ok. 100 tys. PLN. Jednakże istnieją sposoby na zbudowanie komercyjnego symulatora konstelacji, posiadającego uproszczony generator – zbudowanego w technice radia definiowanego programowo SDR (ang. *software-defined radio*). Wspomniana technika polega na tym, że działanie podstawowych elementów elektronicznych (np. mieszaczy, modulatorów) jest wykonywane za pomocą programu komputerowego[24]. Takie rozwiązanie zdecydowanie obniża koszt generatora, czyniąc urządzenie zagłuszające tańszym. Drugim, technicznym, problemem użytkowania jest brak możliwości zachowania pożądanej ilości czasu pomiędzy wysyłanymi fałszywymi, a prawdziwymi sygnałami. Szczególne znaczenie tego parametru występuje podczas fazy śledzenia przy dostrojeniu odbiornika do wysyłania prawdziwych sygnałów z satelity. Aby zwiększyć jego możliwości w fazie śledzenia, należy spełnić warunek zapewnienia zgodności częstotliwości i fazy fali nośnej, fazy ciągu pseudolosowego oraz taktu danych nawigacyjnych pomiędzy sygnałami z satelitów oraz sygnału spoofera w punkcie odbioru sygnału;
2. połączenie odbiornika i generatora fałszywych sygnałów– zasadą działania spoofera jest to, że odbiornik w fazie początkowej dostraja się do prawdziwych sygnałów wysyłanych przez satelity. W ten sposób pozyskuje on dane o pozycji geograficznej, czasie oraz efemerydach – danych dotyczących przebiegu orbity satelitów systemu GPS oraz odchyleń od niej. W kolejnym etapie zadaniem generatora jest wytworzenie i przesłanie fałszywych sygnałów o wartości mocy i opóźnieniu dobranymi w taki sposób, aby mogły one odpowiadać parametrom satelitów, śledzonych w pierwszej

[23] J. Magiera, R. Katulski, *Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing*..., s. 1.
[24] L. Chen i in., *Embedding and re-embedding of virtual links in software-defined multi-radio multi-channel multi-hop wireless networks*, „Computer Communications" (2019).

fazie. Aby przeprowadzić atak *spoofingowy* z użyciem urządzenia łączącego odbiornik i generator fałszywych sygnałów, należy znać dokładną odległość pomiędzy zakłócanym odbiornikiem, a spooferem. Dzięki precyzyjnej znajomości tej odległości możliwe jest zachowanie zgodności faz fal nośnych, co pozwala również na właściwe działanie urządzenia. Wykrycie aktywności tego urządzenia przez stronę przeciwną osiągalne jest poprzez analizę kierunku nadejścia sygnału (ang. *Direction-of-Arrival* – DOA)[25], z uwagi na to, że – w odróżnieniu od sygnałów odbieranych z satelitów – wszystkie fałszywe sygnały odbierane są z jednego kierunku;

3. urządzenia o charakterze teoretycznym – zasada działania tego typu urządzenia polega na nadawaniu sygnałów przez wiele anten, które są rozmieszczone wokół zakłócanego odbiornika, co z kolei odtwarza separację przestrzenną satelitów. Każdy z nadawanych sygnałów jest odpowiednio opóźniany względem aktualnego położenia odbiornika. Urządzenia o charakterze teoretycznym są niewykrywalne przez metodę analizy kierunku przysyłanych sygnałów i w praktycznym zastosowaniu ich możliwości wykorzystania są wysoce nieprawdopodobne.

Jednym ze światowych ośrodków prowadzących badania naukowe dotyczące możliwości *spoofingu* jako skutecznej metody zakłóceń jest Texas University w Stanach Zjednoczonych. W ramach prowadzonych analiz wykonano testy, których celem było przejęcie bezzałogowego statku powietrznego, korzystającego z nawigacji GPS. Podczas badań użyto spoofera drugiej klasy, który odbierał opóźnienia fałszywych sygnałów w oparciu o znajomość prawdziwej pozycji bezzałogowej platformy. Zadaniem zaimplementowanych urządzeń GPS na pokładzie bezzałogowego statku powietrznego, korzystającego z autopilota było utrzymanie swojej pozycji. W rezultacie poprzez *spoofing* doprowadzono do przemieszczenia się prowadzonego bezzałogowego aparatu latającego w płaszczyźnie pionowej (zmiana wysokości). Co więcej, w tym przypadku *spoofing* spowodował zmiany wysokości zakłócanej platformy bezzałogowej, mimo że bazował on głównie na wysokościomierzu ciśnieniowym[26].

Spektakularnym przykładem obrazującym możliwości oraz zagrożenia wynikające z zastosowania techniki *spoofingu* w stosunku do bezzałogowych statków powietrznych jest przechwycenie amerykańskiego bezzałogowego systemu powietrznego RQ-170 Sentinel (bez uszkodzenia go), jakie miało miejsce w Iranie w grudniu 2011 roku. Agresorzy analizowali szczątki poprzednio uszkodzonych bezzałogowych statków powietrznych. Na ich podstawie ustalili oni pasma częstotliwości wykorzystywane do komunikacji pomiędzy platformą a naziemną stacją kontroli. Co więcej, zauważono, że w przypadku próby *spoofingu* platforma bezzałogowa przełącza się w tryb autonomicznego lotu w celu kontynuowania programowego

[25] F. Polak, W. Sikorski, K. Siodła, *Lokalizacja źródeł wyładowań niezupełnych z wykorzystaniem matryc mikropaskowych anten UHF*, „Przegląd Elketrotechniczny" t. 1 nr 10 (2018), s. 122.
[26] *Researchers use spoofing to „hack" into a flying drone*, https://www.bbc.com/news/technology-18643134, 2012.(07.06.2019).

lotu. Na podstawie odczytów z systemu GPS poszukuje ona współrzędnych bazy w celu bezpiecznego powrotu. Atakujący po zagłuszeniu kanału komunikacji dokonali *spoofingu* sygnału pochodzącego z satelitów systemu GPS i podszyli informację o koordynatach lotniska w Afganistanie. Problemem okazało się to, że do lądowania należało wybrać miejsce znajdujące się na takiej samej wysokości co amerykańska baza lotnicza[27], z uwagi na odczyt i porównanie danych przez platformę wysokości z wysokościomierza ciśnieniowego.

Jednym ze sposobów na ochronę systemów wojskowych jest amerykański moduł selektywnej antyspoofingowej dostępności SAASM (ang. *Selective Availability Anti-spoofing Module*). Umożliwia on pominięcie konieczności synchronizacji sygnałów PPS (ang. *Precise Positioning Service*) emitowanych w strefie działania serwisu wojskowego z serwisem cywilnym SPS (ang. *Standard Positioning Service*) systemu GPS. W ten sposób dzięki nowatorskim rozwiązaniom sprzętowo-programowym odbiorniki PPS mają możliwość bezpośredniej synchronizacji z kodem wojskowym P(Y)[28]. Warunkiem koniecznym przy takim założeniu jest posiadanie tzw. kluczy kryptograficznych przez odbiornik PPS. Odbiorniki SAASM wykorzystują dwa typy kluczy kryptograficznych, umożliwiających detekcję przekłamanych sygnałów GPS oraz usuwanie selektywnej dostępności. System SAASM ma na celu także zapewnienie dokładności sygnału w sytuacji zastosowania zakłócenia odbiornika GPS. Dodatkowo posiada on możliwość stosowania wyłącznie sygnału cywilnego (np. w sytuacji zagrożenia) oraz możliwość wyłączenia/włączenia sygnału nawigacyjnego dla autoryzowanych użytkowników.

Należy podkreślić, że proces produkcji i dystrybucji odbiorników SAASM podlega ścisłemu nadzorowi przez Departament Obrony USA. Każdy moduł po skonstruowaniu przekazywany jest do niejawnego ośrodka w celu uzupełnienia oprogramowania kryptograficznego (ang. *Key Data Processor* – KDP). Następnie wraca on do producenta, gdzie poddawany jest produkcyjnym testom odbiorczym. O dystrybucji modułów do użytkowników końcowych decyduje Połączone Biuro Projektu GPS (*Joint Program Office* – JPO). Warunkiem przyjęcia odbiornika jest zaliczanie się danego państwa do sojuszniczej grupy militarnej wysokiego poziomu dla Stanów Zjednoczonych[29]. Od 2006 roku w system SAASM wyposażane są wszystkie urządzenia GSP z przeznaczeniem wojskowym.

---

[27] L. D. A. Faria i in., *Susceptibility of GPS-Dependent Complex Systems to Spoofing*, „Journal of Aerospace Technology and Management" t. 10 (2018), s. 2.

[28] Kody systemu GPS oznaczane akronimem PRN, pochodzącym od ang. *pseudorandom*, oznaczającym pseudolosowy. Kody pseudolosowe PRN stanowią pozornie przypadkowe ciągi zer i jedynek logicznych. W rzeczywistości są one generowane zgodnie ze znanymi algorytmami, opisanymi w specyfikacji systemu ICD–GPS–200. W systemie GPS są stosowane dwa rodzaje kodów PRN: kod C/A (ang. *Coarse/Acquisition* oraz *Clear/Access* – zgrubna lub wstępna akwizycja/swobodny dostęp) – przeznaczony dla użytkowników cywilnych. Drugim kodem (przeznaczonym dla użytkowników wojskowych) jest P(Y) (ang. *Precision*). Kod Y jest specjalnie zaszyfrowaną wersją kodu P. A.E. Suzer, H. Oktal, *PRN code correlation in GPS receiver* [w:] *2017 8th International Conference on Recent Advances in Space Technologies (RAST)*, IEEE 2017.

[29] M. Specht, *Wojskowe odbiorniki GPS z modułem SAASM - wprowadzenie do zagadnienia*, „Zeszyty Naukowe Akademii Marynarki Wojennej" t. R. 54 nr 3 (2013), ss. 153–154.

Antycypując dalszy rozwój jammerów oraz systemów spoofingowych, należy wziąć pod uwagę rosnącą autonomię BSP[30] w niektórych opracowaniach – autonomizację[31], a więc zastępowanie człowieka algorytmami matematycznymi, które przy wytyczaniu tras przelotu korzystają z podatnego systemu GPS, służącego nie tylko do kontroli przelotu, lecz także do korygowania planu lotu z uwagi na różne sytuacje np. gwałtowana burza oraz potrzeba jej ominięcia, zwalnianie oraz aktywowanie elementów przestrzeni powietrznej, itp.). W tym celu powstaje między innymi środowisko wirtualnej symulacji do testowania środków bezpieczeństwa w sieci komunikacyjnej bezzałogowych systemów powietrznych. Poprzez stworzenie środowiska możliwe jest wykazanie wszelkich słabości związanych z wykorzystaniem systemów bezzałogowych oraz niekompletności w ich zabezpieczeniach. Kompletny system wymagałby przede wszystkim symulacji innych systemów ważnych dla operacji UAV, takich jak Globalny System Nawigacji Satelitarnej (ang. *Global Navigation Satelitte System* – GNSS).

Analizując urządzenia zakłócające działanie bezzałogowych systemów powietrznych, wartym podkreślenia jest fakt, że ich zastosowanie ma ograniczenia prawne. Zgodnie z prawem polskim oraz Unii Europejskiej używanie zagłuszaczy jest nielegalne. Takie wyposażenie można posiadać, ale korzystanie z niego bez zezwolenia podlega karze grzywny. Przykładem ograniczeń prawnych jest[32] Artykuł 178; ust. 3 tego aktu wskazuje na możliwość ograniczenia zakresu i obszaru eksploatacji sieci telekomunikacyjnych oraz używania w tym celu urządzeń radiowych. Z zagłuszaczy legalnie mogą korzystać jedynie siły zbrojne, policja oraz inne podmioty odpowiadające za bezpieczeństwo publiczne, np. Agencja Bezpieczeństwa Wewnętrznego. Nadmienić należy, że podmioty wskazane w ustawie mogą używać urządzeń zagłuszających jedynie na mocy pozwolenia wydanego przez Prezesa Urzędu Komunikacji Elektronicznej. Ma to na celu nieblokowanie częstotliwości wykorzystywanych przez operatorów sieci komórkowych. Poza zapisami dotyczącymi jedynie pasm sieci telefonii komórkowych trudno doszukać się innych wskazań prawnych na temat ograniczeń w stosowaniu na przykład urządzeń zakłócających systemy nawigacji satelitarnej, których powszechnie używa się do nawigacji statków powietrznych.

[30] Autonomię BSP tłumaczy się jako możliwość bezzałogowego systemu powietrznego do startu, wykonania misji oraz powrotu do bazy bez znaczących interwencji człowieka. Niektóre opracowania, w zależności od jej (do czego odnosi się ten zaimek?) poziomu zaawansowania technologicznego, traktują o pojęciu pełnej autonomii BSP (ang. *full UAV autonomy*). K.P. Valavanis, G.J. Vachtsevanos, *UAV Autonomy: Introduction* [w:] *Handbook of Unmanned Aerial Vehicles*, Dordrecht 2015.W tym rozumieniu, że powyżej wymienione fazy lotu (wykonywanej operacji) są dokonywane bez udziału człowieka.

[31] R. Elgohary, *Software Development for Autonomous Unmanned Aerial Vehicle* [w:] brak tytułu publikacji 2014; A. Kuptel, *„Autonomisation" of Security and Defence Systems*, „Security and Defence Quarterly" t. 23 nr 1 (2019), ss. 81–84.

[32] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (DzU z 2004 r. Nr 171, poz. 1800, z późn. zm.).

## NIEKINETYCZNE SYSTEMY NEUTRALIZACJI BEZZAŁOGOWYCH SYSTEMÓW POWIETRZNYCH – PRZEGLĄD ROZWIĄZAŃ

Jedną z propozycji niekinetycznych systemów neutralizacji bezzałogowych systemów powietrznych jest opracowany w 2015 roku system obrony naziemnej przed bezzałogowymi statkami powietrznymi AUDS (ang. *Anti-UAV Defence System*)[33]. Powstał on w wyniku prac trzech konsorcjów brytyjskich – Enterprise Control Systems, Chess Dynamics i Blighter Surveillance Systems. Budowa (Rysunek 2) oraz działanie systemu składa się z trzech komponentów/etapów: wykrycie (ang. *detect*), śledzenie (inaczej trakowanie – ang. *track*) oraz neutralizacja (ang. *defeat*[34]). Ogólne możliwości systemu pozwalają na wykrycie (poniżej 15 sekund), śledzenie i neutralizację obiektu bezzałogowego o zasięgu do 10 km od miejsca bazowania urządzenia.

W pierwszym etapie działania systemu AUDS następuje wykrycie wrogiego obiektu. Służy do tego modułowa, nieobrotowa stacja radiolokacyjna, tzw. e-scaner (Rysunek 2a), wykorzystująca antenę z pasywnym system PESA (ang. *Passive Electronically Scanned Array*). Jego działanie polega na wykorzystaniu (jako źródła sygnału) emitera mikrofalowego, dystrybułowanego poprzez moduły anteny, gdzie każdy komponent anteny jest modułem nadawczo-odbiorczym. Z uwagi na wykrycie gabarytowo małych i wolno lecących obiektów wykorzystuje on również impulsowy radar ze zmodulowaną częstotliwościowo falą nośną (ang. *Frequency Modulated Continuous Wave* – FMCW). Stacja radiolokacyjna wykorzystuje technologię 3D[35], umożliwiającą lokalizację bezzałogowych systemów powietrznych niskich kategorii[36], które wykonane są z materiałów kompozytowych, często w formie monolitu, zmniejszając ilość metalowych, dobrze odbijających promieniowanie elementów.

Ważący około 30 kg system wykrywania obiektów zapewnia pokrycie radarowe 180° lub 360° o elewacji pionowej w zależności od użytej anteny w zakresie 10÷15° (antena M10S) lub 20÷30° (antena W20S). Urządzenie wykrywa bezzałogowe platformy powietrzne do 3,6 kg, w zakresie prędkości od zawisu (0 km/h) do 400 km/h.

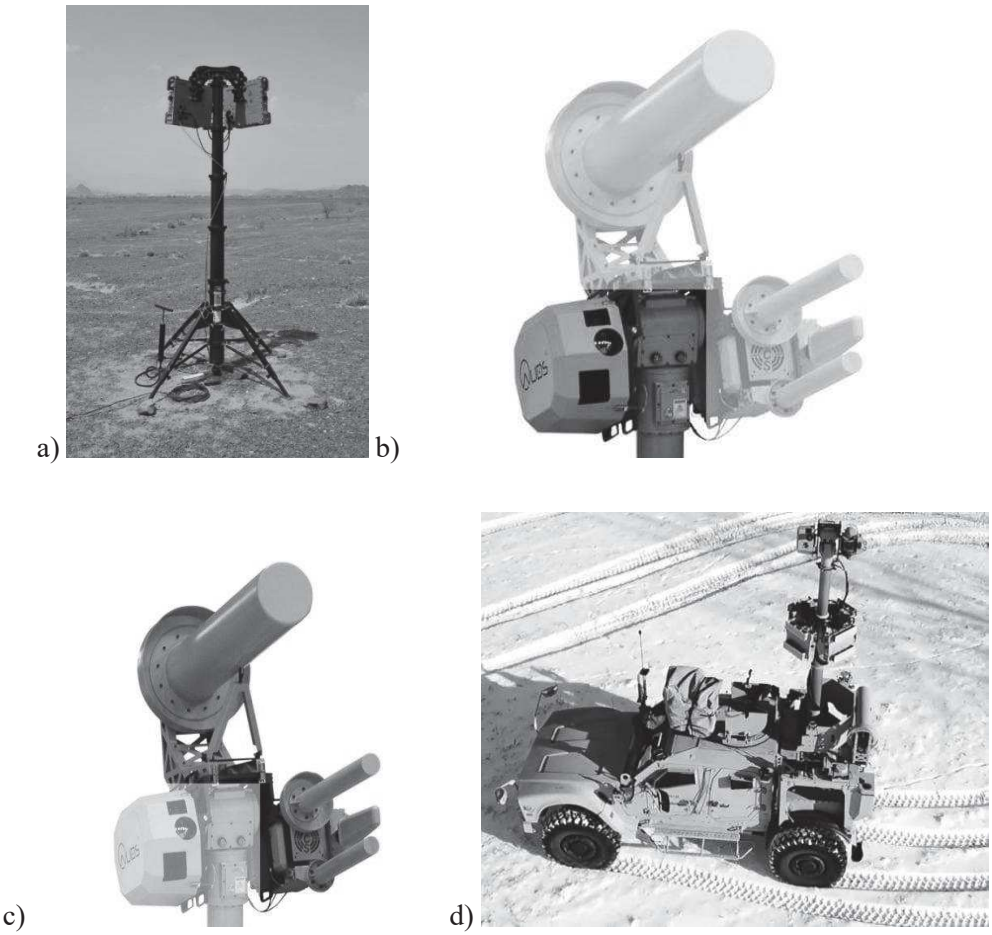
---

[33] Vide: B.-H. Sheu i in., *Dual-axis rotary platform with UAV image recognition and tracking*, „Microelectronics Reliability" t. 95 (2019).

[34] Tłumaczone dosłownie jako „zniszczenie". W tym kontekście zaproponowano polskojęzyczny odpowiednik „neutralizacja" z uwagi na to, że „zniszczenie" kojarzone jest ze zniszczeniem fizycznym. Co prawda w niektórych przypadkach jest to efektem działania systemu AUDS, lecz nie jest to konsekwencją bezpośrednią.

[35] Nazwa pochodzi od akronimu, pochodzącego od anglojęzycznej nazwy *Digital Drone Detection*, co można przetłumaczyć jako „cyfrowa detekcja systemów bezzałogowych".

[36] Na potrzeby tego opracowania za bezzałogowe statki powietrzne niskich kategorii uważa się, bezzałogowe systemy powietrzne klasy I o masie poniżej 150 kg, pułapie do 360 m oraz zasięgu do 50 km. Kategorie te, zgodnie z typologią to: Small, Mini i Micro. R. Bielawski, *Wybrane zagadnienia z budowy statków powietrznych. Definicje, pojęcia i klasyfikacje*, Warszawa 2015, s. 80.



**Rysunek 2.** Budowa poszczególnych komponentów systemu obrony naziemnej przed bezzałogowymi systemami powietrznymi AUDS
Źródło: *AUDS Web Page* 2019, https://www.auds.com/technology/.

Drugim elementem systemu jest czujnik elektrooptyczny (ang. *EO sensor*), służący do śledzenia obiektów bezzałogowych (Rysunek 2b) małych gabarytów, poruszających się z dużymi prędkościami. Czujnik elektrooptyczny wykorzystuje dodatkowo podwójny system kamer. Stanowi go kamera termowizyjna emitująca fale o średniej długości (ang. *Medium Wave Thermal Imager* – TI) wyposażona w możliwość elektronicznego zbliżania obiektu – e-zoom. Drugim zaimplementowanym urządzeniem jest kamera światła dziennego w rozdzielczości HD. Jest nią trzeciej generacji kamera dzienna Piranha, z wbudowanym filtrem podczerwieni wspomagającym działanie urządzenia w porze zachodu Słońca lub w ciemności.

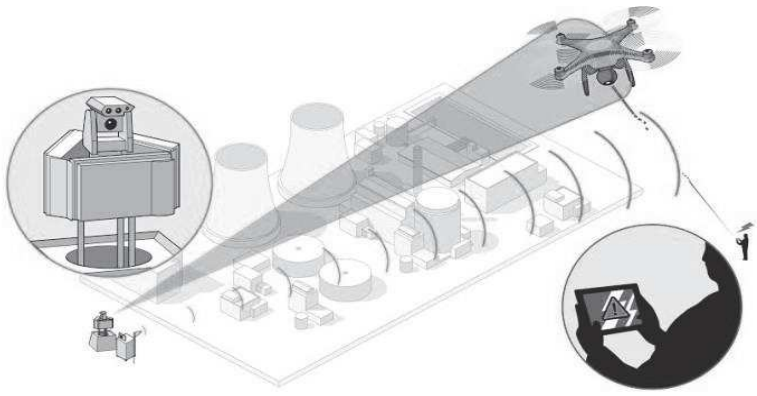
Trzeci komponent systemu AUDS służy do neutralizacji platform bezzałogowych (Rysunek 2c). Głównym elementem rażącym jest inhibitor radiowy (ang. *radio-frequency Inhibitor*) zakłócający system łączności dowodzenia i kontroli C2. Inhibitor zbudowany jest w technice radia definiowanego programowo SDR. Dodatkowo podsystem wyposażony jest w anteny kierunkowe o wysokim zysku, osiowo zamontowane z czujnikiem elektrooptycznym i posiadające możliwości nominalnej szerokości wiązki wynoszącej 20°. Ograniczanie pasma radiowego w stosunku do obiektów powietrznych może następować wybiórczo lub w zakresie od 400 MHz to 6 GHz

ze szczególnym uwzględnieniem najczęściej występujących pasm – 433 MHz; 915 MHz; 2,4 GHz; 5,8 GHz, oraz pasma globalnych systemów nawigacji satelitarnej GNSS.

Głównymi założeniami działania systemu była neutralizacja obiektów bezzałogowych wykonujących misje rozpoznawcze, mogących być nosicielami małych bomb bądź improwizowanych ładunków wybuchowych (ang. *Improvised Explosive Device* – IED). Producent przewiduje również zastosowanie zestawu w stosunku do bezzałogowych systemów powietrznych, mogących wykonywać nieautoryzowane loty na małych wysokościach i stanowić zagrożenie dla lądujących i startujących statków powietrznych, również w rozumieniu możliwości dokonania aktu terroru lub nieuprawnionej ingerencji z użyciem BSP. Kolejny, zdefiniowany problem, który może być ograniczony przez tego typu BSP, to przemyt narkotyków oraz innych niebezpiecznych i niedozwolonych substancji, a także przechwytywanie numerów IP urządzeń lotniskowych bądź elementów infrastruktury lotniskowej, a także krytycznej (np. elektrownie). System AUDS może również wspomagać ochronę VIP-ów oraz obszarów, gdzie operowanie bezzałogowymi statkami powietrznymi jest niedozwolone (np. okolice fabryk produkujących uzbrojenie) lub ograniczone odpowiednimi, elastycznymi strukturami przestrzeni powietrznej – strefy D, P i R[37].

Dodatkowo atutem systemu jest to, że może on działać jako element stacjonarny (Rysunek 2a-c) oraz mobilny (Rysunek 2d) – umieszczony najczęściej na samochodach o dużej mobilności[38]. Działa on również w każdych warunkach pogodowych zarówno w dzień, jak i w nocy.

Kolejną propozycją do neutralizacji bezzałogowych systemów powietrznych jest Counter–UAV System. Został on opracowany w 2015 roku przez firmę Airbus Defence and Space. Jego działanie polega na wykrywaniu i neutralizacji obiektów latających – bezzałogowych systemów powietrznych niskich kategorii, które bezprawnie wkroczyły na niedozwolone obszary krytyczne (



Rysunek 3).

[37] D – strefa niebezpieczna (ang. *Danger Area*), P – strefa zakazana (ang. *Prohibited Area*), R – strefa o ograniczonym ruchu lotniczym (ang. *Restricted Area*). Należą one do elastycznych elementów (struktur) przestrzeni powietrznej.
[38] *AUDS Web Page*.

**Rysunek 3.** Sposób działania systemu do neutralizacji bezzałogowych systemów powietrznych Counter-UAV (Airbus Defence and Space)
Źródło: Airbus, *Counter-UAV System from Airbus Defence and Space protects large installations and events from illicit intrusion*, 2015[39].

System działa w oparciu o urządzenia przeznaczone do przeciwdziałania elektronicznego z dużą skutecznością, pozwalając na minimalizowanie zjawiska *collateral damage*[40]. Dzięki łączeniu zsyntezowanych danych z różnych źródeł, takich jak radary operacyjne, kamery podczerwieni oraz radionamierniki, zapewnia on wysoką efektywność, gwarantując zasięg do 10 km. Samo zakłócanie agresora realizowane jest przez jammer, przykrywający sygnał nawigacyjny oraz komunikację pomiędzy bezzałogową platformą a jej operatorem. Z uwagi na możliwość zastosowania urządzenia w miejscach zapewnienia komunikacji (np. lotniska – model wykorzystuje tzw. system inteligentnego, selektywnego zakłócania SRJT, ang. *Smart Responsive Jamming Technology*). Pozwala ona na zakłócanie jedynie częstotliwości wykorzystywanej przez rażoną platformę bezzałogową, nie powodując zakłóceń innych, okolicznych systemów wymiany informacji. Counter–UAV System posiada również moduł spoofingowy, służący do przejęcia kontroli oraz neutralizacji potencjalnego agresora.

Przeznaczeniem systemu, zgodnie z zapowiedzią producenta firmy Airbus Defence and Space, mogą być elementy infrastruktury krytycznej państwa (np. elektrownie jądrowe, porty lotnicze, lotniska wojskowe) oraz inne obszary, gdzie wykonywanie operacji przez nieautoryzowane, bezzałogowe systemy powietrzne może być niepożądane z punktu widzenia bezpieczeństwa państwa.

Inną propozycją systemu do neutralizacji bezzałogowych systemów powietrznych jest *Compact Laser Weapons System* (CLWS) firmy Boeing, będący częścią amerykańskiego programu *Mobile Expeditionary High Energy Laser* (MEHEL). Jego działanie oparte jest o emisję wiązki światła laserowego dużej mocy (trzy wersje emisji: 2, 5 i 10 kW), które emitowane jest do rażonego obiektu latającego przez około 15 s. Światło emitowane przez laser naświetla rażony obiekt, powodując zwiększenie temperatury, a w efekcie zapalenie jego poszycia. Dzięki niewielkiej masie własnej, wynoszącej ok. 2,3 kg jest ono mobilne oraz

[39]Airbus, *Counter-UAV System from Airbus Defence and Space protects large installations and events from illicit intrusion*, 2015, https://www.airbus.com/newsroom/press-releases/en/2015/09/counter-uav-system-from-airbus-defence-and-space-protects-large-installations-and-events-from-illicit-intrusion.html.(30.05.2019).
[40] Termin *collateral damage* oznacza straty i zniszczenia niezamierzone NATO Standardization Agency (NSA), *AAP-6. Słownik terminów i definicji NATO*..., s. 103.

trudne do wykrycia przez przeciwnika. Zazwyczaj jest implementowane na pojazdach, okrętach oraz innych mobilnych platformach[41].

Kolejnym dostępnym, niekinetycznym urządzeniem przeznaczonym do neutralizacji bezzałogowych aparatów latających jest mobilny zestaw DRONEKILLER, rozwijany przez amerykańską firmę IXI Technology. Urządzenie działa w oparciu o zakłócania pasma radiowego w zakresach 426÷445 MHz; 902÷928 MHz; 2400÷2483 MHz; 5725÷5850 MHz oraz systemu C2 (wykorzystującego GPS oraz GLONASS L1) naruszyciela, a także emisję ukierunkowanej wiązki energii (ang. *directed-energy weapon* – DEW) w jego kierunku. Urządzenie zasilane jest ogniwem litowo-jonowym, wielokrotnego ładowania (prądem w zakresie 9÷21V DC), pozwalającym na pracę z aktywnym trybem do 2 h oraz z możliwością wykrywania obiektów przez 8 godzin. Jego atutem są niewielkie wymiary (długość 61 cm, wysokość 24 cm oraz szerokość 10 cm) oraz masa wynosząca ok. 3,4 kg. Model ten może być eksploatowany w zakresie temperatur od –20 do +40°C (magazynowane w zakresie –40 do +85°C). Jest odporny na wibracje mechaniczne oraz szoki termiczne. Zasięg wykrywania obiektów powietrznych przez to urządzenie wynosi do 800 m w stożku 30º. Czas użycia i neutralizacji obiektu wynosi poniżej 1 min. Ponadto posiada ustawienia wspomagające, w zależności od intensywności światła oraz pory dnia i nocy.

System powstał z myślą o przeciwdziałaniu przestępczości polegającej na wykorzystywaniu bezzałogowych platform latających do zrzutu bomb, granatów oraz improwizowanych ładunków wybuchowych typu IED. Może być również użyty w stosunku do BSP naruszających aktywowane struktury przestrzeni powietrznej, a także odbywających loty w przestrzeni niekontrolowanej. System ten stanowi dobrą alternatywę do ochrony wojskowych baz lotniczych oraz portów lotniczych, a także innych obiektów o znaczeniu strategicznym. System może być używany jako wyposażenie osobiste konwojentów oraz personelu odpowiedzialnego za bezpieczeństwo (np. ochronę VIP). Omawianą platformę wykorzystuje się również do uzupełnienia większych i automatycznych systemów do neutralizacji BSP[42].

Kolejnym urządzeniem neutralizującym bezzałogowe systemy powietrzne jest rodzime rozwiązanie firmy Hertz Systems o nazwie „Jastrząb". W swojej budowie posiada on dookólną stację radiolokacyjną, dającą możliwość symultanicznego wykrywania wielu platform jednocześnie w czasie rzeczywistym. Zastosowanie tego systemu pozwala również na odróżnianie naruszycieli od samolotów załogowych czy ptactwa, co skutecznie zmniejszy prawdopodobieństwo pomyłki. Model ten może być wykorzystywany stacjonarnie, jak również na platformie mobilnej (np. samochód terenowy). Elementem aktywnym systemu jest neutralizator wysyłający sygnał zakłócający, pozwalający na odcięcie komunikacji pomiędzy

[41] Boeing, *Silent Strike Boeing's Compact Laser Weapons System tracks and disables UAVs*, https://www.boeing.com/features/2015/08/bds-compact-laser-08-15.page.(01.06.2019).
[42] Unmanned-Airspace, *IXI Technology Drone Killer "uses software define radio technology" to disable UAS threats*, https://www.unmannedairspace.info/counter-uas-systems-and-policies/ixi-technology-drone-killer-uses-software-define-radio-technology-disable-uas-threats/.(07.07.2019).

naruszycielem, a jego operatorem, umożliwiając tym samym bezpieczne sprowadzenie go na ziemię. Zasięg działania urządzenia wynosi do 3 km.

System Jastrząb powstał z myślą o zwiększeniu bezpieczeństwa wokół lotnisk cywilnych, zważywszy na możliwość wykonywania lotów przez bezzałogowe statki powietrzne zagrażające lotnictwu komunikacyjnemu. Poza tym zastosowaniem producent wskazuje na używanie BSP jako przedmiotu ataku terrorystycznego skierowanego przeciwko ludności cywilnej, jak również w stosunku do kluczowych obiektów strategicznych i wojskowych. Kolejnym przeznaczeniem systemu Jastrząb może być przeciwdziałanie przemytowi transportu broni oraz narkotyków, a w stosunku do terrorystów ISIS – przeciwdziałanie wykorzystaniu BSP do bombardowania ludności cywilnej oraz pojazdów[43].

## ZAKOŃCZENIE

W pracy wyszczególniono cztery podstawowe techniki zamierzonych zakłóceń skierowanych przeciw bezzałogowym systemom powietrznym – *jamming*, *spoofing*, *meaconing* oraz kompilację tych technik uzupełnioną intruzją i interferencją.

Wskazano na możliwości urządzeń zakłócających zbudowanych przy użyciu tych technik – jammery i spoofery, jako najczęściej dostępne i występujące. Dokonano ich charakterystyki, podziałów i możliwości technicznych oraz przedstawiono wyniki badań przeprowadzonych przez ośrodki naukowe na świecie. Antycypując poziom bezpieczeństwa bezzałogowych systemów powietrznych, operujących w nowym środowisku zakłóceń zamierzonych, szczególną uwagę zwrócono na dwa aspekty. Po pierwsze, przewidziano problem zachowania poziomu bezpieczeństwa BSP w obliczu autonomizacji tych systemów. Po drugie, zauważono brak uregulowań prawnych w tym kontekście. Obecnie obowiązujące prawo telekomunikacyjne odnosi się jedynie do sieci telekomunikacyjnych zajmowanych często przez operatorów sieci komórkowych (istnieje możliwość ich zakłócenia przez tego typu urządzenia). W przepisach prawnych brak jest obecnie odwołania do innych, technicznych aspektów, które zawierają tego typu urządzenia, np. emisja wiązki światła laserowego, zakłócenia częstotliwości radiowych czy systemów nawigacji satelitarnej.

Jako rozwiązanie narastającego problemu dotyczącego zakłóceń zamierzonych zaproponowano niekinetyczne systemy neutralizacji bezzałogowych systemów powietrznych. Dokonano przeglądu tych urządzeń, wskazując na takie ich zalety jak: wykrywanie, śledzenie i neutralizacja obiektów, ich dużą mobilność oraz stosunkowo duży zasięg (do ok. 10 km). Z drugiej strony są to urządzenia, które mogą neutralizować BSP niskich kategorii.

### FINANSOWANIE

[43] Hertz_Systems, *System antydronowy Jastrząb*, https://www.hertzsystems.com/product/systemy-antydronowe/ (03.06.2019).

Artykuł został sfinansowany ze środków na działalność statutową, w ramach realizacji zadania badawczego „Wykorzystanie bezzałogowych aparatów latających w zapewnieniu bezpieczeństwa" ujętego w „Planie zadaniowo-finansowym działalności naukowej Akademii Sztuki Wojennej na rok 2019".

## BIBLIOGRAFIA

Airbus. 2015. Counter-UAV System from Airbus Defence and Space protects large installations and events from illicit intrusion, https://www.airbus.com/newsroom/press-releases/en/2015/09/counter-uav-system-from-airbus-defence-and-space-protects-large-installations-and-events-from-illicit-intrusion.html.

AUDS Web Page. 2019. https://www.auds.com/technology/.

Bazzano Federica, Montuschi Paolo, Lamberti Fabrizio, Paravati Gianluca, Casola Silvia, Ceròn Gabriel, Londoño Jaime, Tanese Flavio. 2017. Mental Workload Assessment for UAV Traffic Control Using Consumer-Grade BCI Equipment. In: Horain P., Achard C., Mallem M. (eds) Intelligent Human Computer Interaction. IHCI 2017. Lecture Notes in Computer Science, vol 10688. 60-72, Springer, Cham.

Bielawski Radosław. 2015. Wybrane zagadnienia z budowy statków powietrznych. Definicje, pojęcia i klasyfikacje. Warszawa: Wydawnictwo Akademii Obrony Narodowej.

Boeing. 2015. Silent Strike Boeing's Compact Laser Weapons System tracks and disables UAVs, https://www.boeing.com/features/2015/08/bds-compact-laser-08-15.page.

Buesnel Guy. 2015. "Threats to satellite navigation systems", Network Security (Nr 3): 14-18, DOI: 10.1016/S1353-4858(15)30019-2.

Chen Lunde, Abdellatif Slim , Francklin Armel, Tegueu Simo, Gayraud Thierry. 2019. "Embedding and re-embedding of virtual links in software-defined multi-radio multi-channel multi-hop wireless networks" Computer Communications (Vol. 145): 161-175, DOI: 10.1016/j.comcom.2019.06.012.

Elgohary Rania. 2014. "Software Development for Autonomous Unmanned Aerial Vehicle". In: Das V.V., Elkafrawy P. (eds) Signal Processing and Information Technology. SPIT 2012. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (Vol 117): 57-64. Springer, Cham.

Faria Lester de Abreu, Silvestre Caio Augusto de Melo, Correia Marcelino Aparecido Feitosa, Roso Nelson A. 2018. "Susceptibility of GPS-Dependent Complex Systems to Spoofing" Journal of Aerospace Technology and Management (t. 10). https://dx.doi.org/10.5028/jatm.v10.839.

Ferrara Nunzia Giorgia, Bhuiyan Mohammad Zahidul H., Söderholm Stefan, Ruotsalainen Laura, Kuusniemi Heidi. 2018. "A new implementation of narrowband interference detection, characterization, and mitigation technique for a software-defined multi-GNSS receiver" GPS Solutions (t. 22, nr 4), https://doi.org/10.1007/s10291-018-0769-z.

Figurski Mariusz, Szołucha Marcin, Mielnik Piotr, Gałuszkiewicz Marcin, Wrona Maciej, Szymański Piotr. 2011. "Wpływ zakłóceń na pomiary GPS. GPS kontra zagłuszanie Geodeta (t. 1, nr 188): 46-51.

Graf Rudolf. 1999. Modern Dictionary of Electronics, Elsevier.

Grover Kanika, Lim Alvin, Yang Qing. 2014 "Jamming and anti-jamming techniques in wireless networks: a survey International Journal of Ad Hoc and Ubiquitous Computing (t. 17, nr 4): 1-16, DOI: 10.1504/IJAHUC.2014.066419, http://www.inderscience.com/link.php?id=66419.

Hertz_Systems. 2019. System antydronowy Jastrząb, https://www.hertzsystems.com/product/systemy-antydronowe/.

Jamming GPS. 2019. https://www.dlp-expert.pl/blog/id,194/geoforum.pl/upload/review/file/188_s46_51_z.pdf.

Kattenborn Teja, Lopatin Javier, Förster Michael, Christian Andreas, Fabian Braun, Fassnacht Ewald, 2019. "UAV data as alternative to field sampling to map woody invasive species based on combined Sentinel-1 and Sentinel-2 data". Remote Sensing of Environment (t. 227): 61-73, DOI: 10.1016/j.rse.2019.03.025.

Kowaleczko Piotr, Sulkowski Jarosław, 2012. "Podatność systemu nawigacji satelitarnej GPS na zakłócenia i wynikające z niej zagrożenia dla transportu" Logistyka" (t. 3): 1115-1121.

Kuptel Artur. 2019. ""Autonomisation" of Security and Defence Systems" Security and Defence Quarterly" (t. 23, nr 1): 79-96, DOI: 10.35467/sdq/105430, http://www.journalssystem.com/sdq/,105430,0,2.html.

Loukas George. 2015. "Cyber-Physical Attack Steps" Cyber-Physical Attacks, Elsevier.

Magiera Jarosław. 2015. Analiza i badania systemu antyspoofingowego GPS. Wydawnictwo Politechniki Gdańskiej. https://eti.pg.edu.pl/documents/176852/24639848/Autoreferat_JMagiera.pdf.

Magiera Jarosław, Katulski Ryszard, 2015. "Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing" Journal of Applied Research and Technology (t. 13, nr 1): 45-57 DOI: 10.1016/S1665-6423(15)30004-3.

Marnach Daniel, Mauw Sjouke, Martins Miguel, Harpes Carlo. 2013. "Detecting Meaconing Attacks by Analysing the Clock Bias of Gnss Receivers". Artificial Satellites. (t. 48, nr 2): 63-83, DOI: 10.2478/arsa-2013-0006.

NATO Standardization Agency (NSA). 2005. AAP-6. Słownik terminów i definicji NATO.

1986. Operations Reporting Meaconing, Intrusion, Jamming and Interference of Electromagnetic Systems, RCS: JCS-1066(MIN).

Polak Filip, Sikorski Wojciech, Siodła Krzysztof. 2018. "Lokalizacja źródeł wyładowań niezupełnych z wykorzystaniem matryc mikropaskowych anten UHF" Przegląd Elketrotechniczny (t. 1, nr 10): 122-123, DOI: 10.15199/48.2018.10.28.

Price Jeffrey, Forrest Jeffrey. 2013. Practical Aviation Security, Elsevier.

2012. Researchers use spoofing to „hack" into a flying drone, https://www.bbc.com/news/technology-18643134.

Riahi Manesh Mohsen, Kaabouch Naima. 2019. "Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions". Computers & Security (t. 85): 386-401, DOI: 10.1016/j.cose.2019.05.003.

Rügamer Alexander, Kowalewski Dirk. 2015. Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!, https://www.fig.net/resources/proceedings/fig_proceedings/fig2015/papers/ts05g/TS05G_ruegamer_kowalewski_7486.pdf.

Sabatini Roberto, Moore Terry, Ramasamy Subramanian. 2017. "Global navigation satellite

systems performance analysis and augmentation strategies in aviation". Progress in Aerospace Sciences (t. 95): 45-98, DOI: 10.1016/j.paerosci.2017.10.002.

Sheu Bor-Horng, Chiu Chih-Cheng, Lu Wei-Ting, Lien Chun-Chieh, Liu Tung-Kuan, Chen Wen-Ping. 2019. "Dual-axis rotary platform with UAV image recognition and tracking", Microelectronics Reliability (t. 95): 8-17, DOI: 10.1016/j.microrel.2019.02.005.

Specht Mariusz. 2013. "Wojskowe odbiorniki GPS z modułem SAASM - wprowadzenie do zagadnienia" Zeszyty Naukowe Akademii Marynarki Wojennej (R. 54, nr 3): 147-156, DOI: 10.5604/0860889X/1086932

Stewart Mark, Mueller John. 2018. Evaluating Aviation Security. Elsevier.

Strużak Ryszard, Sobolewski Janusz. 2014. "Wirtualna zajętość widma w sieciach radia kognitywnego - algorytmy oceny". Telekomunikacja i Techniki Infomacyjne" (t. 1–2): 33-48.

Suzer Ahmet Esat, Oktal Hakan. 2017. "PRN code correlation in GPS receiver" 2017 8th International Conference on Recent Advances in Space Technologies (RAST), IEEE 2017.

Trzaskowski Zbigniew. 2018. "Bezpieczeństwo globalnych systemów nawigacji satelitarnej a możliwości ich zakłócenia – jamming" Bezpieczeństwo w środowisku lotniczym i kosmicznym: 159-163. Semper. Warszawa.

Unmanned-Airspace, IXI Technology Drone Killer "uses software define radio technology" to disable UAS threats, 2018. https://www.unmannedairspace.info/counter-uas-systems-and-policies/ixi-technology-drone-killer-uses-software-define-radio-technology-disable-uas-threats/.

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (DzU z 2004 r. Nr 171, poz. 1800, z późn. zm.).

Valavanis Kimon, Vachtsevanos George. 2015. UAV Autonomy: Introduction, Springer, Dordrecht.