Zbigniew Piskor[1]
Państwowa Akademia Nauk Stosowanych w Chełmie

https://doi.org/10.29316/9788368103373_16

EWOLUCJA CYBERZAGROŻEŃ TRANSPORTU LOTNICZEGO

THE EVOLUTION OF CYBER THREATS TO AIR TRANSPORT

Streszczenie

Rozdział porusza problematykę cyberzagrożeń w lotniczych systemach informatycznych jako ważnego czynnika prowadzącego do zagrożeń dla bezpieczeństwa transportu lotniczego, wykorzystującego urządzenia IT do prowadzenia większości swoich operacji przez internet. Na świecie obserwuje się stały wzrost liczby cyberataków na wszystkie sektory działalności lotniczej. Operacje w sieci muszą być chronione przy użyciu kompleksowych przepisów dotyczących cyberbezpieczeństwa. Celem jest analiza wpływu tego typu ryzyka na poziom bezpieczeństwa w transporcie lotniczym. Stosownie do przyjętego celu sformułowano główny problem badawczy: Jak niepoprawne działania w korzystaniu z urządzeń IT powodowane przez organizacje wpływają na poziom cyberbezpieczeństwa transportu lotniczego? Uzyskanie odpowiedzi na powyższe pytanie wymagało zastosowania metod badawczych, w tym dokonania krytycznej analizy aktów prawnych i wybranych pozycji literatury przedmiotu. Przeprowadzona analiza wskazuje, że aby poprawić działalność branży i organizacji lotniczych, należy rozważyć wprowadzenie odpowiednich

[1] https://orcid.org/0000-0002-4456-1104, e-mail: zbpis@wp.pl

środków oraz przyjąć wyznaczone kierunki zmian. Tezę tę potwierdzają statystyki zdarzeń cybernetycznych oraz liczne działania podejmowane przez państwa w celu zwalczania cyberzagrożeń.

Słowa kluczowe: cyberzagrożenia, lotnictwo, bezpieczeństwo, ochrona, statki powietrzne

Abstract

The article addresses the issue of cyber threats to aviation IT systems as an important factor contributing to security risks in air transport, which relies on devices to conduct most of its operations over the Internet. Worldwide, there is a steady increase in cyberattacks across all sectors of aviation activity. Network operations must be protected using comprehensive cybersecurity regulations. The goal is to analyse the impact of this type of security-related risk on security-related proceedings in air transport. In accordance with the adopted objective, the main research problem was formulated as follows: How do improper actions in the use of IT devices by the organisation affect the level of cybersecurity in air transport? Obtaining an answer to the above question required applying research methods, including a critical analysis of legal acts and selected literature in the field. The analysis of the indicated areas shows that to improve the operations of the aviation industry and organisations, it is necessary to implement appropriate measures and adopt the designated directions of change. This thesis is supported by statistics on cyber incidents and by numerous actions taken by countries to combat cyber threats.

Keywords: cybersecurity, hazards, aviation, safety, security, plane

Wstęp

Cyberprzestrzeń stanowi nieodłączny komponent współczesnego świata. Globalne lotnictwo ze swoją infrastrukturą cyfrową charakteryzuje się rozległymi wzajemnymi powiązaniami i złożonością oraz wysokim poziomem ekspozycji w mediach społecznych, a także kluczową rolą w rozwoju społeczno-gospodarczym krajów i państw. Poziom globalnych wzajemnych połączeń systemów i sieci stwarza bezprecedensowy rozwój technologicznych instrumentów charakteryzujących się powiązaniami i złożonością szeregu transformacji w wykorzystaniu mocy technologii w celu zwiększenia wydajności w przepływie danych, które wykraczają poza granice państw. Przeciwdziałanie zagrożeniom i ryzykom dla lotnictwa musi opierać się na współdziałaniu i współpracy między wszystkimi zainteresowanymi stronami.

W tym celu idealnym dla społeczności lotniczej jest Międzynarodowa Organizacja Lotnictwa Cywilnego przy ONZ która podejmując wysiłki na rzecz cyberbezpieczeństwa w lotnictwie były spójne, zharmonizowane, zgodne z priorytetami międzynarodowego lotnictwa cywilnego i obejmujące:

- opracowywanie (SARP) norm i zalecanych metod postępowania załącznika 17 – Ochrony lotnictwa cywilnego (Konwencja o międzynarodowym lotnictwie cywilnym, 1944),
- zapewnieniu, aby ramy międzynarodowego prawa lotniczego były odpowiednie do przeciwdziałania cyberatakom na lotnictwo cywilne,
- wspieranie dyskusji o cyberbezpieczeństwie w lotnictwie na szczeblu globalnym, regionalnym i krajowym,
- rozwijanie inicjatyw wspierających budowanie, wdrażanie zdolności z zakresu cyberbezpieczeństwa lotniczego dla społeczności lotniczej,
- podnoszenie świadomości na temat znaczenia rozwiązywania problemu ochrony cyberprzestrzeni dla lotnictwa cywilnego.

Strategia cybernetycznego bezpieczeństwa w lotnictwie stanowi podstawę wizji ICAO z którą globalne cywilne lotnictwo ma być odporne na cyberataki i wprowadzać innowacje. Zbudowana jest na siedmiu filarach:

1. Polityka w zakresie bezpieczeństwa cybernetycznego.
2. Przepisy ustawowe i wykonawcze.
3. Zarządzanie.
4. Zarządzanie incydentami, planowanie awaryjne.
5. Budowanie zdolności, szkolenia i kultury cyberbezpieczeństwa.
6. Współpraca międzynarodowa.
7. Wymiana informacji.

Rozwiązywanie problemu cyberbezpieczeństwa w cywilnym lotnictwie stało się na forum ICAO kwestią bezprecedensową najwyższej rangi, określone poprzez rezolucje Zgromadzenia:

- A39-19, dotyczącej cyberbezpieczeństwa w lotnictwie cywilnym – 2016 rok,
- A40-10, dotycząca problemu cyberbezpieczństwa w lotnictwie cywilnym – 2019 rok,
- A41-19, dotyczącej cyberbezpieczeństwa w lotnictwie cywilnym – 2022 rok,

zawierające klauzule, które uznają wzajemne powiązania między bezpieczeństwem, efektywnością, zarządzaniem, współpracą i współdziałaniem w rozwiązywaniu tak istotnych zagadnień w przeciwdziałaniu cyberatakom na lotnictwo cywilne. Wezwano państwa członkowskie do przyjęcia i wdrożenia Konwencji Pekińskiej z 2010 roku oraz Protokołu Pekińskiego (Żylicz, 2002; International Civil Aviation Organization, 2022).

Europejska Agencja Bezpieczeństwa Lotniczego opublikowała wymagania dotyczące zarządzania ryzykiem informacji – Rozporządzenie Part-IS, w którym zamieszczono wytyczne dostosowania Systemów Zarządzania Bezpieczeństwem Informacji opartych o ISO 27001. Rozporządzenie ma zastosowanie do organów odpowiedzialnych za certyfikację i nadzór nad organizacjami lotniczymi mogącymi mieć wpływ na bezpieczeństwo lotnicze. Ochrona poufności i integralności danych technologii informacyjnych wykorzystywanych w lotnictwie cywilnym. Jako kluczowy element kompleksowej strategii cyberbezpieczeństwa ma zastosowanie do różnych obszarów lotnictwa, podkreślając znaczenie informacji w lotnictwie. Nakłada na nadzory lotnicze oraz organizacje obowiązek stworzenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Organizacje powinny również spełniać wymagania NIS2 (Parlamentu Europejskiego). EASA Part IS oznacza wymagania dotyczące systemu zarządzania bezpieczeństwem informacji określone w rozporządzeniach Unii Europejskiej: Rozporządzenie Delegowane 2022/1645 i Rozporządzenie Wykonawcze 2023/203. Nadrzędnym celem ISMS jest kontrola ryzyka związanego z bezpieczeństwem informacji. Standardem dla ISMS jest ISO/IEC 27001:2022 oraz ISO/IEC 22301, których celem jest zmniejszenie prawdopodobieństwa wystąpienia zakłóceń w przypadku sytuacji kryzysowej, przygotowanie się na ewentualne zakłócenia i posiadanie zdolności do skutecznego reagowania na zakłócenia lub odtworzenia działania w określonym czasie, na wyznaczonym poziomie sprawności organizacji. Norma ISO 31000 Zarządzanie Ryzykiem stanowi wsparcie poprzez zbiór zasad i wytycznych, dobrych praktyk, które należy zastosować w celu utrzymania i udoskonalania skuteczności procesu zarządzania ryzykiem (Syta, 2025, s. 122). Raport dotyczący Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), uzupełnia obecny system zarządzania bezpieczeństwem w zakresie bezpieczeństwa informacji elementami:

- zarządzanie ryzykiem związanym z bezpieczeństwem informacji,
- obsługą incydentów związanych z informacjami,
- obsługą zgłaszanych zdarzeń związanych z bezpieczeństwem informacji,
- strategią zarządzania bezpieczeństwem informacji w branży lotniczej.

Ma na celu ustanowienie najlepszych praktyk w zapewnieniu spójności informacji oraz zmniejszenie nakładów związanych z audytem dla zainteresowanych stron. Ma również na celu dostarczenie dodatkowych wytycznych do Part-IS: Acceptable Means of Complince (AMC) & Guidance Materials (GM). Rozporządzenie Part IS jest obowiązujące dla DOA, POA, lotnisk i operatorów lotniskowych od 16.10.2025. Dla Władzy Lotniczej i pozostałych organizacji lotniczych od 22.02.2026 roku.

Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, świadczenie usług cyfrowych i kluczowych poprzez osiągnięcie poziomu bezpieczeństwa systemów informacyjnych do świadczenia usług oferowanych, zapewnienie obsługi zgodnie z obowiązującymi ustawami w ww. zakresie przez CSIRT GOV, MON, NASK.

Cyberbezpieczeństwo staje się priorytetem dla gospodarki narodowej, stanowi kluczowy temat, który obejmuje w całej branży ochronę systemów informatycznych portów lotniczych, przewoźników lotniczych, danych pasażerów, krytycznej infrastruktury lotniczej przed cyberzagrożeniami. Świat lotniczy we wszystkich aspektach wszedł w nowoczesne technologie informatyczne, a co za tym idzie, również w zagrożenia cybernetyczne. Według prognoz Międzynarodowego Zrzeszenia Przewoźników Powietrznych IATA transport lotniczy kreuje i przyspiesza procesy globalizacji. Wraz z technologią informacyjną określany jest mianem fundamentu i filaru podstawy, przy czym sam tym procesom podlega. Nowe technologie wiążą się z koniecznością zabezpieczenia przed cyberatakami. Społeczne synonimy definiowane jako branżowy zestaw wartości, odczuć, przekonań, a także zachowań organizacji odnoszących się do problemu bezpieczeństwa. Muszą się opierać na wysokim poziomie szacunku i zaufania na linii przełożony–podwładny. Działania te powinny sprowadzać się do pragmatycznych formuł w zakresie kultury elastyczności, sprawiedliwego traktowania, raportowania i uczenia się.

Priorytetyzacja działań prewencyjnych pozwala na lepsze przewidywanie przyszłych zagrożeń, efektywniejszą reakcję już na zaistniałe zdarzenia i incydenty. Poznanie przeciwnika jest fundamentem nowoczesnej cyberobrony.

Sytuacja geopolityczna w transporcie lotniczym

Komunikacja lotnicza jest najdynamiczniej rozwijającą się gałęzią transportu. Latanie stało się normalną częścią naszego życia. Szacuje się, iż zaledwie 5% światowej populacji kiedykolwiek leciało samolotem, z usług transportu lotniczego korzysta coraz więcej podróżnych. Globalny rozwój transportu lotniczego determinowany jest przemianami i trendami w rozwoju światowej gospodarki przy przewidywanym wzroście ruchu o 4,3% rocznie do roku 2035. Lotniska bez stanowisk check-in? Zdalne wieże zarządzania ruchem lotniczym na lotniskach? W przyszłości czekają nas orbitalne loty pasażerskie, czy loty statkami autonomicznymi. Dziś kupno biletu załatwiamy kliknięciem w smartfonie. Korzystając z usług z portu lotniczego za które zapłacimy kartą bądź blikiem. Odprawę bagażu na niektórych lotniskach możemy dokonać w domu. Na lotnisku przechodzimy przez automatyczną bramkę. W samolocie zakładamy słuchawki i surfujemy w internecie. Jedynie dobra organizacja jest w stanie dać dobre produkty i usługi. Stwarza się konieczność wypracowania i stosowania działań globalnych w budowaniu strategii i bezpieczeństwa personalnego w sektorze branży lotniczej. Liczba wszystkich lotów na całym świecie w 2024 roku wyniosła około 100 mln, co oznacza wzrost o 4,3% do roku 2023. ACI (Airports Council International, Międzynarodowe Zrzeszenie Portów Lotniczych) jest organizacją obejmującą 2181 lotnisk w 170 krajach i, według analiz przeprowadzonych, wskazuje, że pierwsze 10 największych lotnisk odpowiada za 9 procent globalnego ruchu lotniczego, przy czym prym wiodą lotniska USA, takie jak Hartsfield-Jackson w Atlancie, Chicago-O'Hare i Dallas. Fort Worth (Airports Council International, 2025). W Europie znajduje się londyńskie Heathrow. Pod względem największego ruchu towarowego znajdują się lotniska w Hongkongu, Szanghaju oraz Memphis w amerykańskim stanie Tennessee. Szacuje się, że wolumen ładunków przewożonych drogą lotniczą wzrósł o 8,4% do 124 mln ton. Lotnisko Szanghaj Pudong awansowało z 21 pozycji w 2023 r. na dziesiątą pozycję w rankingu 2024 roku. Przewidywany wzrost w globalnym ruchu pasażerskim w 2030 roku przekroczy

12 mld pasażerów, natomiast w 2042 roku ma osiągnąć 19,5 mld, co oznacza dwukrotny wzrost w porównaniu z obecnym rokiem, spowodowany rozwojem międzynarodowych rynków w regionie Azji i Pacyfiku oraz Bliskiego Wschodu. Jesteśmy połączeni systemami satelitarnymi w każdej dziedzinie życia. Dla przykładu, w 2018 roku linie lotnicze British Airways zostały ukarane rekordową grzywną w wysokości 183 mln funtów za wyciek danych około 500 tys. pasażerów (Sweney, 2019). Podatność amatorskich i profesjonalnych systemów na zakłócenia czy zakłócanie sygnału GNSS jest faktem. Wykrywanie anomalii GNSS – jammingu i spoofingu – stało się najbardziej odczuwalne w obszarach działań wojennych i terytoriach okupowanych i zaczepnych. Działania poprzez ataki nie są wykonywane na oślep, rozszerzone o ataki jednostkowe, kierunkowe, stają się coraz bardziej wyrafinowane, a obszar FIR Warszawa stał się cywilnym polem walki bez strzelania. Zakłócenia częstotliwości nawigacji satelitarnych, zgodnie z ITU (International Telecommunication Union), nie powinny być zakłócane, a stają się coraz bardziej agresywne i bezwzględne. Przeloty w rejonie tych obszarów stają się niemożliwe z powodu zakłóceń generowanych przez sygnały również naziemne.

Techniki ogólnego zakłócania

Atak jest zdefiniowany jako próba zniszczenia, kradzieży czy uzyskania nieautoryzowanego dostępu czy użycia aktywów (Krawiec, 2019). Cyberprzestępcy wykorzystują różne techniki, aby zdobyć dane do logowania i inne wrażliwe informacje. Ewoluujące taktyki, techniki i procedury stosowane przez cyberprzestępców w działaniu różnorodnych grup przestępczych działających na skalę globalną obejmują zarówno narzędzia, złośliwe oprogramowanie, jak i sposoby poruszania się w sieci. Cyberprzestępcy stosują szeroką gamę taktyk, aby wyłudzić od użytkownika dane dotyczące logowania do kont, nakłonić użytkownika do udostępnienia informacji, pobrania szkodliwych plików. Wzrost złośliwych reklam jest jednym z niepokojących trendów, ponieważ atakujący ukrywają złośliwe oprogramowanie w reklamach internetowych w popularnych wyszukiwarkach – to malvertising polegający na umieszczeniu złośliwego oprogramowania. W przeciwieństwie do ataków phishingowych, które wykorzystują wiadomości e-mailowe, złośliwe reklamy mogą pojawiać się w standardowych wynikach wyszukiwania,

co sprawia, że czujnym okiem użytkownika trudno je wykryć. Umożliwia to pominięcie typowych środków bezpieczeństwa i rozprzestrzenianie złośliwego oprogramowania. Słabe dane uwierzytelniające pozostają głównymi metodami nieautoryzowanego dostępu do sieci. Staje się kluczowym elementem w budowaniu proaktywnych strategii obronnych przez współczesne organizacje. Raport Malwarebytes ujawnił 42% wzrost incydentów związanych ze złośliwym oprogramowaniem tylko w USA, przy czym ataki były wymierzone w popularne marki do wyłudzenia informacji czy dostarczenia złośliwego oprogramowania (Greenberg, 2024). Przestępcy umieszczają złośliwe reklamy, które nie są do odróżnienia od legalnych, co utrudnia ich identyfikację.

Źródłem największej liczby zakłóceń o małej mocy i na niewielką skalę geograficzną są „chuligani elektroniczni", jak złodzieje najczęściej drogich samochodów, kierowcy samochodów ciężarowych, taksówkarze, by nie było ich widać w systemie, hakerzy oraz służby – nie mówią, do jakich celów. Stosują anteny kierunkowe do zakłócania poszczególnych czy wybranych sygnałów samolotów. Przy użyciu dużych mocy ukierunkowane zasięgi mają kilkaset kilometrów. Większość ataków nie dociera do powierzchni ziemi. Atakują wszystkie konstelacje. Włamują się do cywilnej sieci AFTN; widzą, wiedzą, co i kiedy leci. Zakłócenia stały się poważnym problemem bezpieczeństwa lotniczego i geopolitycznego w Europie. Najwięcej incydentów odnotowuje się na wschodniej granicy NATO, na Bliskim Wschodzie oraz na szlakach morskich. Lotnictwo cywilne korzysta z urządzeń VOR, ILS, INS (Inertial Navigation System) / DME oraz procedur awaryjnych w ograniczaniu ryzyka zakłóceń. Europa poprzez wdrażanie OSNMA (Open Service Navigation Message Authentication) w Galileo wzmacnia raportowanie i koordynację działań.

Cyberatak na międzynarodowego dostawcę oprogramowania lotniskowego, firmę Collins, obsługującą system boardingu i odprawy bagażowych, na lotniskach europejskich (Berlin, Bruksela, Londyn, Heathrow) spowodował, że część rejsów została opóźniona lub odwołana – trzeba było przejść na system ręczny „papierzany". Cyberatak na oprogramowanie jest testem ciągłości działania lotnisk w momencie awarii krytycznego elementu (Associated Press, 2025).

Już uzależniliśmy się od urządzeń IT, w tym satelitarnych, co skutkuje atakami na wiele systemów, a co w przyszłości może spowodować skutki

katastrofalne. „System of systems", kontynuując monitorowanie anomalii GNSS (Global Navigation Satellite System) z systemów monitorowania w powietrzu, na ziemi oraz transponderów, umożliwia skuteczne zdiagnozowanie technik i źródeł jammingu i spoofingu (Narkiewicz, 2007).

Spoofing to wirtualne przemieszczanie samolotu w powietrzu przy wykorzystaniu agresywnej techniki „jammowania" w pierwszej kolejności, a następnie podłożenia sfałszowanego sygnału satelitarnego, mówiąc o manipulowaniu sygnałem tak, aby zmienić pozycję i czas. Jest to subiektywne i trudne w pierwszym momencie do jednoznacznej identyfikacji – ikonka ilustrująca liczbę satelitów będzie najprawdopodobniej biała przy zmniejszeniu dostępnych satelit. Pierwsze takie skutki załogi odczuły w trakcie przelotu w rejonie Bliskiego Wschodu. Urządzenia pokładowe przekierowały samolot w rejon Iranu – góry na północ od Teheranu. Spoofing komunikacji VHF, z wykorzystaniem AI do naśladowania służb ATC i pilotów jest zagadnieniem coraz „modniejszym". Natomiast jamming to zakłócanie sygnału. Wystarczy tylko chwila, aby znaleźć się w zainfekowanym obszarze, a powrót do normalności może zająć minutę, co w trakcie lotu – 60 sekund – jest bardzo długim czasem. Nieodpowiedzialnych bawiących się, świadomych i nieświadomych swoich działań, bawiących się tanimi jammerami. Również przy drogach ekspresowych i autostradach. Ataki napędzające falę cyberwymuszeń to:

- Ransomware, polegający na szyfrowaniu danych ofiary i żądaniu okupu za ich odblokowanie, pozostaje najpoważniejszym, najbardziej destrukcyjnym zagrożeniem cybernetycznym, napędzanym przez innowacyjne działania cyberprzestępców, zakłócając krytyczne usługi pasażerskie. Pociąga za sobą konsekwencje regulacyjne, reputacyjne, operacyjne. Przykład awarii na lotniskach pokazuje, jak wiele mamy jeszcze do zrobienia. Zakłócenia świadczą o powszechnym uzależnieniu od dostawcy usług. Odprawy i nadawanie bagażu, stosowane przez linie lotnicze, lotniska, zostały zaszyfrowane przez oprogramowanie ransomware. Pociągnęło to za sobą konsekwencje operacyjne poprzez wyłączenie automatycznych punktów odprawy i systemów nadawania bagażu. Lotniska odwołały dziesiątki lotów i stanęły w obliczu utraty reputacji, kolejek i niepewności; podkreśliły bezpośredni wpływ

incydentów cybernetycznych na biznes. Wstępne dochodzenia wskazują, że jest to kampania ransomware motywowana finansowo.

- Ransomware-as-a-Service (RaaS) – model ten znacząco obniżył barierę wejścia dla atakujących, nieposiadających zaawansowanych umiejętności technicznych w tworzeniu złośliwego oprogramowania, działających na zasadzie podziału zysków poprzez oferowanie gotowego do użycia zestawu narzędzi do infiltracji danych.
- RansomHub – oferująca swym partnerom intratne warunki podziału zysków zapłaconego okupu, co sprzyja pojawianiu się licznych nowych grup ransomware.

Stojący za atakami cyberprzestępcy, stosując bardziej wyrafinowane metody wymuszania, działają w zorganizowany sposób, wykorzystując modele biznesowe, specjalizując się w poszczególnych atakach, co zwiększa ich efektywność i skalę działania. Poprzez zastosowanie sztucznej inteligencji ataki stały się bardziej wyrafinowane, a inwestorzy inwestują w nowe technologie, a przy tym dywersyfikują swoje zyski w inwestycjach legalnych i półlegalnych, co utrudnia władzom wykrycie takich działań. Kluczowe pozostają budowa odporności oraz plan odzyskiwania danych. Firmy muszą dostosowywać strategie cyberbezpieczeństwa organizacji do rozwiązań predykcyjnych i zarządzania ryzykiem.

Czynnik ludzki w organizacjach, w tym kadra zarządzająca, partnerzy biznesowi, służby lotniskowe, pozostaje jednym z najsłabszych i najczęściej atakowanych ogniw w systemach bezpieczeństwa informatycznego. Błędy czy też celowe złośliwe działania pracowników przyczyniły się do około 60% wszystkich potwierdzonych naruszeń bezpieczeństwa. Nieostrożne kliknięcia w wiadomościach phishingowych stwarzają podatność na wyrafinowane techniki inżynierii społecznej – vishing, protexting, jak też błędne wysłanie wrażliwych danych do nieuprawnionych odbiorców, stosowanie słabych haseł, nieprzestrzeganie polityk bezpieczeństwa. Powyższe zagrożenia mogą być przypadkowe, wynikające z braku wiedzy, niedbalstwa, pośpiechu, a może celowe działanie pracownika motywowane chęcią zemsty, na zlecenie konkurencji, obcego wywiadu, aby osiągnąć zysk finansowy. Legalne konta pracownicze przejęte przez zewnętrznych hakerów w wyniku phishingu lub malware'u są szczególnie podstępne i trudne do wykrycia, ponieważ omijają środki bezpieczeństwa, jak systemy IDS/IPS, dzięki

posiadaniu zaufanego dostępu do systemów w organizacji. Szkolenia z zakresu cyberbezpieczeństwa są skutecznym środkiem zaradczym, zarówno teoretycznym, jak i praktycznym, dotyczące rozpoznawania ataków i prób phishingu, są skłonni do prawidłowego zidentyfikowania i zgłaszania takich prób służbom bezpieczeństwa. Budowanie kultury bezpieczeństwa jest kluczowym elementem w redukcji ryzyka i w podnoszeniu świadomości pracowników organizacji lotniczej.

Współczesna cyberprzestępczość staje się coraz bardziej podzielona na specjalizację oraz tworzenie grup do przeprowadzania określonych typów ataków – phishing kits, exploit kits. Wymusza to stosowanie strategii bezpieczeństwa, które adresują nie tylko etap końcowy ataku. Konieczne stają się aktywne monitorowanie aktywności dostępu, analiza trendów, które dadzą obraz złożoności ekosystemu, przewidywalność we wskazaniach nowych wektorów zagrożeń cybernetycznych (Krawiec, 2019; Syta, 2025).

Nie można wykluczyć również degradacji sygnału GNSS (Global Magnetic Storm Index) spowodowanej czynnikami naturalnymi, tak jak wybuchami na Słońcu – wysokim indeksem Kp, niekorzystne ustawienie konstelacji, odbiciowość sygnału nawigacji satelitarnej od przeszkód, załamanie sygnału od przeszkód, zakłócenia przemysłowe.

Kolejnym problemem w przestrzeni powietrznej nad lotniskami są niezidentyfikowane drony zmuszające zarządzających do podjęcia działań w odpowiednich procedurach bezpieczeństwa, w tym do tymczasowego zamknięcia lotnisk. Lotnictwo w dobie wojny hybrydowej stawia wyzwania dla bezpieczeństwa lotnictwa i wymaga weryfikacji procedur. Trzeba balansować między neutralizacją dronów a zachowaniem bezpieczeństwa lotów, co wiąże się z potencjalnymi opóźnieniami i koniecznością zmian w planach pasażerów.

Monitorowanie anomalii GNSS

Postęp cyfrowy naraża sektor na cyberzagrożenia ze wszystkich stron, co ma wpływ na reputację, ciągłość usług, bezpieczeństwo ludzi i obiektów, a w ostateczności na finanse. Raporty CERT.PL pokazują, że liczba ataków odnotowanych w polskiej cyberprzestrzeni drastycznie wzrasta, co stanowi wyzwanie i wiąże się z pojawiającymi się wyzwaniami, takimi jak przeciwdziałanie (CERT Polska, 2025). Zagrożenia dla bezpieczeństwa w cyberprzestrzeni wpływają na działania państwa, dając możliwość wprowadzenia stanów

nadzwyczajnych (Jelonek, 2024). Aby skutecznie móc monitorować, jak też interpretować anomalie, należy wykorzystać w tym celu czujniki naziemne umieszczone nad powierzchnią, a dane z ADS-B poprzez czujniki umieszczone w statkach powietrznych są bardzo pomocne i wiarygodne. Skuteczność zakłócania na ziemi jest ograniczona przede wszystkim rzeźbą terenu, lasami i budynkami. Dużą liczbę czujników i dysponując algorytmami multilateracji, możemy precyzyjnie określić miejsce oraz sposób przemieszczania się źródła zakłóceń. Przeciwnik sprytnie wykorzystuje swoją wirtuozerię i kunszt, przebiegłość i bezwzględność działania, tworząc nowy rozdział wojny hybrydowej. Inteligentny spoofing da się wdrożyć na Bliskim Wschodzie na kilkusetkilometrowym obszarze, a co gdyby takie niepożądane działanie działo się w miejscu o olbrzymim natężeniu ruchu lotniczego – jakie konsekwencje.

Używając merytorycznych przesłanek, wiemy, że temat zakłóceń sygnałów GNSS i spoofingu jest coraz częściej powtarzającym się. Załogi tracą integralność danych GNSS, raportując zagregowane anomalie w określaniu pozycji i integralności danych. Różnorodność standardów i skomplikowany system przy niejednoznacznym systemie interpretacji powoduje, że wyciągnięcie wniosków nastręcza trudności, wskazując na trzy typy wskaźników jakości danych dla systemu ADS-B:

1. Wskaźnik niepewności – wartości parametrów wskazują, że co najmniej 95% pomiarów mieści się w dopuszczalnych granicach niepewności,
2. Wskaźnik dokładności – zastępują wskaźnik niepewności, również wskazują, że co najmniej 95% pomiarów mieści się w dozwolonych granicach dokładności,
3. Wskaźnik integralności – zastępuje wskaźnik niepewności z wersji 0.

W zależności od specyfiki urządzeń, standardów ADS-B, od sytuacji, czy od fazy lotu. Dane oparte na błędach pozycji – (NIC – Navigational Integrity Category), (NACp – Navigation Accuracy Code for position) oraz NUCr, NACv muszą być analizowane z (SIL – Source Integrity Level) w kontekście (ESASSP – EUROCONTROL Specification for ATM Surveillance System Performance). Z danych ADS-B bez dogłębnej analizy stwierdzamy, że coś jest nie tak i wymaga szczegółowej dogłębnej analizy. Dla załóg lotniczych są publikowane depesze NOTAM FIR EPWW – „ANOMALIES IN GNSS SIGNAL MAY BE EXPECTED IN AREA NORTH OF LINE, DEFINED

BY POINTS: 1….N….E, 2….N….E." Zgłoszenia zdarzeń lotniczych związanych z zakłóceniami sygnału GPS w różnych obszarach geograficznych i przedziale czasowym należy raportować w ECCAIRS. Wykorzystanie luk prawnych i działanie za pośrednictwem pozorantów to praktyki stosowane w utrudnianiu działań organów bezpieczeństwa.

W celu zapewnienia cyberbezpieczeństwa stosuje się testy penetracyjne systemów lotniczych w celu wykrycia słabości polegających na symulacji ataków w kontrolowanych warunkach, aby wykryć i naprawić słabości, mając na uwadze aspekty tego procesu, jak:

1. Cel testów penetracyjnych – w identyfikacji słabości systemów, przeprowadzeniu oceny odporności na potencjalne ataki czy zagrożenia, dla wzmocnienia zabezpieczeń przed rzeczywistymi atakami;
2. Zakres testów – dla zarządzania lotami systemów nawigacji i komunikacji powiązany infrastrukturą sieci IT z uwzględnieniem systemów cyberbezpieczeństwa i ochrony;
3. Etapy testów – obejmujące planowanie w tym zakresie i celach oraz metodologię, jak również zbieranie informacji o systemach i infrastrukturze, wykrywanie słabości z użyciem narzędzi do identyfikacji luk. Prowadzenie analizy i raportowanie wyników w tym rekomendacje naprawcze;
4. Metody i narzędzia – z wykorzystaniem ręcznych i automatycznych technik penetracyjnych w symulacji ataków typu phishing, malware, DDoS (Distributed Denial of Service), na poziomie aplikacji i urządzeń;
5. Bezpieczeństwo i zgodność – współpraca z odpowiednimi organami w zapewnieniu minimalizacji ryzyka zakłóceń operacyjnych za pomocą testów przez certyfikowanych specjalistów;
6. Działania naprawcze, wnioski – wdrażanie rekomendowanych zabezpieczeń przez regularne testy, audyty, monitorowanie postępów, analizę wyników.

Szczególne warunki muszą spełniać osoby zajmujące kierownicze stanowiska w organizacjach lotniczych w obszarach wysokiego ryzyka w sektorze bezpieczeństwa – ochrony. Decyzje w szczególnie trudnych warunkach będą podejmowane pod dużą presją, w stresie, co stanowi istotną cechę przywództwa zorientowanego na zadanie (Klich, 2011; Jelonek, 2024).

Podsumowanie

Podstawą cyberbezpieczeństwa jest czynnik ludzki mający wiedzę i praktykę przekładające się na doświadczenie. Mimo rosnących nakładów, nowych regulacji, coraz doskonalszych narzędzi, rosnącej świadomości potrzeby ochrony przed cyberatakami, trudno się oprzeć wrażeniu, że w przyszłości w znaczący sposób wzrośnie ryzyko przetwarzania informacji. Rosnące światowe wydatki na IT wskazują, że w coraz większym stopniu uzależniliśmy się od technologii teleinformatycznych. Dlatego organizacje lotnicze muszą podjąć konkretne kroki w celu zwiększenia liczby personelu posiadającego wiedzę z zakresu cyberbezpieczeństwa i lotnictwa poprzez ciągłą edukację, a poprzez innowacyjne sposoby łączenia ścieżek kariery w dziedzinie technologii informacyjnych z karierą w lotnictwie dla rozwoju umiejętności potrzebnych dla cyberbezpieczeństwa w łączeniu branż lotnictwa cywilnego, obronnego z pozostałymi.

Nie ma dnia ani tygodnia, abyśmy nie byli zaskoczeni czymś nowym. Ataki hakerskie na lotniska poprzez włamania do punktów odprawy bagażu czy wyciek danych personalnych pasażerów na różne sposoby i metody, przy tak rozbudowanej technice, wykorzystujące wszelkie oficjalne i nieoficjalne metody, w tym dostęp do powszechnie stosowanych urządzeń i sieci, muszą być na wszechmiar kontrolowane i zabezpieczone. W obliczu wyzwań kluczowe pozostają ciągłe doskonalenie rozwiązań bezpieczeństwa i płynność ruchu lotniczego.

Standardy cyberbezpieczeństwa w dobie XXI wieku mają szerokie znaczenie w dzisiejszych firmach branży lotniczej, które wykorzystują technologię IT do prowadzenia operacji w sieci. Nie wystarczy umieścić cyberbezpieczeństwo w ustawie o IT, ale aby zmaksymalizować swoje zyski, korporacje wykorzystują technologię w działalności operacyjnej, która musi być chroniona we wszystkich aspektach działalności biznesowej. W wielu przypadkach różniące się pod wieloma względami standard bezpieczeństwa cybernetycznego nie jest optymalny dla zmniejszenia ryzyka. Należy zastanowić się, w jaki sposób przestrzegać przepisów z cyberbezpieczeństwa. Cyberatak na system boardingu i odpraw bagażowych dowodzi, jak ważne jest tworzenie i testowanie procedur awaryjnych. Należy utrzymywać podręczniki ręcznej odprawy i nadawania bagażu na wypadek awarii IT. Rezerwowy dodatkowy

personel w celu zmniejszenia wąskich gardeł. Weryfikacja segmentacji sieci i plany ograniczania incydentów dla połączeń innych firm. Przeprowadzać ćwiczenia odporności okresowe na całym lotnisku, symulując ataki ransomware'a. Przetestować koordynację pod presją, uwzględniając linie lotnicze, obsługę naziemną. Usprawnić udostępnianie informacji w czasie rzeczywistym za pośrednictwem kanałów społecznościowych, oznakowań, aplikacji. Weryfikacja sieci oraz plany ograniczania incydentów.

Przemysł lotniczy jest kluczowy dla gospodarki narodowej, a inwestycje w rozwój technologii i innowacji są niezbędne, aby sprostać rosnącym wymaganiom rynku oraz wyzwaniom związanym ze zrównoważonym rozwojem branży lotniczej. Załącznik 19 ICAO wskazuje nam, że bezpieczeństwo w lotnictwie jest stawiane na pierwszym miejscu. Eksperci wskazują, że aby uchronić się przed utratą danych, należy zachować zdrowy rozsądek i nie pozwolić wywierać na siebie presję. Weryfikować tożsamość autora wiadomości, próbując skontaktować się za pomocą innego urządzenia. Dyskusje w zróżnicowanym i wielokulturowym środowisku na temat „Flying Tomorrow: Enhancing Aviation Security for a Sustainable Future", przygotowując się do rozmów na temat ewolucji bezpieczeństwa lotniczego. Polski rząd zwiększył do rekordowej kwoty 4 mld zł budżet na cyberbezpieczeństwo w 2025 roku.

Literatura

1. Airports Council International. (2025). T*he busiest airports in the world defy global uncertainty and hold top rankings*.
2. Associated Press. (2025). *Cyberattack disrupts check-in systems at major European airports*. AP News. Pobrane z: https://apnews.com/article/29b6d890baf7ac3a22f0f2b2f169b890 (dostęp: 24.02.2026).
3. CERT Polska. (2025). *Raport roczny z działalności CERT Polska w 2024 roku*. CERT Polska.
4. Greenberg, A. (2024). *Malicious ads in search results are driving new generations of scams.* Wired. Pobrane z: https://www.wired.com/story/malicious-ads-in-search-results-are-driving-new-generations-of-scams (dostęp: 24.02.2026).
5. International Civil Aviation Organization. (2022). *Aviation cybersecurity strategy*.

6. Jelonek, A. (2024). *Współczesne zagrożenia bezpieczeństwa*. Akademia Sztuki Wojennej.
7. Klich, E. (2011). *Bezpieczeństwo lotów.* Instytut Technologii Eksploatacji – PIB.
8. Konwencja o międzynarodowym lotnictwie cywilnym, podpisana w Chicago dnia 7 grudnia 1944 r. (1944).
9. Komisja Europejska. (2022). *Rozporządzenie delegowane Komisji (UE) 2022/1645 z dnia 14 lipca 2022 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 w odniesieniu do wymagań dotyczących zarządzania ryzykiem związanym z bezpieczeństwem informacji*. Dz.Urz. UE L 248 z 26.09.2022.
10. Komisja Europejska. (2023). *Rozporządzenie wykonawcze Komisji (UE) 2023/203 z dnia 27 października 2022 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 w odniesieniu do wymagań dotyczących zarządzania ryzykiem związanym z bezpieczeństwem informacji*. Dz.Urz. UE L 31 z 2.02.2023.
11. Krawiec, J. (2019). *Cyberbezpieczeństwo: Podejście systemowe*. Oficyna Wydawnicza Politechniki Warszawskiej.
12. Narkiewicz, J. (2007). *GPS i inne satelitarne systemy nawigacyjne*. Wydawnictwa Komunikacji i Łączności.
13. Parlament Europejski i Rada UE. (2022). *Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148.* Dz.Urz. UE L 333 z 27.12.2022, s. 80-152.
14. Rada Ministrów. (2019). *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024.*
15. Sweney, M. (2019). *BA faces £183m fine over passenger data breach*. The Guardian. Pobrane z: https://www.theguardian.com/business/2019/jul/08/ba-fine-customer-data-breach-british-airways (dostęp: 24.02.2026).
16. Syta, J. (2025). *Zarządzanie cyberbezpieczeństwem*. Wydawnictwo Naukowe PWN.
17. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r. poz. 20).
18. Żylicz, M. (2002). *Prawo lotnicze międzynarodowe, europejskie i krajowe*. Wydawnictwo Prawnicze LexisNexis.