Ewa Dudek[1], Michał Kozłowski[2]
Politechnika Warszawska, Wydział Transportu

Zagadnienie bezpieczeństwa zintegrowanych informacji operacyjnych w porcie lotniczym

1. WPROWADZENIE

W elemencie infrastruktury transportowej, omawianym w tym artykule – w porcie lotniczym zidentyfikować można szereg służb operacyjnych (tj.: zarządzającego portem lotniczym, służby żeglugi powietrznej, agentów obsługi naziemnej, przewoźników lotniczych, i innych) oraz liczne systemy informatyczne (lub zinformatyzowane) wykorzystywane przez te służby (m.in.: Flight Information Display System – FIDS, Baggage Handling System – BHS, Departure Control System – DCS, i inne). Głównym celem eksploatacji portu lotniczego jest obsłużenie ruchu statków powietrznych oraz pasażerów i ich bagażu, jak również poczty i ładunków. Aby zadanie to mogło zostać należycie zrealizowane konieczna jest współpraca wszystkich służb operacyjnych, wspieranych przez zainstalowane systemy. Warto więc rozważyć zagadnienie integracji informacji generowanych, przetwarzanych i przesyłanych pomiędzy tymi służbami w określonych systemach (o różnych formatach i strukturach oraz zabezpieczeniach), a co za tym idzie problem skuteczności i aktualności wymiany informacji pomiędzy tymi wszystkimi służbami zaangażowanymi w procesy eksploatacji portu lotniczego, jak również aspekt stopnia integracji i poziomu bezpieczeństwa przesyłanych danych. Zagadnienie bezpieczeństwa danych operacyjnych ma szczególne znaczenie w przypadku integracji danych na potrzeby wykorzystania w projektach systemów zarządzania operacyjnego A-CDM oraz AMAN/DEMAN, których celem jest podnoszenie poziomu bezpieczeństwa i punktualności oraz obniżanie kosztów i negatywnego oddziaływania transportu lotniczego na środowisko.

W kolejnych rozdziałach zaprezentowane i omówione zostaną atrybuty bezpieczeństwa informacji oraz przedstawiona zostanie koncepcja systemu wspólnego podejmowania decyzji w porcie lotniczym (A-CDM). Podjęta będzie również próba określenia właściwego poziomu bezpieczeństwa danych lotniczych.

2. BEZPIECZEŃSTWO DANYCH/INFORMACJI

Bezpieczeństwo danych i informacji można określić na wiele sposobów. Norma ISO/IEC 27001 [4] definiuje jedynie bezpieczeństwo informacji, jako zachowanie poufności, integralności i dostępności informacji (z zastrzeżeniem, iż dodatkowo mogą być brane pod uwagę inne własności takie jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność). Przy czym wg [4] poufność to właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom. Integralność to właściwość polegająca na zapewnieniu dokładności i kompletności aktywów. Zaś dostępność rozumiana jest jako właściwość bycia dostępnym i użytecznym na żądanie upoważnionej osoby (podmiotu lub ustalonego procesu).

Bezpieczeństwo danych wg [1, 5] polega na ich ochronie, czyli zabezpieczeniu przed nieuprawnionym lub nieprawidłowym, przypadkowym bądź umyślnym ujawnieniem, modyfikacją lub zniszczeniem. Wyróżnia się cztery podstawowe atrybuty bezpieczeństwa danych:

- poufność,
- integralność,
- dostępność,
- spójność.

[1]emdudek@gmail.com
[2]m.kozlowski@wt.pw.edu.pl

Poufność oznacza niedostępność treści zawartych w danych dla wszystkich podmiotów nieuprawnionych do jej odczytania. Danym, których naruszenie poufności byłoby szczególnie niewskazane i kosztowne, przypisywany jest odpowiednio wysoki poziom bezpieczeństwa (poufne, tajne, ściśle tajne, itp.). Bezpośrednim sposobem zapewnienia poufności jest szyfrowanie danych. Procedury uwierzytelniania, ograniczenia uprawnień dostępu czy ograniczanie fizycznego dostępu do systemu komputerowego są środkami pośrednim, prowadzącymi do osiągnięcia tego celu. Pomimo stosowania różnego rodzaju środków, zapewniających poufność, istnieje niebezpieczeństwo przypadkowego lub celowego jej naruszenia. W związku z tym system ochrony powinien nie tylko zapewniać poufność, lecz także gwarantować możliwość wykrycia prób i przypadków jej naruszenia.

Integralność danych oznacza, że dane nie zostaną w żaden nieuprawniony sposób zmienione, a tym samym ich stan pozostanie zgodny z wymaganym i oczekiwanym stanem właściwym. Integralność danych może być naruszona przez nieuprawnionego użytkownika, błędy i zaniedbania popełnione przez użytkownika upoważnionego, a także w wyniku awarii, zakłóceń w transmisji, błędów w oprogramowaniu, działania wirusów, itp. Nieupoważniona modyfikacja nie musi wiązać się z naruszeniem poufności danych. Podobnie jak poufność, integralność musi być zapewniona podczas przetwarzania, przechowywania i przesyłania informacji. Integralność danych zapewnia się stosując funkcje skrótu, a w pewnym stopniu także kody wykrywające i korygujące błędy. W sposób pośredni można przyczynić się do osiągnięcia tego celu poprzez stosowanie procedur uwierzytelniania, ograniczenia uprawnień dostępu, ograniczenie fizycznego dostępu do systemu komputerowego, stosowanie metod zwiększających niezawodność sprzętu i tolerancję na błędy. Konieczne może być także zagwarantowanie możliwości wykrycia każdego przypadku lub próby naruszenia integralności danych.

Dostępność oznacza niczym nieograniczoną możliwość korzystania z danych przez uprawnionych do tego użytkowników. Dostępność danych może być naruszona przez nieupoważnionego użytkownika, błędy popełniane przez użytkownika upoważnionego, a także w wyniku awarii, zakłóceń w transmisji, błędu oprogramowania, przeciążenia systemu. Wstrzymanie przez nieupoważnionego użytkownika dostępu do zasobów może stanowić wstęp do ataku na poufność i integralność danych. Pożądane może być więc zapewnienie możliwości wykrycia każdego przypadku nieuzasadnionej odmowy dostępu do danych.

Dostępność zapewnia się poprzez stosowanie odpowiednio zabezpieczonych systemów operacyjnych, stały nadzór nad stopniem wykorzystania zasobów, stosowanie systemów sterowania ruchem sieciowymi obciążeniem serwerów, stosowanie metod zwiększających niezawodność sprzętu i tolerancję na błędy.

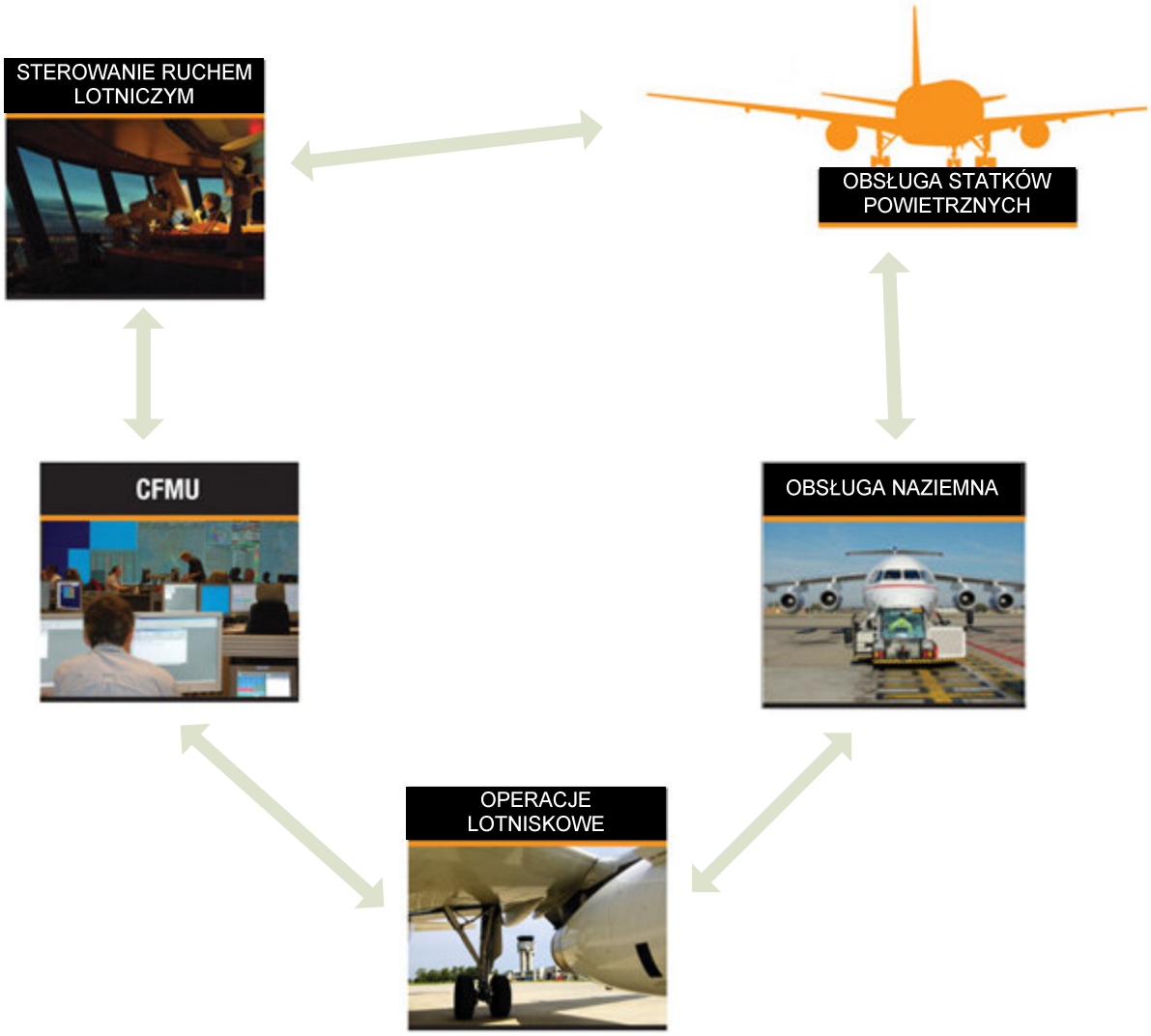
Spójność danych odnosi się przede wszystkim do pakietów danych i oznacza konieczność spełnienia przez każdy element pakietu danych zbioru warunków, sformułowanych w jego definicji. Warunki te zwane są warunkami spójności.

Istnieje związek między integralnością i spójnością danych, choć nie są to pojęcia tożsame. Niekiedy w sposób wyraźny mówi się tylko o trzech pierwszych aspektach bezpieczeństwa danych, traktując spójność, jako szczególny przypadek integralności. Podejście to jest więc tożsame z zaprezentowanym w normie ISO 27001 [4].

3. System wspólnego podejmowania decyzji w porcie lotniczym

Mając na celu zwiększenie stopnia dokładności, dostępności oraz zakresu informacji przekazywanych w portach lotniczych jak również zwiększenie poziomu bezpieczeństwa operacji, wykonywanych w ruchu lotniskowym, warto rozważyć koncepcję Systemu wspólnego podejmowania decyzji w porcie lotniczym. Koncepcja A-CDM (ang. Airport Collaborative Decision Making, pol. System wspólnego podejmowania decyzji w porcie lotniczym) narodziła się na początku lat 90-tych w Stanach Zjednoczonych z inicjatywy grupy przewoźników lotniczych. Inicjatywa ta wynikała ze stwierdzenia niedostatecznej wymiany informacji i współpracy operacyjnej pomiędzy zarządzającymi portami lotniczymi, służbami żeglugi powietrznej, agentami obsługi naziemnej i przewoźnikami lotniczymi. Koncepcja CDM została rozwinięta przez EUROCONTROL. Obecnie A-CDM definiowany jest [6] jako proces, w zakresie którego decyzje operacyjne, dotyczące systemu zarządzania przepływem ruchu lotniczego i przepustowością (ang. Air Traffic Flow and Capacity Management – ATFCM) w portach lotniczych, podejmowane są w oparciu

o interakcję pomiędzy zainteresowanymi, zaangażowanymi w działalność operacyjną i innymi podmiotami uczestniczącymi w ATFCM, a którego celem jest redukcja opóźnień, zwiększenie przewidywalności zdarzeń i optymalizacja wykorzystania zasobów. Wdrożenie A-CDM w głównych europejskich portach lotniczych jest jednym z zadań w ramach realizacji projektu utworzenia Jednolitej Europejskiej Przestrzeni Powietrznej (ang. Single European Sky – SES) [8], określonego w Pakiecie WP6 „Airport Operations" [9]. Z polskich lotnisk, jak dotąd, jedynie Lotnisko Chopina w Warszawie należy do grona wdrażających nawet nie pełny, a tylko tzw. „lokalny" system A-CDM.



Rys. 1. Ogólna koncepcja systemu A-CDM

Źródło: opracowanie na podstawie www.euro-cdm.org [7].

Podstawowe korzyści, wynikające z wdrożenia A-CDM w porcie lotniczym, to przede wszystkim korzyści operacyjne, wynikające ze zwiększenie stopnia dokładności, dostępności oraz zakresu informacji, takie jak:

- poprawa punktualności,
- redukcja kosztów ruchu naziemnego (skrócenie czasów kołowania – mniejsze zużycie paliwa), a tym samym ograniczenie negatywnego oddziaływania na środowisko,
- poprawa wykorzystania infrastruktury i zasobów ludzkich,
- redukcja strat slotów ATFM.

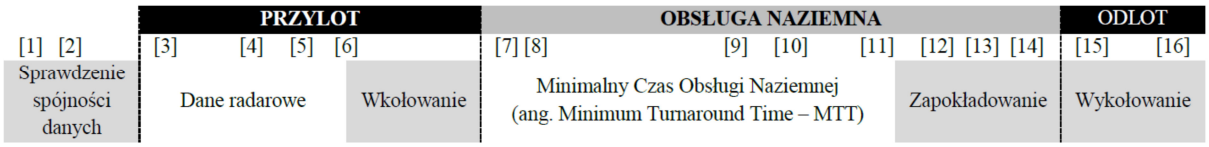
Drugim istotnym obszarem korzyści, wynikających z wdrożenia A-CDM, jest zwiększenie poziomu bezpieczeństwa operacji, wykonywanych w ruchu lotniskowym, poprzez:

- zapewnienie dostępu do kluczowych informacji i danych operacyjnych we właściwym czasie, a tym samym zwiększenie poziomu świadomości personelu i minimalizacja ryzyka nieintencjonalnego błędu ludzkiego,

- lepsze planowanie operacyjne, a tym samym ograniczanie potencjalnego przeciążenia zadaniami (skala, czas) personelu operacyjnego,
- lepsze planowanie przepływu ruchu, a tym samym minimalizacja ryzyka bezpieczeństwa w okresach dużego natężenia ruchu,
- minimalizacja liczby zmian operacyjnych, np. przydziału stanowisk postojowych, a tym samym ograniczenie liczby koniecznych przypadków realokacji zasobów (sprzętowych i ludzkich) agentów obsługi naziemnej,
- alarmy i ostrzeżenia o niespójności danych operacyjnych generowane w A-CDM.

Komponentami (i zasadami) A-CDM, są [6, 7]:

- **wymiana informacji**,
- podejście w oparciu o „16 kamieni milowych", wyznaczających w porządku chronologicznym poszczególne etapy realizacji operacji lotniczych (tj. etapy lotu i obsługi naziemnej) (Rys. 2.) i czas ich realizacji, i w których ustalane są wartości parametrów operacyjnych, determinujących punktualność realizacji procesów operacyjnych związanych z realizacją operacji lotniczych i obsługą przewozu lotniczego,
- zmienny czas kołowania,
- sekwencjonowanie przed odlotem,
- operowanie portu lotniczego w czasie ograniczeń przepustowości, wynikających np. z niekorzystnych meteorologicznych warunków wykonywania lotów,
- wspólne zarządzanie aktualizacją danych o przebiegu lotu – wymiana depesz FUM (ang. Flight Update Messages) oraz DPI (ang. Departure Planning Information).



[1] Złożenie Planu Lotu [FPL] (- 3 godz.).
[2] Przydzielenie ATFM-Slot (- 2 godz.).
[3] Start z lotniska odlotu / Actual Take-Off Time – ATOT.
[4] Aktualizacja danych radarowych.
[5] Podejście końcowe.
[6] Lądowanie / Actual Landing Time – ALDT.
[7] Wejście w bloki / Actual in Block Time – AIBT.
[8] Rozpoczęcie obsługi naziemnej / Actual Ground Handling Time – AGHT.
[9] Ostateczna aktualizacja / Target Off-Block Time – TOBT.
[10] Ustalenie czasu / Target Start up Approval Time – TSAT.
[11] Rozpoczęcie zapokładowania.
[12] Actual Ready Time – ARDT.
[13] Actual Start up Request Time – ASRT.
[14] Wydanie zezwolenia na start.
[15] Wyjście z bloku / Actual Off-Block Time – AOBT.
[16] Start /Actual Take-Off Time – ATOT.

Rys. 2. Schemat rozłożenia kamieni milowych w procesie A-CDM

Źródło: opracowanie własne na podstawie [6].

A-CDM został również wskazany [10] jako komponent rozszerzonych systemów zarządzania przylotami (ang. Arrival Management – AMAN) [11] i odlotami (ang. Departure Management – DMAN) [12], których algorytmy wykorzystują dane generowane, przetwarzane i gromadzone w A-CDM (rys. 2.). Tak więc, system A-CDM stanowi jedno ze źródeł danych dla zaawansowanych systemów zarządzania wykonywaniem operacji w ruchu lotniczym [3], co czyni istotnym zagadnienie zapewnienia bezpieczeństwa,

jakości, aktualności, poprawności, dokładności gromadzonych i przetwarzanych danych oraz ciągłości ich przesyłania.

Stąd wynika zainteresowanie autorów artykułu tymi zagadnieniami wraz z przedstawieniem koncepcji podejścia do zagadnienia zintegrowanego zapewnienia bezpieczeństwa lotniskowych danych operacyjnych.

4. BEZPIECZEŃSTWO OPERACYJNYCH DANYCH LOTNISKOWYCH

System A-CDM opiera się na wymianie i przetwarzaniu informacji. Aby zapewnić jego należyte funkcjonowanie, a tym samym prawidłowe funkcjonowanie innych powiązanych systemów zarządzania ruchem lotniczym, tj. AMAN i DEMAN, konieczne jest określenie poziomu bezpieczeństwa wykorzystywanych danych. Najbardziej naturalnym wydaje się szukanie rozwiązania tego zagadnienia w normie ISO 27001 [4], której już sam tytuł odnosi się do zagadnień bezpieczeństwa i zarządzania bezpieczeństwem informacji. Jednakże poza definicjami i zaleceniami dotyczącymi Systemu Zarządzania Bezpieczeństwem Informacji, norma ta nie określa żadnych algorytmów i miar liczbowych dla danych lotniczych i operacyjnych. Wymagania w tym zakresie określone są w załącznikach 14 [14] i 15 [15] do Konwencji o międzynarodowym lotnictwie cywilnym. Załączniki te określają pojęcia jakości i spójności danych lotniczych, definiowane jako: jakość danych - stopień lub poziom pewności, że dostarczane dane spełniają wymagania użytkownika pod względem dokładności, rozróżnialności i spójności oraz spójność danych lotniczych – stopień pewności, że dane lotnicze i ich wartości nie zostały utracone bądź zmienione od czasu ich przekazania lub autoryzowanej zamiany.

Rada ICAO określiła również w załącznikach do Konwencji o międzynarodowym lotnictwie cywilnym [13, 15] kryteria klasyfikacji i wymagania dotyczące poziomów spójności dla poszczególnych klas danych:

- **dane krytyczne, poziom spójności $1\cdot10^{-8}$** [3]: przy wykorzystaniu zafałszowanych danych krytycznych istnieje wysokie prawdopodobieństwo, że bezpieczny lot i lądowanie statku powietrznego będą zagrożone znacznym ryzykiem wystąpienia katastrofy,
- **dane ważne, poziom spójności $1\cdot10^{-5}$**: przy używaniu zafałszowanych danych niezbędnych istnieje małe prawdopodobieństwo, że bezpieczny lot i lądowanie statku powietrznego będą zagrożone znacznym ryzykiem wystąpienia katastrofy,
- **dane zwykłe, poziom spójności $1\cdot10^{-3}$**: przy używaniu zafałszowanych danych rutynowych istnieje bardzo małe prawdopodobieństwo, że bezpieczny lot i lądowanie statku powietrznego będą poważnie zagrożone znacznym ryzykiem wystąpienia katastrofy.

W załączniku 15 [15] określono również wymaganie stosowania matematycznych algorytmów Cyklicznej Kontroli Nadmiarowej (ang. Cyclic Redundancy Check – CRC) celem zapewnienia odpowiedniego poziomu bezpieczeństwa danych lotniczych. W odniesieniu do danych krytycznych i ważnych wymagane jest stosowanie odpowiednio 32-bitowych lub 24-bitowych algorytmów CRC, a dla danych zwykłych zalecane jest stosowanie 16-bitowych algorytmów CRC.

Cykliczna Kontrola Nadmiarowa to z przyjętej definicji [15] algorytm matematyczny stosowany w odniesieniu do danych cyfrowych, zapewniający odpowiedni poziom ochrony przed ich utratą lub zmianą. Algorytm CRC jest wyliczany jako reszta *R(x)* z dzielenia Modulo-2 dwóch wielomianów binarnych w następujący sposób:

$$\left\{\frac{[x^k M(x)]}{G(x)}\right\}_{mod2} = Q(x) + \frac{R(x)}{G(x)} \tag{1}$$

gdzie:

x – liczba bitów argument wielomianu (wartość danej lotniczej, np.: czas, masa, prędkość, pułap, poziom lotu, gradient zniżania lub wznoszenia),

k – liczba bitów w danej CRC,

[3] Gdzie $1\cdot10^{-8}$ = 0,00000001 – wartość prawdopodobieństwa zdarzenia, o którym mowa w przytoczonej definicji spójności danych lotniczych. Analogicznie dla poziomów spójności $1\cdot10^{-5}$ oraz $1\cdot10^{-3}$.

M(x) – pole informacyjne, składające się z danych zabezpieczonych dana CRC, przedstawioną jako wielomian,
G(x) – wielomian generujący określony dla danej CRC,
Q(x) – iloraz danego dzielenia,
R(x) – reszta z dzielenia zawierająca CRC:

$$R(x) = \sum_{i=1}^{k} r_i x^{k-i} = r_1 x^{k-1} + r_2 x^{k-2} + \cdots + r_k x^0 \quad (2)$$

Jak widać do obliczenia CRC potrzebny jest tzw. „wielomian generujący". Stanowi on podstawę do obliczeń i dlatego jego znajomość jest niezbędna zarówno dla nadawcy jak i odbiorcy. Wielomianem generującym jest łańcuch bitów, w którym kolejne pozycje są współczynnikami przy odpowiednich potęgach wielomianu. Zarówno najstarszy jak i najmłodszy bit wielomianu generującego musi być równy 1, a ciąg przeznaczony do zakodowania musi być od niego dłuższy.

Przykładowe wielomiany generujące [13] dla algorytmów CRC 32- i 24-bitowych, wykorzystywane dla danych lotniczych, są następujące:

$$G(x) = x^{24} + x^{23} + x^{18} + x^{17} + x^{14} + x^{11} + x^{10} + x^7 + x^6 + x^5 + x^4 + x^3 + x + 1 \quad (3)$$

co odpowiada zapisowi binarnemu: 1100001100100110011111011, oraz:

$$G(x) = x^{32} + x^{31} + x^{24} + x^{22} + x^{16} + x^{14} + x^8 + x^7 + x^5 + x^4 + x^3 + x + 1 \quad (4)$$

co odpowiada zapisowi binarnemu: 11000000101000001010000000110111011.

Jak wspomniano wcześniej przy obliczeniach CRC obowiązuje arytmetyka Modulo-2, operacje te są zatem równoznaczne z funkcją XOR (alternatywą wykluczającą). Procedurę postępowania, zapisaną w postaci równania (1) można sprowadzić do następujących operacji elementarnych [2]:

- do ciągu danych należy dodać na końcu tyle bitów zerowych, ile wynosi stopień wielomianu generującego (w przypadku omawianych CRC dla danych lotniczych *k* = 32 lub *k* = 24),
- tak rozszerzony ciąg danych należy podzielić przez wielomian generujący, wg następującego algorytmu:
  a) rozpoczynamy od bitu danych położonego z lewej strony,
  b) jeśli jest on równy 1, to poniżej przepisujemy wielomian generujący, jeśli 0, to wpisujemy same 0,
  c) wykonujemy dodawanie Modulo-2, czyli stosujemy funkcję XOR,
  d) podejmujemy próbę odczytu z ciągu danych kolejnego bitu danych,
  e) jeśli próba się powiodła, to wracamy do kroku a),
  f) jeśli próba nie powiodła się, oznacza to koniec obliczeń.

Reszta, która pozostanie z dzielenia, jest poszukiwaną właśnie wartością Cyklicznej Kontroli Nadmiarowej – CRC. Bity te należy dopisać na koniec ciągu danych zamiast uprzednio dopisanych bitów zerowych.

Przy sprawdzaniu poprawności danych stosuje się taki sam algorytm, lecz tym razem dla całego ciągu bitów (łącznie z CRC), jeśli transmisja była bezbłędna, reszta z dzielenia będzie wynosiła 0.

Przykład [2].

Ponieważ dla 24- i 32-bitowych algorytmów CRC, wymaganych w celu zapewnienia odpowiedniego poziomu bezpieczeństwa danych lotniczych, przykładowe obliczenia byłyby czaso- i przestrzeniochłonne, na potrzeby zobrazowania zasad i metody wyliczania Cyklicznej Kontroli Nadmiarowej przedstawiony został przykład, w którym wielomian generujący jest stopnia 4-tego (a nie 32-giego czy 24-tego): x^4+x^2+1, co odpowiada zapisowi: $1x^4+0x^3+1x^2+0x^1+1x^0$, czyli ciągowi binarnemu 10101.

Ciąg z danymi……...……: 10011011,
Wielomian generujący……..…: 10101,
Ciąg danych z dopisanymi zerami…: 100110110000.
100110110000 : 10101
101010

```
00110
 01100
 00000
 --------
 01100
  11001
  10101
  --------
  01100
   11001
   10101
   --------
   01100
    11000
    10101
    --------
    01101
    11010
     10101
     --------
     01111
      11110
      10101
      --------
      01011
       10110
       10101
       --------
       00011
```

0011 – poszukiwana wartość CRC.

Zatem ciąg z dopisanym CRC ma postać: 100110110011.

Koniec przykładu.

Poniżej przedstawiono (Rys. 3.) format bloku danych lotniczych z uwzględnieniem 24-bitowego algorytmu CRC.

Rys. 3. Format bloku danych lotniczych z uwzględnieniem 24-bitowego algorytmu CRC

Źródło: opracowanie na podstawie [13].

W przedmiocie rozważań otwarte pozostaje pytanie, którą klasę danych przyjąć i który algorytm CRC wybrać jako adekwatne do potrzeb służb operacyjnych portu lotniczego? Wychodząc ze stwierdzenia, że największy zakres integracji wynika z merytorycznego zakresu A-CDM i w odniesieniu do przytoczonych

powyżej definicji (i wykładni) klas spójności danych lotniczych, wystarczającym wydaje się zapewnienie spójności operacyjnych danych lotniskowych na poziomie $1 \cdot 10^{-3}$ (dane zwykłe). Uzasadnieniem tego wyboru jest fakt, że dane czasowe (planowane i aktualizowane na bieżąco), dotyczące obsługi naziemnej statku powietrznego oraz przewozu lotniczego, nie są przetwarzane w procesach o krytycznym lub znaczącym wpływie na bezpieczeństwo operacji lotniczych.

Jeżeli jednak zostanie uwzględniona ewentualność wykorzystywania A-CDM (w szczególności w aspekcie gromadzenia i przetwarzania danych operacyjnych) jako komponentu systemów AMAN/DEMAN [3], o (przynajmniej) znaczącym wpływie na bezpieczeństwo, to zasadnym wydaje się dokonanie wyboru poziomu spójności $1 \cdot 10^{-5}$ (dane ważne). Uzasadnieniem przyjęcia tego poziomu spójności operacyjnych danych lotniskowych jest również fakt, że w zakresie A-CDM przetwarzane są również dane i informacje lotnicze należące swoim zakresem do planu lotów (ang. Flight Plan – FPL) i ruchowych danych radarowych (rys. 2.), dla których w praktyce przyjmuje się właśnie ten poziom. Przyjęcie tego rozwiązania zapewni także równoważny poziom i jednolitość algorytmów CRC dla operacyjnych danych lotniskowych, pochodzących z różnych źródeł, co jest kluczowym zagadnieniem przy integracji danych.

Dokonanie klasyfikacji i wyboru wymaganego poziomu spójności operacyjnych danych lotniskowych, w szczególności w aspekcie systemu A-CDM otwiera kolejne zagadnienie problemowe, tj. opracowanie i implementacji adekwatnego algorytmu CRC. Rozwiązanie tego problemu będzie wymagało zidentyfikowania struktur logicznych i środowisk software'owych oraz platform hardware'owych, wykorzystywanych przez poszczególnych tzw. „Partnerów CDM", będących jednocześnie dostawcami i odbiorcami danych. Potencjalnie, możliwe są dwa warianty praktycznego rozwiązania tego problemu:

- utworzenie jednej bazodanowej dynamicznej hurtowni danych i zbioru interface'ów;
- utworzenie zintegrowanej sieci.

Dokonanie (poprzedzonego analizą) wyboru jednego z tych wariantów będzie determinowało zakres i stopień integracji (systemów) operacyjnych danych lotniskowych, a tym samym architekturę i strukturę logiczną, dla której zostanie opracowany i zaimplementowany adekwatny algorytm CRC.

5. PODSUMOWANIE

Założenia i cele strategiczne określane przez Parlament i Komisję Europejską w wydawanych aktach prawnych [8, 10] wiążą się z obowiązkiem wdrażania odpowiednich systemów zarządzania operacjami w ruchu lotniczym, obsługą naziemną statków powietrznych i przewozu lotniczego w portach lotniczych. Funkcjonowanie tych systemów (m.in.: A-CDM, AMAN / DEMAN) oparte jest na przetwarzaniu i wymianie lotniczych (i lotniskowych) danych operacyjnych w różnych systemach teleinformatycznych. Złożoność struktur tych danych, przy jednoczesnym ich znaczeniu dla bezpieczeństwa i sprawności funkcjonowania transportu lotniczego czynią bardzo istotnym problem „ciągłej i bezpiecznej integracji" tych danych. Z przeprowadzonego studium wynika, że właściwym „miejscem" do ulokowania platformy integracji i wymiany lotniskowych danych operacyjnych jest system A-CDM. Platforma ta powinna być wyposażona w odpowiednie zabezpieczenia danych.

Dokumenty źródłowe nie określają jednak wprost wymagań i specyfikacji, jak również atrybutów bezpieczeństwa zintegrowanych lotniskowych danych operacyjnych. Z tego wynikała potrzeba przeprowadzenia przedstawionego w artykule studium literaturowego oraz analiz operacyjnych procesów i systemów ruchu i przewozu lotniczego.

Uzyskane wyniki wskazują, że do przedmiotowego problemu – zapewnienia bezpieczeństwa zintegrowanych lotniskowych danych operacyjnych – należy podejść odpowiednio szeroko, integrując zasady, metody, rozwiązania i algorytmy określone odpowiednio w standardach ICAO i normach ISO, co będzie przedmiotem dalszej pracy autorów.

Streszczenie

W artykule zaprezentowano i omówiono atrybuty bezpieczeństwa informacji, bazując na standardach zawartych w załącznikach do Konwencji o międzynarodowym lotnictwie cywilnym oraz standardach ISO. Następnie opisano System wspólnego podejmowania decyzji w porcie lotniczym (A-CDM), opierający swe działanie na wymianie informacji, a jednocześnie stanowiący jedno ze źródeł danych dla zaawansowanych systemów zarządzania wykonywaniem operacji w ruchu lotniczym. Aby wymiana i przetwarzanie informacji lotniskowych mogły się odbywać w należyty sposób rozważono zagadnienie bezpieczeństwa danych lotniczych i operacyjnych, w aspekcie kryteriów klasyfikacji i wymagań dotyczących poziomów spójności dla poszczególnych klas danych oraz wymaganie stosowania matematycznych algorytmów Cyklicznej Kontroli Nadmiarowej. Na koniec podjęto próbę określenia którą klasę danych przyjąć i który algorytm CRC wybrać jako adekwatne do potrzeb służb operacyjnych portu lotniczego. Uzyskane wyniki wykazały, że do zagadnienia zapewnienia bezpieczeństwa zintegrowanych lotniskowych danych operacyjnych należy podejść odpowiednio szeroko, integrując zasady, metody, rozwiązania i algorytmy określone odpowiednio w standardach ICAO i normach ISO, co będzie przedmiotem dalszej pracy autorów.

Słowa kluczowe: bezpieczeństwo informacji, port lotniczy, integracja danych.

The issue of integrated operational information safety at the airport

Abstract

The article presents and discusses the attributes of information security, based on standards contained in the Annexes to the Convention on International Civil Aviation and ISO standards. Subsequently it describes Airport Collaborative Decision Making (A-CDM) System, basing on information exchange and being one of the data sources for advanced air traffic operation systems. In order to assure proper airport data processing and exchange, the aspect of data security was considered, and what followed classification criteria and requirements for data consistency levels in particular classes as well as requirement of CRC application were described. At the end an attempt to determine which data class and which CRC algorithm are to be chosen as adequate to the airport's operational services needs was made. The results showed that the issue of ensuring integrated airport's data security must be approached in a complex way, integrating principles, methods, solutions and algorithms defined in ICAO and ISO standards, which will be the subject of authors' future study.

Keywords: information security, airport, data integration.

LITERATURA

[1] Bilski T., Stokłosa J., Pankowski T., Bezpieczeństwo danych w systemach informatycznych, Wydawnictwo Naukowe PWN, 2001, Warszawa-Poznań.
[2] Fulmański P., Sobieski Ś., Wstęp do informatyki, Uniwersytet Łódzki, styczeń 2004.
[3] Kwasiborska A., Kozłowski M., Skorupski J., Stelmach A., Operacyjne i teoretyczne aspekty nowoczesnego zarządzania ruchem lotniczym, Przegląd Komunikacyjny, Nr 2/2015, str. 9-13.
[4] Norma PN-ISO/IEC 27001:2007, Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji, Polski Komitet Normalizacyjny, 2007, Warszawa.
[5] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz. U. z 2010 r. Nr 182, poz. 1228.
[6] Airport Collaborative Decision Making – Improving efficiency while helping the environment, ACI Europe & EUROCONTROL 2010.
[7] www.euro-cdm.org.
[8] Rozporządzenie Parlamentu Europejskiego i Rady (WE) Nr 1070/2009 z dnia 21 października 2009 r. zmieniające rozporządzenia (WE) nr 549/2004, (WE) nr 550/2004, (WE) nr 551/2004 oraz (WE) nr 552/2004 w celu poprawienia skuteczności działania i zrównoważonego rozwoju europejskiego systemu lotnictwa.
[9] SESAR Joint Undertaking Program WP6 – Airport Operations.
[10] Rozporządzenie Wykonawcze Komisji (UE) Nr 716/2014 z dnia 27 czerwca 2014 r. w sprawie ustanowienia wspólnego projektu pilotażowego wspierającego realizację centralnego planu zarządzania ruchem lotniczym w Europie.
[11] Arrival Manager – Implementation Guidelines and Lessons Learned, European Organization for the Safety of Air Navigation, EUROCONTROL 2010.
[12] The EUROCONTROL DMAN Prototype – Description of DMAN in the A-CDM context, EUROCONTROL 2010.
[13] Załącznik 10 do Konwencji o międzynarodowym lotnictwie cywilnym, Łączność lotnicza, tom I, Organizacja Międzynarodowego Lotnictwa Cywilnego, lipiec 2006.

[14] Załącznik 14 do Konwencji o międzynarodowym lotnictwie cywilnym, Lotniska, Organizacja Międzynarodowego Lotnictwa Cywilnego, lipiec 2009.
[15] Załącznik 15 do Konwencji o międzynarodowym lotnictwie cywilnym, Służby Informacji Lotniczej, Organizacja Międzynarodowego Lotnictwa Cywilnego, lipiec 2013.