Warszawa, dnia 28 marca 2012 r.
Poz. 26

OBWIESZCZENIE NR 6
PREZESA URZĘDU LOTNICTWA CYWILNEGO

z dnia 27 marca 2012 r.

w sprawie ogłoszenia wymagań ustanowionych przez Organizację Międzynarodowego Lotnictwa Cywilnego (ICAO) w Doc 9855 – Wytyczne w sprawie użycia Internetu w zastosowaniach lotniczych

Na podstawie art. 23 ust. 2 pkt 2 ustawy z dnia 3 lipca 2002 r. - Prawo lotnicze (Dz. U. z 2006 r. Nr 100, poz. 696, z późn. zm.[1)]) ogłasza się jako załącznik do niniejszego obwieszczenia wymagania ustanowione przez Organizację Międzynarodowego Lotnictwa Cywilnego (ICAO) w Doc 9855 – Wytyczne w sprawie użycia Internetu w zastosowaniach lotniczych (wyd. pierwsze).

p.o. Prezesa Urzędu Lotnictwa Cywilnego

Wiceprezes ds. Standardów Lotniczych
Tomasz Kądziołka

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 104, poz. 708 i 711, Nr 141, poz. 1008, Nr 170, poz. 1217 i Nr 249, poz. 1829, z 2007 r. Nr 50, poz. 331 i Nr 82, poz. 558, z 2008 r. Nr 97, poz. 625, Nr 144, poz. 901, Nr 177, poz. 1095, Nr 180, poz. 1113 i Nr 227, poz. 1505, z 2009 r. Nr 18, poz. 97 i Nr 42, poz. 340, z 2010 r. Nr 47, poz. 278 i Nr 182, poz. 1228 oraz z 2011 r. Nr 80, poz. 432, Nr 106, poz. 622, Nr 170, poz. 1015, Nr 171, poz. 1016 i Nr 240, poz. 1429.

Załącznik do Obwieszczenia nr 6
Prezesa Urzędu Lotnictwa Cywilnego
z dnia 27 marca 2012 r.

Doc 9855
AN/459

WYTYCZNE W SPRAWIE UŻYCIA INTERNETU W ZASTOSOWANIACH LOTNICZYCH

Zatwierdzone przez Sekretarza Generalnego
i opublikowane pod jego nadzorem

Wydanie pierwsze - 2005

Organizacja Międzynarodowego Lotnictwa Cywilnego (ICAO)

ZMIANY

Wydania zmian są regularnie publikowane w *Dzienniku ICAO* oraz w comiesięcznym *Suplemencie do Katalogu wydawnictw i audiowizualnych pomocy szkoleniowych ICAO*, z którymi posiadacze niniejszej publikacji powinni się zapoznać. Tabele umieszczone poniżej służą do rejestracji zmian i korekt.

REJESTRACJA ZMIAN I KOREKT

ZMIANY		
Nr	Data	Osoba wprowadzająca

KOREKTY		
Nr	Data	Osoba wprowadzająca

PRZEDMOWA

Dokument ten został opracowany z pomocą grupy *Aviation Use of the Public Internet Study Group (AUPISG),* w celu pomocy państwom, w dobie wzmożonego użycia Internetu w zastosowaniach lotniczych.

Dokument ten zawiera wytyczne w sprawie wykorzystania Internetu jako środka zapewniającego łączność naziemną w zastosowaniach lotniczych, dla których czas nie jest czynnikiem krytycznym. Termin „czas nie czynnikiem krytycznym" oznacza, że informacja transmitowana przez Internet nie ma natychmiastowego wpływu na trwający lot statku powietrznego. Nacisk położono również na materiał, który może pomóc państwom akredytować instytucje zapewniające informacje lotnicze przez Internet.

Stosowanie się do poniższych wytycznych zapobiegnie lub zminimalizuje możliwość użycia różnych procedur przez państwa i organizacje międzynarodowe, które będą wykorzystywać Internet w zastosowaniach operacyjnych.

Zadaniem wytycznych jest podanie najlepszych praktyk, a nie szczegółowych wymagań technicznych. Bazują one na sprawdzonych procedurach operacyjnych i gotowych do wykorzystania produktach. Podane w wytycznych przykłady mogą być przestarzałe w związku z tym, że poziom technologii internetowych szybko się zmienia. Zaleca się implementację najbardziej odpowiedniego, dostępnego w danym momencie rozwiązania. Ponadto wytyczne nie odnoszą się do usług normalnie zapewnianych przez infrastrukturę telekomunikacyjną, takich jak dzierżawione linie łączności i sieci intranetowe, które mogą wykorzystywać technologie internetowe.

Dokument zawiera rys historyczny i rozważania ogólne na temat służb lotniczych wykorzystujących Internet oraz rozważania odnoszące się do określonych rodzajów usług.

Należy podkreślić, że dokument ten nie zawiera stanowiska ICAO na temat, gdzie i kiedy należy wykorzystać lub nie należy wykorzystywać Internetu do zastosowań lotniczych. ICAO może określić swoje stanowisko w tym względzie w przyszłości, jeśli uznane to zostanie za konieczne.

SPIS TREŚCI

SŁOWNIK POJĘĆ

Uwaga. – Wyjaśnienie pojęć przedstawione poniżej służy zrozumieniu terminów w kontekście ich użycia w dokumencie.

Przeglądarka / Browser. Oprogramowanie służące do otworzenia i przeglądania strony internetowej. Przeglądarka odczytuje kod HTML lub XML (patrz poniżej) z plików strony internetowej, uruchamia zawarte tam skrypty i programy, zapewnia kodowanie/dekodowanie dla potrzeb bezpieczeństwa transmisji, gdy jest to niezbędne wyświetla grafikę (z wyjątkiem przeglądarek tekstowych), odtwarza muzykę i filmy oraz zapewnia linki do powiązanych stron.

Strefa zdemilitaryzowana / Demilitarized zone (DMZ). Sieć posadowiona pomiędzy dwoma sieciami. Nie jest to część sieci wewnętrznej ani część bezpośrednio Internetu. Infrastruktura wykorzystywana w tej strefie jest częściowo odporna na ataki zewnętrzne, jednakże ciągle pozostaje wrażliwa.

Ataki odmowy usług (DoS) / Denial of service (DoS) attacks. Usiłowanie zawładnięcia stroną internetową lub serwerem. Następstwem ataku jest fakt, że normalni użytkownicy rywalizują z atakującym o dostęp do tych samych zasobów. Rezultatem ataku może być zablokowanie dostępu dla normalnych użytkowników lub zablokowanie całej infrastruktury. Ataki typu DDoS (Distributed DoS) są natomiast skoordynowanymi atakami z wielu miejsc jednocześnie i mogą być znacznie trudniejsze do odparcia. Atak DoS jest często stosowany przez atakującego jako środek odwracający uwagę w czasie usiłowania uzyskania dostępu do systemu.

Certyfikat cyfrowy / Digital certificate. Elektroniczny środek uwierzytelniający użytkownika dla potrzeb zawierania transakcji poprzez sieć internetową. Jest on wydawany przez instytucję certyfikującą. Zawiera on nazwę użytkownika, numer seryjny, datę ważności, kopię certyfikatu klucza publicznego posiadacza (używanego do kodowania i dekodowania wiadomości i podpisów cyfrowych) oraz podpis cyfrowy instytucji wydającej certyfikat, po to aby odbiorca mógł zweryfikować prawdziwość certyfikatu. Niektóre certyfikaty cyfrowe spełniają rekomendację X.509 Sekcji Standaryzacji Telekomunikacyjnej ITU (International Telecommunication Union). Certyfikaty cyfrowe mogą być przechowywane w rejestrach, aby zweryfikowani użytkownicy mogli sprawdzić klucze publiczne innych użytkowników.

Poczta elektroniczna / Electronic mail (email). Jeden ze standardowych protokołów internetowych, który umożliwia komunikowanie się wzajemne ludziom posiadającym różne komputery i systemy operacyjne. Email umożliwia wysyłanie poczty jeden-do-jeden lub jeden-do-wielu. Poczta jest odbierana i przechowywana na serwerze pocztowym organizacji lub przez dostawcę usług internetowych do czasu zalogowania się i odebrania poczty przez adresata.

Język XML / Extensible Markup Language (XML). Etap rozwoju formatów danych sieciowych (poza HTML).

Extranet. Sieć uzupełniająca sieć intranetową poprzez zapewnianie dostępu dla klientów, dostawców, podwykonawców i innych podmiotów spoza organizacji, którym niezbędny jest określony zakres informacji o organizacji. Na ogół nie jest połączona z Internetem.

Zapora / Firewall. Urządzenie chroniące zasoby sieci prywatnej przed użytkownikami innych sieci. Zasadniczo zapora, ściśle współpracując z routerem, filtruje wszystkie pakiety danych sieciowych w celu oceny, czy pozwolić im dotrzeć do miejsca przeznaczenia. Zapora jest często instalowana niezależnie od reszty sieci. W ten sposób żadne zapytanie zewnętrzne nie może bezpośrednio dotrzeć do zasobów sieciowych.

Hipermedia / Hypermedia. Podobnie jak hipertekst, jednakże połączone z elementami grafiki, audio i video.

Hipertekst / Hypertext. Forma organizacji tekstu zawierająca linki do innych stron tekstu lub do multimediów, dostępne przez kliknięcie lub wybranie linku.

Język HTML / Hypertext Markup Language (HTML). System kodowania używany do tworzenia stron sieci internetowej (WWW). Strona stworzona w języku HTML ma postać pliku tekstowego zawierającego formatki (tagi) w nawiasach, które definiują rodzaj i wielkość czcionki, wstawiają na stronę grafikę, formatują tabele i obramowania, definiują układ tekstu, wstawiają odwołania do uruchamianych programów oraz innych stron internetowych (linki).

Protokół https / Hypertext Transport Protocol (Secure) (https). Mechanizm kodowania w sieci internetowej. Jest to protokół HTTP opierający się na SSL.

Internet. System o zasięgu światowym stanowiący połączenie sieci komputerowych i wykorzystujący protokół TCP/IP do transmisji i pozyskiwania danych.

Instytucja zapewniająca informację lotniczą przez Internet (IASP) / Internet aviation service provider (IASP). Akredytowana organizacja zapewniająca informację lotniczą przy wykorzystaniu Internetu jako środka komunikacji.

Protokół internetowy (IP) / Internet protocol (IP). Protokół używany do kierowania pakietów danych od źródła do miejsca przeznaczenia w środowisku internetowym.

Dostawca usług internetowych (ISP) / Internet service provider (ISP). Podmiot zapewniający dostęp do Internetu oraz infrastrukturę do realizacji tego dostępu.

Intranet. Sieć prywatna w ramach pojedynczej organizacji, wykorzystująca protokół TCP/IP do transmisji i pozyskiwania danych. Strony intranetowe są generalnie niedostępne z poziomu Internetu. Są one dostępne tylko dla członków organizacji.

Zintegrowany z systemem operacyjnym / Operating system (OS) integrated. Cecha lub funkcja, która jest zintegrowana z systemem operacyjnym (np. Internet Explorer w systemie Windows).

Port. Zdefiniowany adres wewnętrzny, który służy jako ścieżka z poziomu aplikacji do poziomu komunikacyjnego (TCP) i odwrotnie.

Kluczowa infrastruktura publiczna (PKI) / Public key infrastructure (PKI). System obejmujący certyfikaty cyfrowe, władze certyfikujące i inne instytucje rejestrujące, który dokonuje weryfikacji i potwierdzenia tożsamości stron transakcji internetowej. Systemy takie obecnie znajdują się w fazie ewolucji. Nie ma więc pojedynczego takiego systemu, ani jednego ogólnie przyjętego standardu jego tworzenia.

Nadmiarowa macierz niezależnych dysków (pierwotnie – nadmiarowa macierz tanich dysków) (RAID) / Redundant array of independent disks (originally redundant array of inexpensive disks) (RAID). Sposób przechowywania tych samych danych w różnych miejscach (a więc nadmiarowo) powodujący, że operacje wejścia/wyjścia mogą w sposób zbalansowany zachodzić w tym samym czasie, poprawiając wydajność. Nadmiarowość powoduje wzrost średniego czasu poprawnej pracy (MTBF) i również zwiększa tolerancję na błędy. Macierz RAID jest widziana przez system operacyjny jako jeden dysk logiczny.

Ocena ryzyka / Risk assessment. Ocena zagrożeń dla systemu. Prawdopodobieństwo, że zagrożenia te spowodują szkody oraz wpływ tych szkód.

Router. Urządzenie determinujące następny punkt sieciowy, do którego będzie przekazywany pakiet danych, po jego drodze do punktu przeznaczenia. Router jest podłączony do co najmniej dwóch sieci i kieruje drogą przesyłania pakietów danych, bazując na wynikach monitorowania stanu sieci, do których jest podłączony. Routery tworzą bieżące zestawienia dostępnych dróg przesyłania danych i na tej podstawie określają najlepszą dostępną drogę dla danego pakietu danych.

RSA. Internetowy system kodowania i potwierdzania tożsamości bazujący na algorytmie, który opracowali Ron Rivest, Adi Shamir i Leonard Adleman w 1977 r. System jest własnością firmy RSA Security, która licencjonuje technologie oparte na tym algorytmie.

Secure Sockets Layer (SSL). Metoda kodowanej łączności przez internet. SSL zapewnia, że niezmieniona informacja zostanie przesłana tylko do odbiorcy. Strony internetowe banków oraz sklepów często wykorzystują technologię SSL do zabezpieczenia przesyłanych danych o kartach kredytowych oraz innych poufnych informacji.

SecurID. RSA SecurID® jest „silnym” mechanizmem potwierdzania tożsamości, wymagającym zarówno tokena, jak i osobistego numeru identyfikacyjnego (PIN).

Serwer / Server. Komputer lub urządzenie sieciowe, które dostarcza lub zarządza zasobami sieciowymi. Przykładem może być serwer plików, który jest komputerem i urządzeniem magazynującym dane. Każdy użytkownik sieci może przechowywać pliki na serwerze. Serwer drukarkowy jest komputerem zarządzającym jedną lub więcej drukarkami, a serwer sieciowy jest komputerem zarządzającym ruchem w sieci. Serwer bazodanowy jest systemem komputerowym, który obsługuje zapytania dotyczące bazy danych. Serwery są często urządzeniami dedykowanymi, to znaczy nie wykonują innych zadań poza przydzielonymi. Jednakże w wieloprocesowych systemach operacyjnych, komputer może wykonywać wiele programów jednocześnie. W tym przypadku serwer może się odwoływać do programu zarządzającego zasobami, a nie do komputera.

Silna autentyfikacja / Strong authentication. Dwupoziomowa metoda potwierdzania tożsamości, oparta na czymś znanym użytkownikowi (np. hasło/PIN) oraz na czymś co użytkownik posiada (np. token - karta uwierzytelniająca). Uwierzytelnienie dwupoziomowe zapewnia znacznie bardziej skuteczne potwierdzenie tożsamości użytkownika. Patrz również RSA SecurID.

Protokół TCP / Transmission Control Protocol (TCP). Protokół komunikacyjny (używany w Internecie), który zapewnia pewną komunikację host-host w sieci opartej na transmisji pakietowej lub w strukturze będącej połączeniem takich sieci.

Adres URL / Uniform Resource Locator (URL). Oznaczenie lokalizacji danych zasobów w Internecie. Może być wprowadzone do okna adresowego przeglądarki internetowej, w celu połączenia się z danymi zasobami (np. stroną internetową).

Wirtualna sieć prywatna (VPN) / Virtual private network (VPN). Sieć, która wykorzystuje autentyfikowany kanał stworzony w sieci publicznej (np. w Internecie). Dostęp do kanału VPN wymaga potwierdzenia tożsamości i wykorzystuje silne procedury autentyfikacji. Dane przesyłane w sieci są kodowane i w ten sposób niedostępne z poziomu sieci publicznej.

Strona sieci / Website. Jedna lub więcej powiązanych ze sobą stron internetowych o podobnej tematyce lub zarządzanych czy posiadanych przez jeden podmiot.

World Wide Web (WWW). Protokół internetowy wykorzystujący HTML, hipertekst i hipermedia do tworzenia stron zawierających linki do innych stron. Strony WWW mogą zawierać grafikę, pliki dźwiękowe i video oraz tekst.

Rozdział 1

WPROWADZENIE

1.1 Słowo „Internet” powstało ze skrócenia frazy „interconnected network”. Dokument poniższy często odwołuje się do pojęcia „publiczny Internet” (lub po prostu Internet), który jest luźnym połączeniem sieci komputerowych wykorzystujących do komunikacji między sobą protokół TCP/IP. Podobne znaczenie ma termin „World Wide Web (WWW)”, oznaczający globalną sieć składającą się z serwerów (oprogramowanie zainstalowane na komputerach podłączonych do Internetu), w której jednocześnie przetwarzane są pliki tekstowe, graficzne, dźwiękowe i video oraz linki (aktywne odniesienia do innych miejsc lub zasobów sieciowych).

1.2 Początków Internetu należy szukać w pracach badawczych prowadzonych w Stanach Zjednoczonych w latach 60-tych, mających na celu opracowanie bezpiecznej sieci komputerowej. Wysiłki te zaowocowały powstaniem sieci ARPANET (Advanced Research Projects Agency Net), która rozpoczęła swoje operacyjne funkcjonowanie w 1969 r., łącząc ze sobą komputery na kilku uniwersytetach w Stanach Zjednoczonych. Jakkolwiek pierwszy email został przesłany przez sieć ARPANET w 1972 r., to data 1 stycznia 1983 r. jest uważana za „oficjalny” początek Internetu, kiedy to został on oparty na protokole TCP/IP, opracowanym w latach 70-tych i zaakceptowanym przez rząd Stanów Zjednoczonych w 1978 r. Inne sieci były stopniowo przyłączane do sieci ARPANET i w ten sposób Internet się rozwijał. Działanie sieci ARPANET zostało zakończone w 1989 r. lecz Internet kontynuował swój dynamiczny rozwój oparty na dużym zainteresowaniu, dostępności wydajnych komputerów osobistych, linii łączności takich jak łącza światłowodowe, jak również sieci lokalnych i rozległych. Kontrola transmisji internetowych została przekazana instytucjom komercyjnym w 1995 r.

1.3 Użytkownicy Internetu normalnie korzystają z usług dostarczanych przez dostawców usług internetowych (ISP). Ogromne i ciągle rosnące zapotrzebowanie na usługi internetowe (od 200 mln w 1998 r. do 500 mln użytkowników w 2002 r.) jest najskuteczniejszym bodźcem, który skłania dostawców usług do ciągłej poprawy pojemności / wydajności systemów i oferowania coraz lepszych usług. Można z tego wysnuć generalny wniosek, że gdziekolwiek jest dostępny Internet (oraz istnieje konkurencja rynkowa) prawdopodobieństwo znalezienia odpowiedniego poziomu usług wzrasta.

1.4 Tradycyjnie lotnictwo cywilne nalegało na posiadanie własnych, specjalizowanych systemów łączności, które zapewniają niezawodność, integralność i bezpieczeństwo. Spowodowało to niechęć personelu lotniczego do Internetu, który nie jest kontrolowany przez żaden podmiot związany z lotnictwem cywilnym. Jednakże w związku z szeroką i łatwą dostępnością Internetu, biorąc pod uwagę fakt, że jest on stosunkowo tani, szybki i łatwy do wykorzystania, niektóre państwa zdecydowały się na wykorzystanie Internetu do niektórych zastosowań (np. meteorologicznych i służby informacji lotniczej). W niektórych regionach świata, gdzie specjalizowane systemy łączności lotniczej są niewystarczające lub ich utrzymywanie jest nieopłacalne z powodu niewielkiego ruchu lotniczego, Internet jest używany jako środek łączności ziemia – ziemia.

1.5 ICAO intensywnie wykorzystuje usługi oferowane przez Internet (głównie email oraz dostęp do stron) do rozpowszechniania informacji, dokumentów oraz korespondencji

administracyjnej. Łatwość wykorzystania, dostępność i wysoki poziom integralności usług internetowych znacznie polepszyło możliwości komunikacyjne organizacji. Jednakże koncepcja wykorzystania Internetu do zastosowań związanych z bezpieczeństwem lotniczym jest traktowana przez ICAO z ostrożnością. Jest to spowodowane głównie faktem włożenia dużego wysiłku w standaryzację systemów łączności spełniających rygorystyczne wymagania operacyjne związane z bezpieczeństwem oczekując, że zostaną one implementowane przez państwa zgodnie z regionalnymi planami żeglugi powietrznej.

1.6 W obszarze systemów łączności ziemia-ziemia system AMHS (ATS message handling system), który jest nowoczesnym systemem łączności ziemia-ziemia stanowiącym część lotniczej sieci telekomunikacyjnej (ATN), został opracowany przez ICAO w celu zastąpienia przestarzałej, stałej telekomunikacyjnej sieci lotniczej (AFTN). Podobnie jak AFTN (oraz sieć CIDIN – wspólna sieć wymiany danych ICAO), AMHS jest systemem dedykowanym, wspierającym lotnicze rozwiązania związane z bezpieczeństwem. Do chwili obecnej jednakże, system został wdrożony w bardzo ograniczonym zakresie i upłynie jeszcze wiele lat zanim będzie dostępny prawdziwie globalny system wymiany informacji. W międzyczasie, Internet jawi się jako system wymiany informacji dla środowiska lotniczego. Co więcej, w odróżnieniu od AFTN, CIDIN czy AMHS, które są sieciami zamkniętymi, ograniczonymi do autoryzowanych użytkowników, Internet jest otwarty i dlatego pozwala pilotom oraz innym bieżącym czy potencjalnym użytkownikom informacji lotniczych na dostęp do baz danych, jak również kontakt z odpowiednimi instytucjami, o ile to konieczne, z domu lub innego miejsca dysponującego odpowiednim połączeniem. Z tego powodu Internet jest korzystnym uzupełnieniem obecnego systemu łączności lotniczej.

1.7 Mając na uwadze powyższe oraz w odpowiedzi na rekomendacje regionalnych grup planowania i implementacji oraz Meteorological (MET) Divisional Meeting w 2002 r., ICAO rozpoczęło studia na temat wykorzystania Internetu we wszystkich kategoriach zastosowań lotniczych (tylko w kontekście łączności ziemia-ziemia) oraz związanymi z tym zagadnieniami niezawodności, integralności, dostępności i bezpieczeństwa. Wytyczne zawarte w poniższym dokumencie są wstępnym wynikiem tych studiów.

1.8 Dokument poniższy zawiera wytyczne w sprawie wykorzystania Internetu do zastosowań lotniczych ziemia-ziemia, dla których czas nie jest czynnikiem krytycznym. Zastosowania takie na ogół związane są z rozpowszechnianiem / wymianą informacji pomiędzy:

a) władzami danego państwa a użytkownikami (w ramach państwa);
b) dwiema lub więcej władzami różnych państw;
c) stroną trzecią (zwykle podmiotem komercyjnym) a użytkownikami (w ramach tego samego lub różnych państw).

1.9 Użytkownicy informacji lotniczych muszą być pewni, że dane które wykorzystują są zapewniane przez podmiot zaakceptowany przez dane państwo oraz jest on odpowiednio zarządzany i zabezpieczona jest integralność danych. Problem ten jest o wiele bardziej

złożony, gdy informacja jest transmitowana przez Internet. Pociąga to za sobą dwa procesy akredytacyjne. Jeden obejmujący źródło informacji lotniczej i drugi obejmujący dostarczanie tej informacji poprzez Internet. Wytyczne zawarte w tym dokumencie odnoszą się do dostarczania informacji lotniczej przez Internet.

Rozdział 2

ODPOWIEDZIALNOŚĆ PAŃSTW

2.1 UWAGI OGÓLNE

2.1.1 Ogólnie rzecz biorąc, użycie Internetu jako środka zapewniania lub wymiany informacji operacyjnych nie zwalnia państw z obowiązku utworzenia stałej służby lotniczej (AFS) oraz innych środków i służb wprowadzonych poprzez porozumienia regionalne i udokumentowanych w regionalnych planach żeglugi powietrznej ICAO.

2.1.2 Dodatkowo, tak jak pozostałe środki czy służby, wykorzystanie Internetu jako środka wymiany danych czy wiadomości powinno być przedmiotem porozumień dwustronnych, trójstronnych czy regionalnych. Powinno to być również odzwierciedlone w regionalnych planach żeglugi powietrznej.

2.1.3 Państwo, które zezwala na użycie Internetu powinno:

a) akredytować podmioty (zwane instytucjami zapewniającymi informację lotniczą przez Internet (IASP)) zapewniające informację i jej wymianę przez Internet; oraz
b) zapewnić sobie posiadanie wiedzy specjalistycznej w zakresie technologii informacyjnych i bezpieczeństwa informacyjnego, odpowiednich do nadzoru procesu akredytacji, o którym mowa dalej.

2.1.4 Dla potrzeb akredytacji / nadzoru nad IASP, państwa powinny:

a) publikować i uaktualniać listę akredytowanych IASP zawierającą szczegółowy opis zapewnianej służby oraz termin ważności akredytacji;
b) wymagać, aby IASP informował użytkowników o wszystkich ograniczeniach związanych z dostarczaniem przez niego usług. IASP powinien również poinformować jak zamierza zapewniać służbę w przypadku awarii. Na przykład w razie awarii systemu internetowego podczas składania planu lotu użytkownik powinien zadzwonić do służb ruchu lotniczego lub systemu ruchu lotniczego i złożyć plan lotu konwencjonalnie;
c) wymagać, aby IASP zredukował, pomimo używania dobrze zaprojektowanych interfejsów użytkownika, możliwość przypadkowego wprowadzania przez niego nieprawidłowej informacji, jak również zapewnić użytkownikowi odpowiednie szkolenie; oraz
d) przeprowadzić ponowny proces akredytacji IASP po upływie przynajmniej 3 lat lub w przypadku wprowadzenia przez niego znaczących zmian w infrastrukturze czy zmian organizacyjnych.

2.2 MAJĄCE ZASTOSOWANIE PRZEPISY ICAO

2.2.1 Załącznik 15 do Konwencji o międzynarodowym lotnictwie cywilnym – „Służby informacji lotniczej", Rozdział 3, określa odpowiedzialność państw w zakresie zapewniania informacji lotniczej oraz funkcje służby informacji lotniczej. Zawarte są w nim także przepisy odnoszące się do ustanowienia systemu jakości, wymiany informacji lotniczej, praw autorskich itd. Filozofią stanowiącą podstawę Załącznika 15, który ma swoje źródło w

artykule 28 Konwencji o międzynarodowym lotnictwie cywilnym jest fakt, że każde państwo jest odpowiedzialne za udostępnianie jakiejkolwiek części czy całości informacji dotyczącej jego terytorium i terytoriów innych, gdzie zapewnia służby ruchu lotniczego. Informacja ta jest wymagana dla potrzeb operacji statków powietrznych w ruchu międzynarodowym.

2.2.2 Szczególnie należy podkreślić zapisy z pkt 3.1 Załącznika 15 mówiące, że państwo jest odpowiedzialne za publikowane informacje bez względu na to czy samo zapewnia służbę informacji lotniczej, ma uzgodnione z innym państwem wspólne zapewnianie tej służby, czy też deleguje zapewnianie służby do agencji pozarządowej. Dodatkowo, w przypadku wykorzystania Internetu jako środka publikacji informacji lotniczej, państwa powinny zapewnić, że odpowiednie procesy i procedury systemu jakości są wdrożone dla zabezpieczenia informacji publikowanych pod ich nadzorem a także powinny akredytować serwisy internetowe, które publikują tę informację.

2.2.3 Załącznik 3 do Konwencji o międzynarodowym lotnictwie cywilnym - „Służba meteorologiczna dla międzynarodowej żeglugi powietrznej", Rozdział 2, pkt 2.2, określa odpowiedzialność państw w zakresie zapewniania i wykorzystania informacji meteorologicznych, jak również wymagań jakościowych dla tej informacji.

2.2.4 Załącznik 4 do Konwencji o międzynarodowym lotnictwie cywilnym - „Mapy lotnicze", Rozdział 2, pkt 2.17, określa wymagania w zakresie zarządzania jakością danych lotniczych w postaci map.

2.3 AKREDYTACJA IASP

2.3.1 Należy odróżnić akredytację IASP od akredytacji źródeł informacji lotniczych. Akredytacja źródeł danych, włączając w to gromadzenie, formatowanie i dostarczanie ich na czas jest warunkiem wstępnym akredytacji IASP i nie jest przedmiotem tego dokumentu.

2.3.2 W celu zapewnienia, że informacja dostarczana przez Internet spełnia najlepsze praktyki w zakresie poufności, integralności, autentyczności i dostępności, państwa opracowują procedury akredytacji IASP zapewniających informację i służby przez Internet. Dalsze punkty zawierają wytyczne w tym zakresie.

2.3.3 Pożądane jest, aby państwa wymagały od IASP przestrzegania procedur określonych na rysunku 2.1. Poszczególne państwa mogą uzupełniać te procedury, o ile uznają to za stosowne.

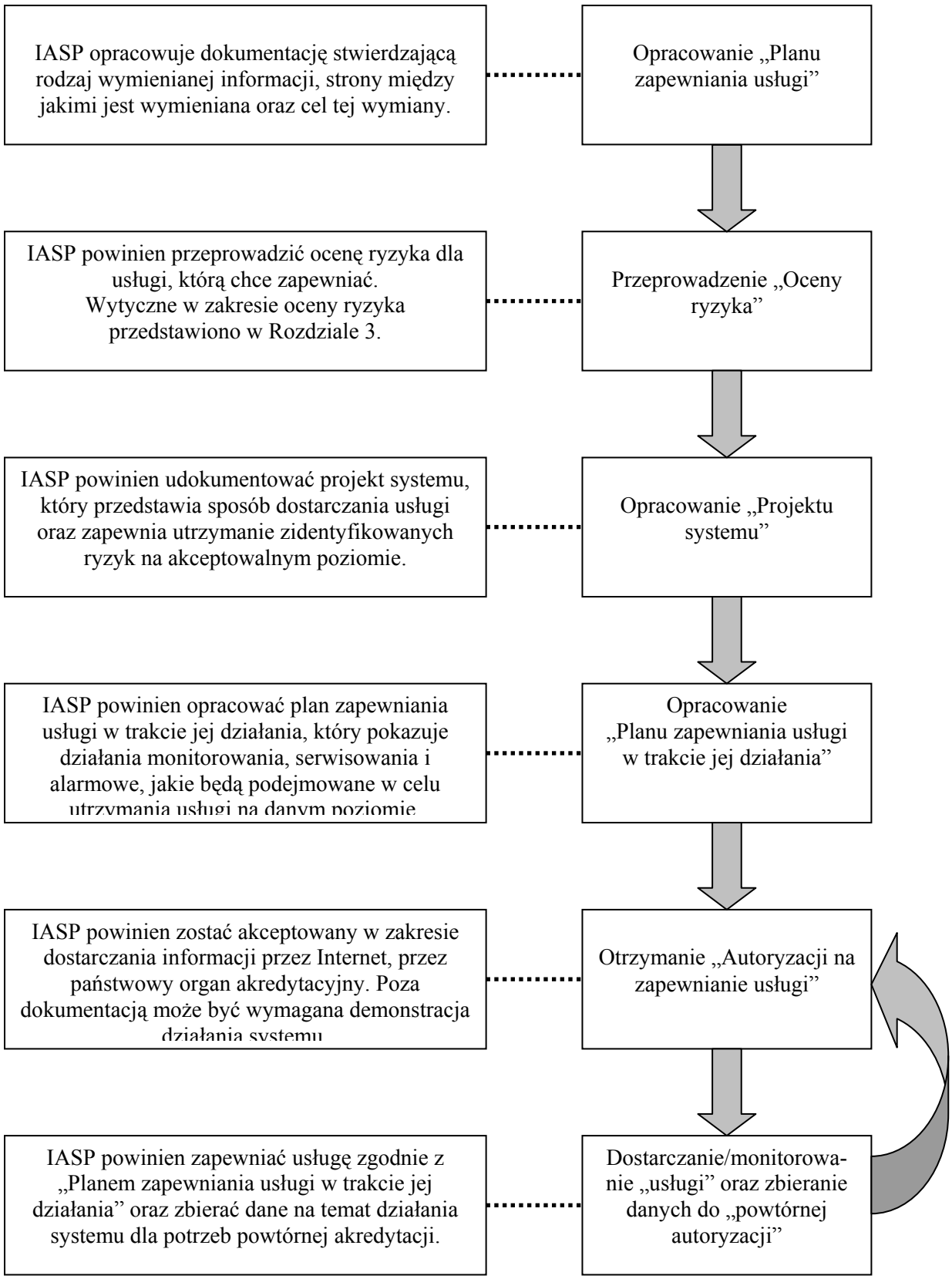
2.3.4 Podstawowe elementy typowego procesu akredytacji opisanego na rysunku 2.1 są wyjaśnione w kolejnych punktach.

Plan zapewniania usługi

2.3.5 IASP powinien mieć opis usług internetowych, które będą zapewniane. Opis usług będzie zawierał:

a) rodzaje usług. Typowe usługi to służba informacji lotniczej (AIS), MET, łączność AFTN, składanie planów lotu (nie ogranicza się dostępności innych usług);
b) obszar dostępności (np. lokalnie, regionalnie czy globalnie);
c) rynek docelowy (lotnictwo ogólne, biznesowe, komercyjne).

Plan zapewniania służby jest warunkiem wstępnym procesu zarządzania ryzykiem.



Rys. 2.1 Typowy proces oceny IASP

Ocena ryzyka

2.3.6 Po opracowaniu planu zapewniania służby, IASP będzie musiał oszacować ryzyko związane z zapewnianiem służby przez Internet. Wytyczne dotyczące oceny ryzyka zawarto w rozdziale 3.

Projekt systemu

2.3.7 Po zidentyfikowaniu ryzyka związanego ze służbą, IASP powinien zaprojektować system w taki sposób, aby zmniejszyć poziom ryzyka dla służby, którą zamierza dostarczać do akceptowalnego poziomu. Wytyczne dotyczące strategii zmniejszania ryzyka zawarto w rozdziale 3.

Plan zapewniania usługi w trakcie jej działania

2.3.8 Po opracowaniu planu zapewniania służby, oceny ryzyka i projektu systemu, IASP musi rozważyć, w jaki sposób usługa będzie utrzymywana na wymaganym poziomie jakości.

Serwisowanie systemu

2.3.9 IASP musi mieć plan serwisowania systemu, w celu zabezpieczenia jego ciągłego funkcjonowania, odpowiednio do rodzaju zapewnianej użytkownikom usługi. Plan powinien zawierać prewencyjne zabiegi serwisowe w odniesieniu do sprzętu i oprogramowania. Priorytetowo należy traktować regularne uaktualnianie oprogramowania odpowiedzialnego za bezpieczeństwo. IASP musi zdefiniować również części zapasowe, które mają być przechowywane w celu spełnienia zdefiniowanych wymagań czasowych na usprawnienie systemu. Należy również zdefiniować minimalne wymagania dotyczące wyszkolenia personelu serwisowego.

Umowa z dostawcą usług internetowych (ISP)

2.3.10 Instytucja zapewniająca informację lotniczą przez Internet (IASP) powinna posiadać porozumienie SLA (Service Level Agreement) z dostawcą usług internetowych (ISP). Porozumienie powinno zawierać wymagania dotyczące dostępności usługi, włączając w to czas napraw, raportowanie usterek, punkty kontaktowe oraz miesięczne raporty funkcjonowania usługi.

Rejestr danych i operacji

2.3.11 Instytucja zapewniająca informację lotniczą przez Internet (IASP) powinna spełniać wymagania zarządzania danymi podane w Załącznikach do Konwencji o międzynarodowym lotnictwie cywilnym w zakresie usług, które oferuje. Odnosi się to do utrzymywania rejestrów o danych udostępnianych w każdym momencie czasowym, jak również rejestrów operacji, w celu udokumentowania jakie dane udostępniono poszczególnym użytkownikom.

Uwaga. – W przypadku utrzymywania rejestrów dotyczących oprogramowania, sieci i/lub plików z historią dostępu, okres ich przechowywania ustanowi państwo. Trzydzieści dni kalendarzowych (jak w Załączniku 10 - Telekomunikacja lotnicza, Tom II – Procedury telekomunikacyjne oraz dokumentach o statusie PANS) *dla przechowywania wiadomości AFTN jest uważane za wystarczające. Jednakże w przypadku wiadomości o wypadku, incydencie lub opóźnieniu samolotu, lub wiadomości przechowywanej na polecenie państwa, IASP powinien ją przechowywać ciągle lub do czasu, gdy jej zniszczenie jest dozwolone prawem. IASP powinien udostępniać te informacje na polecenie państwa, w formie możliwej do odczytania i potwierdzenia jej autentyczności.*

Planowana/nieplanowana przerwa w pracy systemu
2.3.12 IASP powinien mieć wdrożone plany, dotyczące zarządzania przerwami w pracy systemu.

Plany awaryjne
2.3.13 IASP powinien mieć plany awaryjne odpowiednie do rodzaju usług jakie zapewnia.

Operacyjne monitorowanie systemu
2.3.14 IASP powinien opracować listę kryteriów oceny systemu i wymagań, które pozwolą państwowej władzy akredytującej na określenie, czy system spełnia te wymagania.

Autoryzacja usługi
2.3.15 Państwowa władza akredytująca powinna ocenić proces projektowania systemu IASP oraz planowanie zapewniania usługi w trakcie jej działania, w celu oceny zapewniania usługi oraz zapewnienia, że strategie ograniczania ryzyka są wdrożone dla potrzeb redukcji zidentyfikowanych ryzyk do akceptowalnego poziomu.

2.3.16 Przed pierwszą akredytacją państwo może poprosić o zademonstrowanie usług oferowanych przez Internet, w celu upewnienia się, że system spełnia wymagania.

2.3.17 Dodatkowo, państwo może zwrócić się do IASP, aby przeprowadził on całościowe testy systemu przy pomocy firmy specjalizującej się w ocenie bezpieczeństwa teleinformatycznego. Testy powinny obejmować odporność na próby włamania się do systemu, próby skanowania portów i usług oraz testy konieczne do upewnienia się, że system operacyjny i oprogramowanie (w tym oprogramowanie antywirusowe) ma zainstalowane najnowsze uaktualnienia związane z bezpieczeństwem.

2.3.18 Państwa powinny akredytować IASP w zakresie dostarczania usług na stały okres czasu (np. 1-2 lata). W przypadku zwrócenia się IASP o wznowienie akredytacji, powinien on dostarczyć dane historyczne związane z zapewnianą służbą.

2.3.19 Akredytacji nie można przekazywać. IASP powinien to jasno określić łącząc się z innym dostawcą internetowym. IASP powinien jasno wskazać, które państwo dokonało jego akredytacji w zakresie zapewniania informacji lotniczej przez Internet i jaka informacja może przez niego być dostarczana (zgodnie z planem zapewniania służby przedstawionym państwowej władzy akredytacyjnej).

2.3.20 Zgodnie z aktualnymi przepisami ICAO, akredytacja ma zastosowanie tylko do zapewniania służby dla użytkowników operujących w państwie akredytującym lub z tego państwa.

Zapewnianie służby/ monitoring
2.3.21 IASP powinien aktywnie monitorować jakość usługi internetowej. Kryteria jakości zdefiniowane podczas planowania w trakcie zapewniania służby, powinny być monitorowane z częstotliwością, która pozwoli na natychmiastową poprawę jakości, gdy stwierdzono jej obniżenie poniżej standardów. IASP powinien przechowywać pełne zapisy monitoringu jakości. Zapisy te mogą podlegać sprawdzeniu przez państwową władzę akredytacyjną w trakcie okresu, na który udzielono akredytacji. Powinny one być przedstawione przy ubieganiu się o przedłużenie akredytacji.

2.3.23 IASP powinien umieścić na stronie internetowej linki umożliwiające użytkownikom wyrażanie opinii.

2.3.24 IASP powinien również umieścić uzgodniony link do państwowej władzy akredytacyjnej, w celu umożliwienia użytkownikom sprawdzenia statusu akredytacji oraz przesyłania opinii i komentarzy bezpośrednio do państwowej władzy akredytacyjnej.

2.4 OPŁATY

2.4.1 Państwa ponoszą znaczne koszty zapewniania informacji lotniczej i/lub meteorologicznej. W zdecydowanej większości państw koszty te są przenoszone poprzez system opłat nawigacyjnych na użytkowników. Jednakże w związku z rozwojem nowoczesnych technologii informacyjnych i w kontekście przeważającej obecnie komercjalizacji, użytkownicy końcowi mogą dokonać wyboru pomiędzy nabywaniem produktów od przedmiotowego państwa lub od strony trzeciej – komercyjnego dostawcy.

2.4.2 W związku z tym mogą się zdarzyć przypadki, gdy podmioty komercyjne lub państwa będą chciały nabyć informacje lotnicze czy inną dokumentację związaną z żeglugą powietrzną, od państwa ich pochodzenia. W takim przypadku wymogiem państwa pochodzenia materiałów może być zawarcie oddzielnego porozumienia z rozważaną stroną, obejmującego warunki i koszty, o ile występują, które będą miały zastosowanie przy dostarczaniu informacji w celu jej powtórnego opublikowania. Należy zauważyć, że Załącznik 15 do Konwencji o międzynarodowym lotnictwie cywilnym zawiera przepisy o bezpłatnej wymianie informacji lotniczych pomiędzy państwami członkowskimi ICAO.

2.4.3 Generalnie rzecz biorąc schematy naliczania opłat powinny być zgodne z zasadami określonymi w Doc 9082 — ICAO's Policies on Charges for Airports and Air Navigation Services.

2.5 WSKAŹNIKI JAKOŚCIOWE

Państwo powinno rozważyć, o ile jest to wskazane, wprowadzenie obowiązkowych wskaźników jakościowych dla każdej zapewnianej usługi. Wskaźniki te powinny być zorientowane na użytkownika i mogą być ustanawiane w konsultacji z użytkownikami. Generalnie, wskazane jest aby na liście wskaźników jakościowych znalazły się:

a) ***dostępność czasowa***. Usługa może być niedostępna nie dłużej niż przez określony czas w trakcie każdego miesiąca. Pojedynczy okres braku dostępności usługi nie może być dłuższy niż określony. Obejmuje to również okres braku dostępności usługi spowodowanego planowaną obsługą systemu. Zdefiniowane czasy braku dostępności usług będą oczywiście zróżnicowane, w zależności od rodzaju zapewnianych usług;

b) szybkość dostępu. Usługa powinna zapewniać wyświetlanie stron nie wolniej niż z założoną szybkością. Inny wskaźnik może zostać wprowadzony, jeśli użytkownicy będą ściągać większe pliki danych.

Uwaga. – Wskaźniki jakościowe są ustalane według uznania państwa, jednak z zachowaniem rozsądku. Dodatkowo, państwo powinno stosować spójne zasady do dostawców, w przypadku gdy podobne usługi mają spełniać szeroko rozumiane podobne kryteria.

2.6 WŁASNOŚĆ INTELEKTUALNA

2.6.1 Podczas, gdy problem praw autorskich do materiałów udostępnianych on line jest cały czas opracowywany w większości państw to można założyć, że treści już chronione przez prawo danego państwa są tak samo chronione w przypadku udostępnienia ich przez Internet. Aczkolwiek materiały udostępniane przez państwo w Internecie powinny być chronione w taki sam sposób jak materiały drukowane, umieszczanie ich w Internecie niesie za sobą wyższe ryzyko naruszenia praw autorskich. Najczęściej naruszenie to polega na skopiowaniu całości lub części materiału objętego ochroną praw autorskich, bez zgody państwa.

2.6.2 Niektóre państwa mogą wprowadzić prawa autorskie dla niektórych rodzajów informacji (w wersji drukowanej, elektronicznej czy innej). W wyniku tego, państwa te mogą odmówić dowolnemu podmiotowi zgody na kopiowanie lub dalsze rozpowszechnianie tego materiału. Państwa, które chcą zorganizować rozpowszechnianie swoich informacji mogą wprowadzić zasadę, zgodnie z przepisami ICAO lub prawem krajowym, że warunkiem przyznania licencji na kopiowanie i dalsze rozpowszechnianie informacji lotniczej jest wprowadzenie przez dany podmiot odpowiednich procesów kontroli jakości i audytu.

2.6.3 Najbardziej efektywnym sposobem powiadamiania użytkowników o prawach autorskich dotyczących materiałów opublikowanych w Internecie, jest umieszczanie uwagi o prawach autorskich ® w widocznym miejscu na stronie internetowej. Notatka ta powinna jasno określać co użytkownik może robić z materiałem objętym prawami autorskimi i informować o podejmowaniu kroków prawnych w wypadku naruszenia tych praw. Przykładowe brzmienie uwagi o prawach autorskich, używanej przez państwo zawarte jest w załączniku do tego rozdziału.

2.6.4 Innym sposobem na zminimalizowanie ryzyka naruszenia praw autorskich jest zabezpieczanie przed kopiowaniem lub użycie oprogramowania zarządzającego prawami autorskimi np. generującego cyfrowy „znak wodny”.

– – – – – – – – – – – – – – – – – –

Załącznik do Rozdziału 2

PRZYKŁAD UWAGI O PRAWACH AUTORSKICH

Uwaga. – Poniższa notatka o prawach autorskich jest wykorzystywana przez Australię w internetowym systemie zobrazowania, zawierającym statyczne informacje lotnicze. Użyto jej tutaj za pozwoleniem firmy Airservices Australia.

Wszystkie materiały i publikacje służby informacji lotniczej („publikacje AIS") zapewnianej przez Airservices Australia, są objęte prawami autorskimi. Szczególnie odnosi się to do wszystkich elementów Zintegrowanego Pakietu Informacji Lotniczych („IAIP"). O ile nie określono inaczej, publikacje AIS można wykorzystywać tylko poprzez pobieranie, zobrazowanie lub drukowanie ich (w niezmienionej formie, co obejmuje ta uwaga) do celów informacyjnych. Cele informacyjne obejmują wykorzystanie operacyjne jednakże, z wyjątkiem przypadków określonych w ustawie o prawach autorskich z 1968 r., żadna część publikacji AIS nie może być reprodukowana, przechowywana w systemie pozyskiwania informacji, przesyłana, redystrybuowana, ponownie publikowana lub wykorzystywana w celach komercyjnych bez uprzedniego pisemnego zezwolenia Airservices Australia. Jeśli pożądane jest wykorzystanie jakiejkolwiek części publikacji AIS w sposób niedozwolony powyższą informacją, proszę kontaktować się z działem publikacji Airservices Australia, w celu uzyskania licencji.

Rozdział 3

ROZWAŻANIA TECHNICZNE

3.1 KATEGORIE WIADOMOŚCI

3.1.1 W normalnych warunkach protokół internetowy zabezpiecza integralność przesyłanych wiadomości. Jednakże Internet, jako medium publiczne, jest podatny na niektóre rodzaje ataków (np. ataki odmowy usług (DoS) lub wirusy komputerowe), które mogą w sposób znaczący spowalniać lub czasowo uniemożliwiać korzystanie z niego.

3.1.2 Schematy bezpieczeństwa informacyjnego mogą być wykorzystywane w celu zabezpieczenia autentyczności, integralności czy poufności wiadomości. Środki te jednak nie są w stanie zapobiec przeciążeniom sieci (spowodowanej czasowym dużym natężeniem ruchu czy celowymi zakłóceniami pracy sieci). W związku z tym, wykorzystanie Internetu dla celów operacyjnych w lotnictwie powinno mieć zastosowanie przy przesyłaniu wiadomości, informacji czy danych, dla których czas nie jest czynnikiem krytycznym.

3.1.3 Konieczne jest dokładne określenie, jakie kategorie informacji lotniczych spełniają powyższy warunek, a więc dla których czas nie jest czynnikiem krytycznym. Zgodnie z kategoriami wiadomości i ich priorytetami (w celu przesyłania przez AFTN) w Załączniku 10 do Konwencji o międzynarodowym lotnictwie cywilnym, Tom II, następujące kategorie wiadomości powinny zostać uznane jako te, dla których czas nie jest czynnikiem krytycznym i stąd odpowiednie do transmitowania przez Internet:

a) określone wiadomości MET (patrz rozdział 4 tego podręcznika);
b) wiadomości dotyczące regularności lotów;
c) określone wiadomości AIS (patrz rozdział 5 tego podręcznika);
d) plany lotów i powiązane z nimi wiadomości (patrz rozdział 5 tego podręcznika);
e) wiadomości administracyjne;
f) wiadomości serwisowe (o ile ma to zastosowanie).

3.1.4 Pomimo powyższego, niektóre rodzaje wiadomości dla statku powietrznego w locie, dla których czas jest czynnikiem krytycznym, nie muszą być za takie uznane, jeśli wykorzystywane są przed rozpoczęciem lotu. Dalszy opis wiadomości MET i AIS, dla których czas nie jest czynnikiem krytycznym, zawarty jest odpowiednio w rozdziale 4 i 5.

3.1.5 W przypadku gdy dane, dla których czas jest czynnikiem krytycznym są udostępniane tylko w celach informacyjnych, należy powiadomić użytkowników, że dane te powinny zostać pozyskane odpowiednią drogą w przypadku ich wykorzystania operacyjnego (np. przesyłania do statków powietrznych w trakcie lotu).

3.2 TREŚĆ

3.2.1 IASP musi wziąć pod uwagę materiał w kolejnych podpunktach, w przypadku tworzenia swoich usług.
\

3.2.2 Użytkownicy usługi muszą być powiadomieni o rodzajach informacji udostępnianych poprzez tę usługę. Na przykład użytkownicy szczególnie muszą być poinformowani jaka informacja jest dostępna poprzez usługę w celu upewnienia się, że posiadają wszystkie dane niezbędne dla ich operacji.

3.2.3 Akredytowane służby zapewniające informacje meteorologiczne powinny udostępniać, jako minimalny zestaw, wszystkie produkty wymagane przez Załącznik 3 do Konwencji o międzynarodowym lotnictwie cywilnym i dostępne w państwie, dla których czas nie jest czynnikiem krytycznym ze względu na bezpieczeństwo statków powietrznych w trakcie lotu, czy podczas przygotowania do lotu.

3.2.4 Użytkownicy muszą być poinformowani przez akredytowaną służbę o źródłach informacji, które są przez nią wykorzystywane.

3.2.5 Użytkownicy muszą być poinformowani o ważności informacji, która jest udostępniania.

3.2.6 Informacja historyczna, nie przeznaczona do użytku operacyjnego czy nieakredytowana, powinna być jasno oznaczona, jeśli jest udostępniana poprzez tę samą usługę co informacja operacyjna. Przykładem takiej informacji może być informacja, która straciła ważność czy informacja zarchiwizowana.

Uwaga. – Informacją nieakredytowaną może być informacja dodatkowa lub informacja udostępniana przez usługę, która jest w fazie opracowania lub dostępna w wersji testowej.

3.2.7 Procedury wyjaśniające w jaki sposób najlepiej korzystać z akredytowanych usług powinny zostać udostępnione użytkownikom.

3.3 OCENA I ZARZĄDZANIE RYZYKIEM

3.3.1. Akredytacja IASP opisana wcześniej powinna obejmować również posiadanie przez niego wdrożonego procesu oceny i zarządzania ryzykiem dla usług, które chce zapewniać.

3.3.2. Ocena i minimalizowanie ryzyka wymaga analiz środowiska systemowego w aspekcie fizycznym, logicznym, systematycznym i proceduralnym.

3.3.3. W celu zarządzania ryzykiem, które jest związane z zapewnianiem służby informacji lotniczej poprzez Internet, konieczne jest zrozumienie jakie są te ryzyka. Odbywa się to poprzez proces oceny ryzyka. Po określeniu ryzyka można podjąć odpowiednie działania związane z zarządzaniem ryzykiem i jego utrzymaniem na akceptowalnym poziomie (tzn. poziomie akceptowanym przez IASP i państwo akredytujące).

3.3.4. Wytyczne zawarte w tym rozdziale mają za zadanie uzupełnić standardowy proces zarządzania ryzykiem oraz odnieść się do kwestii typowych dla technologii informacyjnych.

3.3.5. Dalsze informacje na ten temat zawiera ISO/IEC 17799:2000 *Information Technology — Code of Practice for Information Security Management.*

3.3.6. Tematykę tę, w sposób odpowiedni dla osób bez wykształcenia technicznego, omawia publikacja *Secrets and Lies, Digital Security in a Networked World*. Bruce Schneier (John Wiley & Sons, Inc., 2004; ISBN: 0-471-45380-3).

3.4 PROCES OCENY RYZYKA

3.4.1 Proces oceny ryzyka należy przeprowadzić w następujących etapach:

a) identyfikacja zagrożonych zasobów oraz ich wartości, wynikiem czego jest często zdefiniowanie podatności;
b) określenie podatności tych zasobów;
c) identyfikacja zagrożeń dla tych zasobów;
d) identyfikacja źródeł zagrożeń;
e) wyznaczenie lub określenie prawdopodobieństwa zajścia danego zagrożenia i jego wpływu na zasoby;
f) identyfikacja wpływu zagrożenia na zasoby;
g) na podstawie wpływu i prawdopodobieństwa określenie ryzyka dla zasobów;
h) podjęcie decyzji o działaniach ograniczających ryzyko, jeśli jest ono na nieakceptowanym poziomie (np. środki bezpieczeństwa, zarówno techniczne jak proceduralne); oraz
i) powtórna ocena ryzyka w świetle działań ograniczających. Czy ograniczanie ryzyka było skuteczne/wystarczające?

3.4.2 Proces oceny ryzyka powinien zostać powtórzony po każdej zastosowanej strategii ograniczania ryzyka, aż do momentu osiągnięcia akceptowalnego poziomu ryzyka. Dodatkowo, proces oceny i zarządzania ryzykiem powinien być kontynuowany przez cały czas operacyjnego działania usługi. Należy również zauważyć, że wymagane działanie ograniczające będzie proporcjonalne do wartości chronionych zasobów. Każde zagrożenie powinno być opisane w następujących punktach: „zagrożenie", „źródło zagrożenia", „prawdopodobieństwo (zajścia)", „wpływ" i ostatecznie „ryzyko".

Identyfikacja zagrożonych zasobów

3.4.3 Przed zastosowaniem odpowiednich środków bezpieczeństwa, konieczne jest dokładne zrozumienie co będzie ochraniane. We wszystkich systemach do tego zaliczymy:

a) sam system włączając do tego sprzęt i oprogramowanie;
b) dane systemowe; oraz
c) dobre imię organizacji/marki.

3.4.4 Konieczne jest wzięcie pod uwagę połączeń sieciowych i związanego z tym przepływu danych do/z systemu. Każdy następny w łańcuchu system jest również zagrożony i konieczna jest dalsza ocena ryzyka dla tych systemów.

Identyfikacja podatności

3.4.5 Następujące czynniki stanowią o podatności typowego systemu na różne ataki:

a) ***Poufność***. Wrażliwość informacji czy zasobów na nieautoryzowany dostęp, klasyfikowana lub wyznaczana, pociągająca za sobą określony stopień szkody w przypadku wystąpienia nieautoryzowanego dostępu;

b) ***Integralność***. Wrażliwość informacji czy zasobów na zmianę lub zniszczenie;

c) ***Dostępność.*** Wrażliwość usługi zapewniającej informację czy dostęp do zasobów, w części dotyczącej braku jej gotowości operacyjnej;

d) ***Autentyczność.*** Wrażliwość usługi na nieuprawnionego użytkownika, który uzyskał dostęp do informacji czy zasobów.

Identyfikacja zagrożeń dla zasobów

3.4.6 Poniżej opisano zagrożenia powiązane z każdą podatnością:

a) ***Przechwycenie: zagrożenie dla „poufności”.*** Jest to zagrożenie w postaci kogoś uzyskującego nieautoryzowany dostęp do informacji. Czy jakaś osoba może uzyskać dostęp do informacji wrażliwej, do której oglądania nie jest uprawniona (np. z powodów prawnych czy handlowych)? Należy również rozważyć zagrożenie dla informacji, która jest przesyłana.

b) ***Modyfikacja, zagrożenie dla „integralności”.*** Zagrożenie to może stanowić ktoś penetrujący system lub dane. Czy na przykład ktoś może wprowadzić fałszywe dane i poprzez to uczynić prognozę niedokładną? Czy działanie systemu może być upośledzone tak, że pracuje on dalej, jednak dane na jego wyjściu są błędne? Czy dane umieszczone na platformie IASP mogą zostać zmodyfikowane? Czy integralność danych jest zagrożona podczas przesyłania z akredytowanego źródła do IASP; od IASP do użytkownika; od użytkownika do IASP (np. AFTN, składanie planów lotu, obserwacje pogody)? Czy jakakolwiek tego typu penetracja może zostać wykryta?

c) ***Przerwa w pracy, zagrożenie dla „dostępności”.*** Czy usługa jest zapewniana na odpowiednim poziomie dla celów operacyjnych? Czy jakość usługi będzie niższa w godzinach szczytu? Czy wykorzystanie zasobów może zostać zablokowane? Czy uprawnieni użytkownicy mogą zostać pozbawieni dostępu do usługi poprzez masowe wprowadzanie do niego błędnych danych (np. atak odmowy usług – DoS). Najczęstszym przykładem może być przeciążenie serwera wielką ilością żądań dostępu. W ten sposób uprawnieni użytkownicy nie mogą uzyskać dostępu do usługi.

d) ***Podszywanie się, zagrożenie dla „autentyczności”.*** Zagrożenie to pojawia się, gdy jedna osoba podszywa się pod inną. Przykładowo, w usłudze internetowej, czy możliwe jest zapewnienie, że „klienci” logujący się do usługi są rzeczywiście tymi za kogo się podają, ponieważ mogą być osobami usiłującymi uzyskać dostęp do usługi za darmo. Czy możliwa jest weryfikacja, że osoba uzyskująca dostęp na prawach administratora jest rzeczywiście uprawnionym administratorem? Czy użytkownicy mogą zweryfikować, że korzystają z „prawdziwej” usługi a nie z fałszywej, wprowadzonej przez atakującego? Może być szczególnie trudne potwierdzenie, w przypadku transmisji internetowych, że drugi korespondent jest tym za kogo, lub za co się podaje.

3.4.7 Wymienione zagrożenia mogą się ujawnić na wiele sposobów. Niektóre z nich wymieniono poniżej:

a) ***Dane/Informacje.*** Niedostępność, utrata, przechwycenie, zmiana, sfabrykowanie lub zniszczenie;

b) ***Ludzie/personel.*** Zaniedbanie, błąd, brak staranności, nieostrożność, lenistwo, sabotaż lub brak wiedzy;
c) ***Sieć (Intranet, Internet itd.***) Nieautoryzowany dostęp, konserwacja, uszkodzenie lub ataki (np. przechwycenie, żarty, podszywanie się, naruszenie integralności lub odmowa usług);
d) ***Sprzęt.*** Konserwacja, uszkodzenie (w tym zasilania) lub kradzież; oraz
e) ***Oprogramowanie i system.*** Przerwa w działaniu, modyfikacje/uaktualnienia lub nieprawidłowa praca.

Identyfikacja źródeł zagrożeń

3.4.8 Prawdopodobieństwo ataku i jego wpływu zależy od źródła ataku. Należy podzielić zagrożenia ze względu na ich źródło. Najprostszy podział potencjalnych źródeł zagrożeń jest następujący:

a) personel (zwykły);
b) personel (administratorzy);
c) konsultanci/kontrahenci;
d) rywale;
e) hakerzy (niewyszkoleni ale liczni);
f) hakerzy (elita, świetnie wyszkoleni);
g) politycznie umotywowane i zorganizowane jednostki;
h) zdarzenia naturalne.

Identyfikacja prawdopodobieństwa, że zagrożenie się urzeczywistni

3.4.9 Ta część oceny ryzyka jest subiektywna. Dwa czynniki, które należy tutaj rozważyć to:

a) ***Łatwość przeprowadzenia ataku***. Zależy to od wdrożonych środków bezpieczeństwa, rodzaju systemu i miejsca jego zainstalowania. Zależy to również od poziomu wyszkolenia źródła zagrożenia i wystąpienia odpowiedniej sposobności, jak również zasobów jakie posiada źródło zagrożenia. Wszystkie te czynniki mogą zmieniać się w czasie. Niektóre rodzaje ataków mogą się wydawać tylko teoretyczne lub bardzo trudne do przeprowadzenia, jednakże w przypadku opracowania narzędzia, które może je zautomatyzować, stają się łatwe do przeprowadzenia.
b) ***Motywacja źródła zagrożenia***. Dana osoba może podjąć atak, nie znaczy to jednak, że tak się stanie. Z tego powodu ważne jest zrozumienie motywów źródeł zagrożeń.

3.4.10 Przykładowo w typowej nowoczesnej organizacji, personel zwykły nie posiada bezpośredniego dostępu do jej serwera internetowego (tzn. jedyny sposób dostępu to poprzez przeglądarkę). W związku z tym, dla większości personelu przeprowadzenie ataku może być trudne (szczególnie jeśli wdrożono monitoring), nawet jeśli mają motywację w tym kierunku. Sytuacja „administratora systemu" jest inna. Nawet nieumyślnie, administrator systemu może spowodować znaczne szkody i przed takim atakiem nie ma praktycznie obrony. Tak więc administratorzy obdarzani są dużym kredytem zaufania.

3.4.11 Podobnie, słabo wyszkoleni hakerzy zawsze próbują atakować serwery internetowe. Ich motywacją jest to, że mogą się chełpić ilością systemów, które próbowali atakować. Jeśli oprogramowanie systemowe jest serwisowane i stale uaktualniane, ryzyko jest stosunkowo małe. W przypadku dobrze wyszkolonych hakerów istnieje wysokie prawdopodobieństwo

zaatakowania prawie każdego serwera. Pytaniem jest wtedy, który system zostanie zaatakowany?

3.4.12 Zjawiska naturalne (trzęsienia ziemi, powodzie i huragany), aczkolwiek rzadkie, mogą wpływać na zapewnianie usługi i także powinny zostać wzięte pod uwagę w procesie zarządzania ryzykiem.

Identyfikacja wpływu zagrożenia

3.4.13 Analiza w tym przypadku pozostaje ciągle subiektywna. Jej celem jest odpowiedź na pytania (tak wiele jak to możliwe) typu:

a) Ile będzie kosztować odzyskanie zniszczonych danych?
b) Jaka jest wartość danych?
c) Jaki jest koszt dobrej opinii organizacji?
d) Jakie są przewidziane kary umowne związane z umowami?
e) Jaki jest operacyjny wpływ utraty informacji lub braku informacji na użytkownika?

3.4.14 Wpływ zagrożenia lub poziom strat będzie oparty na czynnikach specyficznych dla systemu, włączając w to naturę zagrożenia, funkcjonalność systemu, jego interfejsy z systemami operacyjnymi, krytyczności zapewnianych danych, ciągłości działalności oraz użytkownika informacji.

Ocena ryzyka

3.4.15 Pod warunkiem, że wpływ zagrożenia oraz prawdopodobieństwo zostało określone w standardowej formie zarządzania ryzykiem (bardzo niskie/niskie/średnie/wysokie/bardzo wysokie), ryzyko może być określone w dokładnie taki sam sposób (tzn. jako produkt wpływu i prawdopodobieństwa, gdzie wpływ jest efektem jaki zagrożenie ma na system/organizację, a prawdopodobieństwo jest możliwością, że zagrożenie się ujawni – w zależności od rodzaju i źródła zagrożenia, biorąc pod uwagę poziom wyszkolenia i motywację).

Strategie ograniczania ryzyka

3.4.16 Biorąc pod uwagę wartość usługi lub stopień uszkodzenia usługi, szczególnie ważne jest zastosowanie odpowiedniej strategii ograniczania ryzyka. Przykładowo mały IASP, zapewniający informację przed lotem dla lotnictwa ogólnego, może wymagać znacznie mniej restrykcyjnych środków ograniczania ryzyka niż IASP, który zapewnia składanie planów lotu i odprawę przed lotem dla komercyjnych operatorów lotniczych. Pomimo związku pomiędzy zakresem strategii ograniczania ryzyka i wartością usługi, zawsze trzeba podjąć rozsądne środki, aby zapewnić integralność danych lotniczych.

3.4.17 Należy zauważyć, że zarządzanie uaktualnianiem aplikacji komputerowych jest najważniejszym czynnikiem strategii ograniczania ryzyka. Nie ma znaczenia jak dobrze system został zaprojektowany i zrealizowany, jeśli oprogramowanie jest nieaktualne (tzn. nie zainstalowano ostatniego dostępnego uaktualnienia), system będzie narażony na atak.

3.4.18 Strategie ograniczania ryzyka są grupowane ze względu na cechę, którą mają chronić. Główne cechy i możliwe strategie ograniczania ryzyka wymieniono poniżej:

a) poufność

1) uruchomić procesy w celu zapewnienia, że dane przechowywane przez instytucję zapewniającą usługę są przechowywane z zachowaniem poufności;
2) zapewnić, że projekt systemu, architektura sieciowa i procesy zarządzania zapewniają akceptowalne prawdopodobieństwo naruszeń dostępu;
3) zapewnić akceptowalne prawdopodobieństwo, że dane wrażliwe mogą zostać wykradzione podczas ich przesyłania od instytucji zapewniającej usługę do użytkownika końcowego, poprzez wprowadzenie kodowania danych, o ile jest to właściwe;
4) zapewnić akceptowalne prawdopodobieństwo, bazując na poziomie zagrożenia, że nieautoryzowany lub fałszywie autoryzowany użytkownik uzyska dostęp do strony internetowej;
5) implementacja mechanizmów autoryzacji opartych na nazwie użytkownika i haśle lub innych, o ile właściwe, bazując na poziomie zagrożenia;
6) implementacja procesu rejestracji i weryfikacji użytkownika, odpowiedniego do poziomu zagrożenia;
7) implementacja polityki odpowiedzialności użytkownika opartej na warunkach odpowiednich dla poziomu zagrożenia;
8) zapewnić odpowiednie zarządzanie hasłami; oraz
9) zapewnić bezpieczne rozlokowanie sprzętu.

b) integralność

Uwaga. – Załącznik 15 do Konwencji o międzynarodowym lotnictwie cywilnym, Rozdział 3, pkt 3.2.8 zawiera wymagania dotyczące integralności danych lotniczych, jako część systemu jakości.

1) zapewnić, że dane oryginalne pochodzą z bezpiecznego źródła;
2) zapewnić, że przeformatowanie lub modyfikacja danych oryginalnych nie naraża ich integralności;
3) zapewnić na odpowiednim poziomie prawdopodobieństwo, że dane mogą być zmodyfikowane podczas ich przesyłania pomiędzy źródłem a instytucją zapewniającą usługę poprzez:
   i) zapewnienie na odpowiednim poziomie prawdopodobieństwa, że dane przechowywane przez instytucję zapewniającą usługę nie będą sfałszowane;
   ii) zapewnienie na odpowiednim poziomie prawdopodobieństwa, że dane mogą zostać zmienione podczas ich przesyłania pomiędzy instytucją zapewniającą usługę a użytkownikiem;
   iii) zapewnienie, że w przypadku uszkodzenia danych przechowywanych przez instytucję zapewniającą usługę, zostaną one zastąpione przez dane nieuszkodzone;
   iv) zapewnienie na odpowiednim poziomie prawdopodobieństwa, że przechowywane dane zostaną zaatakowane przez stronę internetową; oraz
   v) zapewnienie, że przechowywane są pliki rejestrujące (logi) transakcje z użytkownikami, w celach dowodowych (powinno być możliwe odtworzenie historii dostępu do produktów, w celu

weryfikacji co otrzymał użytkownik, jeśli produkty nie są archiwizowane).

c) dostępność
   1) implementacja porozumienia SLA (*service level agreement*) z dostawcą usług internetowych – ISP (włączając w to serwisowanie), które zapewni dostępność odpowiednią do ważności strony internetowej;
   2) zapewnienie, że projekt systemu przewiduje rezerwy odpowiednie do ważności strony internetowej;
   3) zapewnienie, że projekt systemu, architektura sieciowa i procesy zarządzania zapewniają akceptowalne prawdopodobieństwo, że platforma może być zablokowana przez złośliwy atak (np. działalność hakerów, wirusy, robaki internetowe, odmowa usług, dystrybuowana odmowa usług, zjawiska naturalne jak powódź);
   4) zapewnienie, że projekt systemu, architektura sieciowa, proces zarządzania i szkolenia utrzymają na akceptowalnym poziomie prawdopodobieństwo, że platforma może zostać uszkodzona przez działania zgodne z zasadami; oraz
   5) implementacja procesu wyrażania opinii przez użytkowników, w celu zapewnienia, że kwestie związane z wydajnością są identyfikowane i przekazywane instytucji zapewniającej usługę.

d) autentyczność
   1) zapewnienie użytkownikowi łatwej weryfikacji, że instytucja zapewniająca usługę jest akredytowana (dla państwa, gdzie użytkownik chce rozpocząć podróż);
   2) zapewnienie użytkownikowi weryfikacji, że instytucja zapewniająca usługę jest tym za kogo się podaje; oraz
   3) zapewnienie, w razie konieczności, weryfikacji użytkownika przez instytucję zapewniającą usługę.

3.4.19 Dodatkowo, o ile to jest niezbędne, IASP powinien być w stanie zapewnić (udowodnić), że użytkownik otrzymał odpowiednią informację.

3.4.20 Po zakończeniu wstępnej oceny ryzyka, proces zarządzania ryzykiem powinien przejść do fazy cyklicznej, gdzie rozważa się wprowadzenie działań ograniczających ryzyko oraz powtórnie przeprowadza jego ocenę aż do chwili, gdy IASP (i państwo akredytujące) zapewni ryzyko na akceptowalnym poziomie. Dodatkowo, w trakcie działania usługi zostaną ujawnione nowe ryzyka. Proces zarządzania ryzykiem powinien je objąć i powtórnie dokonać oceny istniejących oraz nowych ryzyk, w świetle dostępnych informacji i dobrych praktyk.

3.4.21 W załączniku do tego rozdziału zawarto zagrożenia oraz strategie zarządzania ryzykiem, jak również sugestie dotyczące najlepszych praktyk wdrażających je w środowisku technologii informacyjnych.

3.4.22 Dodatkowo, the Open Web Application Security Project (OWASP) (http://www.owasp.org), The Ten Most Critical Web Application Security Vulnerabilities, 2004 Update, zawiera pewną liczbę działań zapobiegających słabym punktom w aplikacjach internetowych.

– – – – – – – – – – – – – – – – – –

Załącznik do Rozdziału 3

AKTUALNE NAJLEPSZE PRAKTYKI DOTYCZĄCE STRATEGII OGRANICZANIA RYZYKA W ŚRODOWISKU TECHNOLOGII INFORMACYJNYCH (IT)

Uwaga. – Postęp technologii internetowych jest szybki, rozwiązania technologiczne wymienione w kolumnie „Najlepsze aktualne praktyki" należy traktować jako przykłady, aktualne w czasie publikacji dokumentu.

Strategia ograniczania ryzyka	Kategoria	Aktualna najlepsza praktyka	Do zastosowania w przypadku gdy wpływ jest	
			Mały	Duży
Implementacja autentyfikacji użytkownika odpowiedniej do poziomu zagrożenia	Autentyczność	• Anonimowy dostęp użytkownika	X	
		• Wymagane hasło i login (nazwa) użytkownika	X	
		• Nazwa użytkownika i hasło z oddzielnym PIN dla określonych funkcji		X
		• Certyfikat cyfrowy (np. SSL)		X
		• Bezpieczny protokół transmisji (https)		X
		• RSA Securit		X
		• VPN, zintegrowany z systemem		X
		• Oprogramowanie klienta (autentyfikacja tokenem)		X
Implementacja rejestracji użytkownika oraz procesu jego weryfikacji odpowiednio do poziomu zagrożenia	Autentyczność	• Rejestracja online bez weryfikacji	X	
		• Rejestracja w formie papierowej bez weryfikacji	X	
		• Rejestracja online z weryfikacją		X
		• Rejestracja w formie papierowej z weryfikacją		X
		• Rejestracja online z danymi dostępowymi przesyłanymi inną drogą (pocztą, emailem), w celu zapewnienia identyfikacji zarejestrowanego użytkownika		X
Implementacja regulaminu dla użytkowników odpowiedniego do poziomu zagrożenia	Autentyczność	• Utrzymywanie hasła w tajemnicy, nie przekazywanie go innym	X	
		• Każdorazowe pełne wylogowanie ze strony	X	
		• Udzielanie rad instytucji zapewniającej usługę w sprawie zmian odpowiednich informacji	X	
Implementacja kodowania danych odpowiedniego do poziomu poufności	Integralność	• HTTPS, SSL	X	
		• PKI (i inne)		X
Utrzymanie na akceptowalnym poziomie prawdopodobieństwa modyfikacji danych, które są przesyłane od źródła do instytucji zapewniającej usługę	Integralność	• Użycie Internetu z odpowiednim kodowaniem i autentyfikacją (HTTPS, SSL)	X	
		• Użycie sieci prywatnej lub wirtualnej sieci prywatnej (VPN) do przesyłania danych z bezpiecznego źródła. Nie należy używać publicznego Internetu bez odpowiednio zabezpieczonego połączenia VPN		X
Utrzymanie na akceptowalnym poziomie prawdopodobieństwa, że dane przechowywane przez instytucję zapewniającą usługę, zostaną zmienione Utrzymanie na akceptowalnym poziomie prawdopodobieństwa, że	Integralność	• Użycie zapory programowej (firewall) oraz specjalnej infrastruktury; uniemożliwienie bezpośredniego dostępu do danych	X	
		• Zastosowanie zapór sprzętowych, serwerów proxy, systemów zabezpieczających przez penetracją serwera (HIPS) oraz systemów wykrywania ataków sieciowych (NIDS), o ile jest to wskazane		X
		• Zastosowanie podwójnych zapór, każdej od innego producenta, w celu eliminacji słabych punktów instytucji zapewniającej usługę		X
		• Weryfikacja dostawcy – certyfikat cyfrowy		X

Strategia ograniczania ryzyka	Kategoria	Aktualna najlepsza praktyka	Do zastosowania w przypadku gdy wpływ jest	
			Mały	Duży
dane zostaną zmienione podczas ich przesyłania od instytucji zapewniającej usługę do użytkownika Utrzymanie na akceptowalnym poziomie prawdopodobieństwa, że dane mogą zostać zaatakowane poprzez stronę internetową		• Eliminacja możliwości ataku typu „man-in-the-middle" (przechwycenie i modyfikacja przesyłanej informacji bez wiedzy stron) i zapewnienie przekazywania informacji bezpośrednio do użytkowników (zapewnia to SSL) • Umieszczanie zapory pomiędzy serwerem internetowym a serwerem aplikacji (jeśli jest) i magazynem danych, w celu utworzenia stref DMZ (zdemilitaryzowanych) • Użycie stref DMZ w celu oddzielenia komponentów funkcjonalnych (tzn. serwera internetowego, serwera aplikacji, serwera bazy danych)		X X X
Zapewnienie, że w przypadku zniszczenia danych przechowywanych przez instytucję zapewniającą usługę, dane mogą zostać odtworzone Zapewnienie przechowywania logów czasowych, rejestrujących transakcje z użytkownikiem dla celów dowodowych (powinna istnieć możliwość odtworzenia, do jakich produktów uzyskiwano dostęp, w celu weryfikacji co użytkownik otrzymał, w przypadku nie archiwizowania produktów)	Integralność	• Przechowywanie plików logów w uniwersalnych formatach, takich jak ASCII • Podpisywanie cyfrowo plików logów • Zapewnienie, że system i systemy zabezpieczeń danych są kontrolowane w sposób bezpieczny • Zapewnienie, że systemy zabezpieczeń są przechowywane w strefie bezpiecznej • Zapewnienie archiwizowania danych poza stroną internetową, w celu ich ewentualnego odtworzenia	X	X X X X
Implementacja procesu wyrażania opinii przez użytkowników, w celu zapewnienia, że uwagi użytkowników są identyfikowane i przetwarzane	Wszystkie	• Obsługa klienta z serwisem telefonicznym i systemem śledzenia raportów o problemach • System wyrażania opinii oraz śledzenia raportów o problemach działający w oparciu o pocztę internetową	X	X
Zapewnienie użytkownikowi łatwego sprawdzenia, że instytucja zapewniająca usługę jest akredytowana (dla państwa, gdzie użytkownik chce rozpocząć podróż) Zapewnienie użytkownikowi łatwego sprawdzenia, że instytucja zapewniająca usługę jest tym za kogo się podaje Zapewnienie, o ile to konieczne, weryfikacji użytkownika przez	Poufność	• Weryfikacja użytkownika poprzez nazwę i hasło • Weryfikacja użytkownika poprzez certyfikat cyfrowy • Weryfikacja instytucji zapewniającej usługę poprzez certyfikat cyfrowy • Eksponowanie na stronie oficjalnego logo, potwierdzającego akredytację (wskazanie w jakim państwie) • Utworzenie hiperłącza łączącego logo ze stroną państwowej władzy akredytacyjnej. Strona państwowej władzy akredytacyjnej powinna zawierać szczegóły na temat jaką usługę dana akredytowana instytucja zapewnia, datę uzyskania oraz datę ważności akredytacji	X X X X	X

Strategia ograniczania ryzyka	Kategoria	Aktualna najlepsza praktyka	Do zastosowania w przypadku gdy wpływ jest	
			Mały	Duży
instytucję zapewniająca usługę				
Implementacja porozumień SLA (Service Level Agreement) z dostawcą usług internetowych (ISP) oraz na konserwację systemu, co zapewni dostępność odpowiednią dla wagi strony internetowej	Dostępność	• Zawarcie porozumienia SLA z dostawcą usług internetowych (ISP), które zawiera kwestie dostępności usługi, przerw w dostępie do niej oraz szerokości pasma	X	
		• Zawarcie umowy na serwisowanie sprzętu i infrastruktury, która zawiera elementy porozumienia SLA	X	
		• Zapewnienie, że wybrany dostawca usług internetowych (ISP) jest w stanie dostarczyć odpowiednie pasmo dostępu, rezerwując pasmo dodatkowe w przypadku przewidywanego wzrostu zapotrzebowania	X	
Zapewnienie, że projekt systemu umożliwia pojemność i elementy nadmiarowe odpowiednie do wagi strony internetowej	Dostępność	• Minimalizacja liczby przypadków, kiedy może nastąpić awaria lub minimalizacja wpływu każdej z możliwych do wystąpienia awarii	X	
		• Utrzymywanie elementów zapasowych podejmujących natychmiast pracę zamiast uszkodzonych (hot standy)/ elementów zapasowych możliwych do zastosowania (cold standy)/ części zapasowych (o ile istnieje potrzeba) dla kluczowej infrastruktury (serwery, routery itd.) tak, aby uszkodzenia mogły być odpowiednio rozwiązane	X	
		• Określenie wymagań pojemnościowych dla systemu (poprzez zastosowanie najlepszych praktyk w zakresie projektowania i testowania obciążenia systemu)	X	
		• Ustalenie rozmiarów infrastruktury odpowiednio do określonej pojemności		X
		• Zastosowanie clusterów serwerów/ farm serwerów oraz systemów balansowania obciążenia	X	
		• Zastosowanie dysków w systemie hot-swap (szybka wymiana dysku uszkodzonego na nowy) / matryc dyskowych RAID, w celu minimalizacji wpływu uszkodzenia dysku		X
		• Zastosowanie podwójnych (zduplikowanych) magazynów danych		X
		• Zastosowanie zdublowanej infrastruktury sieciowej (włączając połączenie z Internetem zapewniane przez ISP) – nie jest konieczne korzystanie z dwóch firm w przypadku, gdy jedna jest w stanie zapewnić odpowiednią infrastrukturę		X
		• Zawarcie dwóch kontraktów na sprzęt i infrastrukturę sieciową z dostawcami (o ile nie występuje konieczność z producentami) – na wypadek bankructwa lub inny	X	
		• Zastosowanie serwerów zasilanych bez przerwy (UPS), w celu uniknięcia krótkich braków zasilania		X
		• Zastosowaniu systemów UPS zasilanych z generatorów spalinowych, w celu uniknięcia dłuższych okresów braku zasilania		X
		• Utrzymywanie kompletnej infrastruktury rezerwowej, na wypadek klęski żywiołowej, w celu zapewnienia nieprzerwanego świadczenia usług	X	
Zapewnienie, że projekt systemu, architektura sieciowa i procesy zarządzania zapewniają akceptowalne prawdopodobieństwo, że platforma może być zablokowana przez złośliwy atak (np. działalność hakerów,	Dostępność	• Implementacja strategii wzmocnienia systemu, która zapewnia wzmocnienie systemu do określonego poziomu poprzez usunięcie lub wyłączenie wszystkich części składowych nie wymaganych dla jego działania. Można do tego zaliczyć ograniczenia dostępu (porty i protokoły), ograniczanie liczby użytkowników, stosowanie haseł, kontroli dostępu, uprawnień użytkownika lub grup użytkowników oraz wykrywanie prób włamania	X	
		• Zastosowanie strategii uaktualniania oprogramowania.		

3-13 Wytyczne w sprawie wykorzystania Internetu w zastosowaniach lotniczych

Strategia ograniczania ryzyka	Kategoria	Aktualna najlepsza praktyka	Do zastosowania w przypadku gdy wpływ jest	
			Mały	Duży
wirusy, robaki internetowe, odmowa usług, dystrybuowana odmowa usług, powódź itd.) Zapewnienie, że projekt systemu, architektura sieciowa, proces zarządzania i szkolenia utrzymają na akceptowalnym poziomie prawdopodobieństwo, że platforma może zostać uszkodzona przez działania zgodne z zasadami		Programy są odpowiednio uaktualniane i serwisowane		X
		• Zastosowanie komponentów sprzętowych przeciwko atakom DoS (odmowa usług) – filtry pakietów / „bezpieczne" routery	X	
		• Zapewnienie, że stosowane jest oprogramowanie antywirusowe oraz, że jest ono aktualne		X
		• Zastosowanie oprogramowania antywirusowego od różnych dostawców, w celu zredukowania wrażliwości instytucji zapewniającej usługę	X	
		• Identyfikacja oczekiwanych schematów dostępu / użytkowania oraz natężenia ruchu	X	
		• Ocena szerokości pasma potrzebnej do zabezpieczenia danych schematów użytkowania oraz natężenia ruchu	X	
		• Zdefiniowanie odpowiednich procedur testowych w celu zapewnienia, że zastosowane udoskonalenie usługi jest w pełni funkcjonalne i nie wpływa negatywnie na jej zapewnianie	X	
		• Zdefiniowanie odpowiednich procedur ulepszania systemu w celu zapewnienia, że po wprowadzeniu ulepszenia jest ono funkcjonalne oraz nie wpływa negatywnie na zapewnianie usługi		X
		• Zapewnienie, że nie są możliwe sesje równoległe dla tego samego konta użytkownika, realizowane z różnych adresów IP		X
		• Zastosowanie zautomatyzowanej aplikacji o wysokiej niezawodności (fail-safe), która powinna być dostępna w przypadku braku dostępu do strony głównej usługi		X
		• Zastosowanie odpowiedniego szkolenia personelu oraz procedur rozwoju, rozbudowy i serwisowania usługi		X
		• Całodobowe, ciągłe monitorowanie infrastruktury oraz oprogramowania. Zastosowanie dobrze zdefiniowanych działań naprawczych, w celu rozwiązania powstałych problemów		X

Rozdział 4

KWESTIE ODNOSZĄCE SIĘ DO INFORMACJI METEOROLOGICZNEJ

4.1 WPROWADZENIE

Zgodnie z Załącznikiem 3 do Konwencji o międzynarodowym lotnictwie cywilnym – *Służba meteorologiczna dla międzynarodowej żeglugi powietrznej*, państwa sygnatariusze Konwencji zobowiązują się do zapewniania usług, które minimalnie zawierają obserwacje i prognozy potrzebne do zabezpieczenia podejmowania decyzji operacyjnych w centrach kontroli obszaru, centrach informacji powietrznej, przez operatorów lotniczych, załogi samolotów czy dowódców załóg. Celem tego rozdziału jest identyfikacja informacji meteorologicznej, która może być zapewniana przez Internet i w jakim zakresie.

4.2 INFORMACJE METEOROLOGICZNE, DLA KTÓRYCH CZAS JEST CZYNNIKIEM KRYTYCZNYM

4.2.1 Informacje meteorologiczne wymienione w pkt 4.2.2 nie powinny być wykorzystywane do podejmowania decyzji operacyjnych, dla których czas jest czynnikiem krytycznym, bez względu na to czy ma to miejsce w trakcie lotu, czy bezpośrednio przed startem. Informacja ta powinna być określana jako informacja meteorologiczna, dla której czas jest czynnikiem krytycznym. Informacja ta powinna być przesyłana poprzez stałą sieć lotniczą (AFS), ponieważ charakterystyki tej sieci zapewniają otrzymanie tej informacji na czas.

4.2.2 Zgodnie z Załącznikiem 10 do Konwencji o międzynarodowym lotnictwie cywilnym – *Telekomunikacja lotnicza*, Tom II, informacje i produkty zawierające lotniczą informację meteorologiczną dzieli się na dwie kategorie, „depesze dotyczące bezpieczeństwa lotów" oraz „depesze meteorologiczne". Depesze dotyczące bezpieczeństwa lotów w zakresie meteorologii lotniczej, dla których można przyjąć, że czas jest czynnikiem krytycznym to:

a) informacje SIGMET;
b) informacje AIREP;
c) informacje AIRMET;
d) informacje na temat popiołów wulkanicznych;
e) informacje na temat cyklonów tropikalnych; oraz
f) zmiany do prognoz TAF.

4.3 INFORMACJE METEOROLOGICZNE, DLA KTÓRYCH CZAS NIE JEST CZYNNIKIEM KRYTYCZNYM

4.3.1 Następujące informacje meteorologiczne są uważane za informacje, dla których czas nie jest czynnikiem krytycznym i mogą być zapewniane przez Internet:

a) informacje meteorologiczne dotyczące prognoz np. TAF, prognoz obszarowych i trasowych, oraz obserwacji takich jak komunikaty METAR oraz SPECI;
b) informacje meteorologiczne zapewniane przez światowe centra prognoz (*World Area Forecast Centres*) np. mapy znaczących zjawisk pogodowych, wiatrów, temperatury i wilgotności względnej;
c) informacje na temat popiołów wulkanicznych w postaci graficznej (VAG) dostarczane przez centra informacji o popiołach wulkanicznych;
d) prognozy obszarowe GAMET; oraz
e) prognozy trasowe (ROFOR).

Uwaga. – Powyższa lista może zawierać również reprezentację danych meteorologicznych w uniwersalnej postaci binarnej (BUFR) oraz przetworzone dane meteorologiczne prezentowane w formacie przedstawiającym wartości dla współrzędnych punktów, wyrażone w postaci binarnej (GRIB).

4.3.2 Usługi dla operatorów oraz załóg lotniczych, w celu planowania lotu pod centralnym nadzorem operacyjnym są uważane za takie, dla których czas nie jest czynnikiem krytycznym. Informacja meteorologiczna do planowania lotu przez operatorów może zawierać:

a) aktualne i prognozowane wiatry górne, temperaturę górnych warstw powietrza aż do wysokości tropopauzy, informacja o wiatrach maksymalnych oraz zmiany do wymienionych informacji;
b) bieżące i prognozowane znaczące zjawiska pogodowe na trasie oraz informacje o prądach strumieniowych, jak również wszelkie zmiany w tym zakresie;
c) prognozy na start;
d) komunikaty METAR oraz, jeśli są dostępne, SPECI dla lotniska startu, lotnisk zapasowych na trasie, lotniska lądowania oraz zapasowych lotnisk lądowania, zgodnie z ustaleniami w regionalnym porozumieniu o żegludze powietrznej;
e) prognozy TAF oraz zmiany do nich dla lotniska startu, lotnisk zapasowych na trasie, lotniska lądowania oraz zapasowych lotnisk lądowania, zgodnie z ustaleniami w regionalnym porozumieniu o żegludze powietrznej; oraz
f) informacje SIGMET oraz informacje AIREP, odpowiednie do rozważanych tras, zgodnie z ustaleniami w regionalnym porozumieniu o żegludze powietrznej.

Rozdział 5

KWESTIE ZWIĄZANE ZE SŁUŻBĄ INFORMACJI LOTNICZEJ (AIS)

5.1 WPROWADZENIE

5.1.1 Celem tego rozdziału jest identyfikacja informacji lotniczych, które mogą być zapewniane przez Internet i w jakim kontekście może się to odbywać.

5.1.2 Normy i zalecane metody postępowania (SARPs) Załącznika 15 do Konwencji o międzynarodowym lotnictwie cywilnym – *Służby Informacji Lotniczej*, Załącznika 4 do Konwencji o międzynarodowym lotnictwie cywilnym – *Mapy lotnicze* oraz wytyczne zawarte w *Aeronautical Information Services Manual* (Doc 8126), zostały wprowadzone w celu jednolitości i zgodności w zakresie zapewniania informacji lotniczych.

5.1.3 Aczkolwiek służba informacji lotniczej zapewniana przez Internet może być dostosowana dla potrzeb zabezpieczenia operacyjnych potrzeb użytkowników (personel związany z operacjami lotniczymi włączając w to załogi, planowanie lotów, symulatory lotów, jak również jednostki służb ruchu lotniczego odpowiedzialne za służbę informacji powietrznej i służby odpowiedzialne za odprawę przed lotem), to powinna ona spełniać wymagania wyżej wymienionych norm.

5.1.4 System zarządzania jakością powinien być wdrożony, w celu upewnienia użytkowników, że zapewniana informacja lotnicza spełnia wymagania w zakresie jakości i możliwości jej prześledzenia (Załącznik 15 do Konwencji o międzynarodowym lotnictwie cywilnym, Rozdział 3, pkt 3.2.5).

5.2 INFORMACJE LOTNICZE, DLA KTÓRYCH CZAS JEST CZYNNIKIEM KRYTYCZNYM

5.2.1 Następujące informacje lotnicze uważane są za takie, dla których czas jest czynnikiem krytycznym i podczas ich przesyłania przez Internet nie powinny być wykorzystywane do podejmowania decyzji operacyjnych, bez względu na to czy ma to miejsce w trakcie lotu czy bezpośrednio przed odlotem:

a) informacja dynamiczna o charakterze czasowym, taka jak aktualne krajowe i międzynarodowe NOTAM (w tym SNOWTAM, ASHTAM oraz listy kontrolne); oraz
b) inne informacje o pilnym charakterze, udostępniane załogom w formie biuletynu informacji przed lotem (PIB).

5.2.2 Załącznik 15 do Konwencji o międzynarodowym lotnictwie cywilnym, Rozdział 5, pkt 5.3.2.1 określa, że kiedykolwiek jest to możliwe, do dystrybucji NOTAM jest używana AFS (stała służba lotnicza).

5.2.3 W zapewnianych biuletynach informacji przed lotem lub produktach formatem i graficznie przystosowanych dla potrzeb klienta, powinny się przynajmniej znaleźć informacje, które są dostępne w dokumentach papierowych, służących do ich opracowania.

5.3 INFORMACJE LOTNICZE, DLA KTÓRYCH CZAS NIE JEST CZYNNIKIEM KRYTYCZNYM

Następujące podstawowe, statyczne informacje AIS są uważane za takie, dla których czas nie jest czynnikiem krytycznym i mogą być dostarczane przez Internet:

a) ***Informacje Statyczne***. Informacje wydawane na stałe lub o długim czasie trwania, takie jak:
   1) Zbiór Informacji Lotniczych (AIP) (zawierający informacje o lotniskach, szczegółowy opis rejonów informacji powietrznej (FIR), pomocy nawigacyjnych, mapy, schematy, dane o przeszkodach, drogi lotnicze itd.);
   2) Zmiany do AIP, zarówno zmiany w cyklu AIRAC jak i zmiany zwykłe;
   3) Suplementy do AIP, zarówno w cyklu AIRAC jak i zwykłe;
   4) Biuletyny Informacji Lotniczych (AIC);
   5) Miesięczne, drukowane zestawienie ważnych NOTAM, zawierające również numery ostatnich zmian do AIP, wydanych AIC oraz listę kontrolną Suplementów do AIP; oraz
   6) NOTAM z listą kontrolną ważnych NOTAM, wydawany co miesiąc, który zawiera również numery ostatnich Zmian do AIP, Suplementów do AIP oraz przynajmniej AIC dystrybuowanych międzynarodowo.

b) ***Informacje podstawowe***. Dane wymagane do umożliwienia przetwarzania innych informacji, które mogą się składać z danych stałych, o długim czasie trwania lub danych statycznych nie dostarczanych użytkownikom (listy odniesień, drogi specjalne/zwykłe, pliki dystrybucyjne, kryteria selekcji, kryteria powiązane).

5.4 ZAPEWNIANIE INFORMACJI STATYCZNYCH I PODSTAWOWYCH

5.4.1 Informacja statyczna i podstawowa, może być informacją zarówno stałą, jak i o długim czasie trwania. Musi być określona data wejścia informacji w życie. Każda publikacja powinna zawierać datę. Jeżeli poszczególne strony mają inne daty wejścia w życie, każda strona powinna tę datę zawierać. W przypadku, gdy elementy danych lotniczych są publikowane niezależnie, muszą posiadać datę wejścia w życie.

5.4.2 Wspólne daty wejścia w życie, ustalone co 28 dni zgodnie z systemem regulacji AIRAC, mają być używane do publikacji informacji zawartej w Dodatku 4, Część 1, Załącznika 15 do Konwencji o międzynarodowym lotnictwie cywilnym i również są zalecane przy publikacji informacji zawartej w Części 2 Dodatku 4 (szczegóły w Rozdziale 6 Załącznika 15). W celu ułatwienia, w okresie przejściowym pomiędzy datą wejścia w życie a następną datą publikacji (zgodnie z AIRAC) informacja lotnicza bieżąca, informacja z

poprzedniego cyklu i następnego cyklu, powinna być udostępniona przez określony czas. W przypadku uruchomienia takiego systemu, szczególnie ważna jest kwestia jasnego oznaczenia dat wejścia w życie dla wszystkich dostępnych informacji.

5.4.3 Internet może być użyty w celu zapewniania informacji zgodnie z systemem AIRAC. Powinny jednak być kontynuowane odpowiednie formy dystrybucji informacji drukowanej (Załącznik 15, pkt 6.2). System AIRAC został wprowadzony po to, aby planowana do wprowadzenia informacja dotarła do użytkowników: instytucji dystrybuujących informacje lotnicze, firmy lotnicze, produkujące mapy i bazy danych itd. Wymagane jest zachowanie poufności (patrz Rozdział 3 tego podręcznika). Organizacje rozważające dostarczanie informacji lotniczych powinny się upewnić, że użytkownicy są zapoznani z systemem AIRAC i rozumieją daty wejścia w życie, powiązane z informacją.

5.5 ZAPEWNIANIE MAP

5.5.1 Normy Załącznika 4 i 15 do Konwencji o międzynarodowym lotnictwie cywilnym odnoszą się do zawartości i układu graficznego map wymienionych w Załączniku 4 oraz innych map w AIP, włączając w to mapy udostępniane przez służby informacji lotniczej państwa przez Internet. Mapy powinny być dostępne w skalach określonych przez Załącznik 4. Jeśli dozwolone jest skalowanie mapy, użytkownicy powinni zostać poinformowani o skali, do jakiej zachowana jest jakość mapy. Przewiduje się, że w krótkim czasie większość map udostępnianych przez Internet będzie dostępna w identycznej prezentacji graficznej jak obecne ich kopie papierowe. Należy jednak zauważyć, że przy pomocy niektórych systemów informacji kartograficznej i geograficznej (GIS) możliwe jest wytwarzanie map w formatach zapewniających większą funkcjonalność, włączając w to możliwość kontroli przez użytkownika rodzajów wyświetlanej informacji. W przypadku udostępniania takich elektronicznych map, należy po ich wyświetleniu (po raz pierwszy) zapewnić zobrazowanie wszystkich dostępnych informacji. Informacje o krytycznym znaczeniu dla bezpieczeństwa muszą być zawsze wyświetlane (niemożliwe jest ich wyłączenie).

5.5.2 Optymalne formaty graficzne używane do produkcji map umieszczanych w Internecie mogą być różne od tych stosowanych do tworzenia dokumentów i powinny zostać wybrane, uwzględniając poniższe:

a) dostępność opcji zobrazowania graficznego z programów kartograficznych lub skanerów;
b) dostępność wyprodukowanych map dla klientów (kompatybilność z systemami operacyjnymi, przeglądarkami internetowymi, kolorowanie i drukowanie);
c) funkcjonalność map i jakość obrazu;
d) wielkość pliku danych mapy (i związany z tym czas transmisji); oraz
e) format otwarty lub komercyjny, powiązany z odpowiednimi kosztami.

Rozdział 6

KWESTIE ODNOSZĄCE SIĘ DO PLANÓW LOTU

6.1 WPROWADZENIE

6.1.1 Celem tego rozdziału są wytyczne w sprawie składania i zarządzania planami lotów (z i do stałej służby lotniczej (AFS)) poprzez Internet.

6.1.2 Internet może służyć jako środek zapewniania aplikacji, służących do składania i zbierania planów lotu bezpośrednio od użytkowników. Dodatkowo Internet pozwala na implementację mechanizmów, które powiadamiają użytkownika o akceptacji planów lotu i pozwalają następnie na modyfikacje/odwołanie złożonych planów lotu. Aplikacje internetowe obsługujące plany lotów są często dostępne w połączeniu z aplikacjami MET i AIS, zapewniając pełny zestaw informacji lotniczych.

6.2 SKŁADANIE PLANÓW LOTU

6.2.1 Standardowy format planu lotu i kryteria walidacji opisane w *Procedurach Służb Żeglugi Powietrznej – Zarządzanie Ruchem Lotniczym* (PANS-ATM, Doc 4444) mają być stosowane.

6.2.2 Wykorzystanie Internetu do składania planów lotu może zredukować nakład pracy ręcznej służb ruchu lotniczego, poprzez zaoferowanie użytkownikowi aplikacji zbierających poprawne składniowo plany lotów i w sposób bezpieczny przesyłających je do dalszych etapów przetwarzania w środowisku operacyjnym.

6.2.3 Trzeba zauważyć, że system może być narażony na ataki odmowy usług (DoS) poprzez taki interfejs internetowy. Jeśli jest możliwe składanie nieograniczonej liczby planów lotu, możliwe jest zablokowanie możliwości złożenia planu lotu przez użytkownika uprawnionego. Dodatkowo, we w pełni zautomatyzowanym systemie, możliwe jest również oddziaływanie na system operacyjny. Wymagane jest zastosowanie ręcznych lub automatycznych procedur kontrolnych, w celu zredukowania ryzyka ataku DoS.

6.2.4 Składanie planów lotu przez Internet może być łatwo rozszerzone w odniesieniu do lotów, na które nie ma potrzeby ich składać. Przykładowo, może to zapewnić możliwość monitorowania lotów VFR wykonywanych w celu poszukiwania i ratownictwa.

6.3 ZARZĄDZANIE PLANAMI LOTÓW

6.3.1 Internet może zapewnić użytkownikowi bezpośrednią wiedzę na temat akceptacji, zmian lub odrzucenia planów lotu, w sposób zautomatyzowany i kontrolowany, w czasie rzeczywistym, w zależności od dostępnych środków telekomunikacyjnych i wymaganych interfejsów.

6.3.2 Informacja o akceptacji planu lotu powinna być udostępniona użytkownikowi, umożliwiając następnie konsultacje i modyfikację/odwołanie złożonego planu lotu. Głównym

zagrożeniem dla systemu operacyjnego jest brak kompatybilności aplikacji internetowych z odpowiednimi interfejsami AFS.

Rozdział 7

INNE ZASTOSOWANIA

7.1 PRZESYŁANIE INFORMACJI AFTN

7.1.1 Przyjmuje się, że użycie Internetu jako alternatywnego środka łączności służącego do przesyłania wiadomości AFTN pomiędzy państwami, ma miejsce w wypadkach wyjątkowych (np. w przypadku, gdy odpowiednie linie łączności są niedostępne/niesprawne lub utrzymywanie ich się nie opłaca, z powodu małego natężenia ruchu).

7.1.2 W przypadku implementacji łączności typu AFTN w Internecie, powinny być przestrzegane normy Załącznika 10 do Konwencji o międzynarodowym lotnictwie cywilnym, Tom II, dotyczące formatu, przetwarzania i przechowywania informacji.

7.1.3 Odpowiednia uwaga powinna zostać poświęcona procesom oceny i zarządzania ryzyka, omówionym w Rozdziale 3 tego podręcznika.

--- KONIEC ---