ROZPORZĄDZENIE KOMISJI (WE) NR 482/2008

z dnia 30 maja 2008 r.

ustanawiające system zapewnienia bezpieczeństwa oprogramowania do stosowania przez instytucje zapewniające służby żeglugi powietrznej oraz zmieniające załącznik II do rozporządzenia (WE) nr 2096/2005

(Tekst mający znaczenie dla EOG)

KOMISJA WSPÓLNOT EUROPEJSKICH,

uwzględniając Traktat ustanawiający Wspólnotę Europejską,

uwzględniając rozporządzenie (WE) nr 550/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. w sprawie zapewniania służb żeglugi powietrznej w jednolitej europejskiej przestrzeni powietrznej (rozporządzenie w sprawie zapewniania służb) ([1]), w szczególności jego art. 4,

a także mając na uwadze, co następuje:

(1) Zgodnie z rozporządzeniem (WE) nr 550/2004 Komisja zobowiązana jest określić i przyjąć odpowiednie przepisy dotyczące wymagań Eurocontrol w zakresie przepisów bezpieczeństwa („ESARR"), uwzględniając obowiązujące prawodawstwo wspólnotowe. ESARR 6, zatytułowany „Oprogramowanie w systemach zarządzania ruchem lotniczym", określa zestaw prawnych wymagań w zakresie bezpieczeństwa, których celem jest wdrożenie systemu zapewnienia bezpieczeństwa oprogramowania.

(2) Rozporządzenie Komisji (WE) nr 2096/2005 z dnia 20 grudnia 2005 r. ustanawiające wspólne wymagania dotyczące zapewniania służb żeglugi powietrznej ([2]) stanowi w motywie 12 ostatnie zdanie, że „odnośne przepisy ESARR 1 dotyczące nadzoru nad bezpieczeństwem w zarządzaniu ruchem lotniczym oraz ESARR 6 dotyczące oprogramowania w systemach zarządzania ruchem lotniczym powinny być zidentyfikowane i przyjęte w drodze odrębnych aktów Wspólnoty".

(3) Załącznik II do rozporządzenia (WE) 2096/2005 wymaga od instytucji zapewniających służby ruchu lotniczego wdrożenia systemu zarządzania bezpieczeństwem, jak również wymagań bezpieczeństwa w zakresie oceny i ograniczania ryzyka w odniesieniu do zmian. W ramach systemu zarządzania bezpieczeństwem oraz w ramach procesu oceny i ograniczania ryzyka w odniesieniu do zmian instytucje zapewniające służby ruchu lotniczego powinny określić i wdrożyć system zapewnienia bezpieczeństwa oprogramowania, dotyczący konkretnie kwestii związanych z oprogramowaniem.

(4) Zasadniczym celem w zakresie bezpieczeństwa oprogramowania, jaki należy spełnić w odniesieniu do systemów funkcjonalnych obejmujących oprogramowanie, jest zapewnienie ograniczenia do akceptowalnego poziomu ryzyka związanego z wykorzystaniem oprogramowania w Europejskiej Sieci Zarządzania Ruchem Lotniczym (oprogramowanie „EATMN").

(5) Niniejsze rozporządzenie nie powinno obejmować operacji wojskowych i szkoleń, o których mowa w art. 1 ust. 2 rozporządzenia (WE) nr 549/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiającego ramy tworzenia jednolitej europejskiej przestrzeni powietrznej (rozporządzenie ramowe) ([3]).

(6) Dlatego załącznik II do rozporządzenia (WE) nr 2096/2005 powinien zostać odpowiednio zmieniony.

(7) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią Komitetu ds. Jednolitej Przestrzeni Powietrznej,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Przedmiot i zakres

1. Niniejsze rozporządzenie ustanawia wymagania dotyczące określenia i wdrożenia systemu zapewnienia bezpieczeństwa oprogramowania przez instytucje zapewniające służby ruchu lotniczego (ATS), podmioty zarządzające przepływem ruchu lotniczego (ATFM) oraz zarządzające przestrzenią powietrzną (ASM) dla ogólnego ruchu lotniczego, a także dostawców służb łączności, nawigacji i dozorowania (CNS).

Ustala ono i przyjmuje obowiązkowe przepisy dotyczące wymagań Eurocontrol w zakresie przepisów bezpieczeństwa – ESARR 6 – zatytułowanego „Oprogramowanie w systemach zarządzania ruchem lotniczym", wydanego dnia 6 listopada 2003 r.

2. Niniejsze rozporządzenie stosuje się do nowego oprogramowania i do wszelkich zmian w oprogramowaniu systemów ATS, ASM, ATFM i CNS.

Niniejszego rozporządzenia nie stosuje się do oprogramowania pokładowych części składowych systemów statków powietrznych ani do urządzeń kosmicznych.

Artykuł 2

Definicje

Dla celów niniejszego rozporządzenia stosuje się definicje z art. 2 rozporządzenia (WE) nr 549/2004.

([1]) Dz.U. L 96 z 31.3.2004, s. 10.

([2]) Dz.U. L 335 z 21.12.2005, s. 13. Rozporządzenie zmienione rozporządzeniem (WE) nr 1315/2007 (Dz.U. L 291 z 9.11.2007, s. 16).

([3]) Dz.U. L 96 z 31.3.2004, s. 1.

Ponadto zastosowanie mają niżej wymienione definicje:

1) „oprogramowanie" oznacza programy komputerowe i odpowiednie dane konfiguracyjne, w tym oprogramowanie istniejące, z wyłączeniem elektronicznych elementów, takich jak specjalistyczne obwody zintegrowane do aplikacji, programowalne tablice bramek lub sterowniki mocy;

2) „dane konfiguracyjne" oznaczają dane konfigurujące ogólny system oprogramowania do celów jego poszczególnych zastosowań;

3) „oprogramowanie istniejące" oznacza oprogramowanie, które nie zostało opracowane na potrzeby bieżącego kontraktu;

4) „zapewnienie bezpieczeństwa" oznacza wszelkie zaplanowane i systematyczne działania konieczne dla zapewnienia odpowiedniego poziomu wiarygodności produktu, usługi, instytucji lub systemu funkcjonalnego jako gwarantujących zadowalający lub akceptowalny poziom bezpieczeństwa;

5) „instytucja" oznacza dostawcę ATS, dostawcę CNS lub podmiot ATFM lub ASM;

6) „system funkcjonalny" oznacza kombinację systemów, procedur i zasobów ludzkich zorganizowanych w celu pełnienia określonej funkcji w ramach ATM;

7) „ryzyko" oznacza połączenie ogólnego prawdopodobieństwa wystąpienia lub częstotliwości występowania szkodliwego skutku wywołanego zagrożeniem oraz rozmiarów tego skutku;

8) „zagrożenie" oznacza wszelkie sytuacje, zdarzenia i okoliczności, które mogłyby skutkować wypadkiem;

9) „nowe oprogramowanie" oznacza oprogramowanie, które zostało zamówione lub na które zawarto wiążące kontrakty po wejściu w życie niniejszego rozporządzenia;

10) „cel w zakresie bezpieczeństwa" oznacza jakościowe lub ilościowe określenie maksymalnej częstotliwości lub prawdopodobieństwa wystąpienia zagrożenia;

11) „wymóg bezpieczeństwa" oznacza środek ograniczający ryzyko, określony przez strategię ograniczania ryzyka, dla osiągnięcia określonego celu w zakresie bezpieczeństwa, w tym wymagania organizacyjne, operacyjne, proceduralne, funkcjonalne, eksploatacyjne oraz dotyczące interoperacyjności lub wpływu na środowisko;

12) „szybkie przejście lub zamiana urodzeń w czasie pracy" oznacza wymianę składników systemu Europejskiej Sieci Zarządzania Ruchem Lotniczym (EATMN) lub oprogramowania w trakcie działania systemu;

13) „wymóg w zakresie bezpieczeństwa oprogramowania" oznacza opis tego, co oprogramowanie ma wygenerować przy uwzględnieniu wprowadzonych danych i ograniczeń, a jego spełnienie zapewnia bezpieczne i zgodne z potrzebami działanie oprogramowania EATMN;

14) „oprogramowanie EATMN" oznacza oprogramowanie stosowane w systemach EATMN, o których mowa w art. 1;

15) „zasadność wymagań" oznacza potwierdzenie poprzez badanie oraz przedstawienie obiektywnych dowodów na to, że szczególne wymagania dotyczące określonego zastosowania są zgodne z zamierzeniami;

16) „wymagane do niezależnego osiągnięcia" oznacza, w ramach procesu weryfikacji oprogramowania, czynności weryfikacyjne przeprowadzane przez osobę lub osoby inne niż osoba lub osoby odpowiedzialne za opracowanie kontrolowanego elementu;

17) „wadliwe działanie oprogramowania" oznacza brak możliwości poprawnego wykonania przez program żądanej funkcji;

18) „awaria oprogramowania" oznacza brak możliwości wykonania przez program żądanej funkcji;

19) „COTS" oznacza dostępną w sprzedaży aplikację, sprzedawaną przez sprzedawców na podstawie ogólnodostępnych katalogów, w której nie można zastosować osobistych ustawień, ani też nie można jej rozbudować;

20) „składniki oprogramowania" oznaczają moduł oprogramowania, który może być zainstalowany lub połączony z innymi modułami w celu stworzenia aplikacji oprogramowania zgodnej z potrzebami klienta;

21) „niezależne składniki oprogramowania" oznaczają te składniki oprogramowania, które nie przestają działać z powodu tej samej awarii, która spowodowała zagrożenie;

22) „czas reakcji oprogramowania" oznacza czas, w jakim oprogramowanie reaguje na wprowadzone dane lub okresowo przeprowadzane operacje, i/lub działanie oprogramowania w zakresie transakcji lub wiadomości przetworzonych w jednostce czasu;

23) „wydajność oprogramowania" oznacza zdolność oprogramowania do przetworzenia określonej liczby danych;

24) „dokładność" oznacza wymaganą precyzję obliczeń;

25) „stopień wykorzystania zasobów oprogramowania" oznacza ilość zasobów w ramach systemu komputerowego, które mogą być wykorzystane przez oprogramowanie aplikacji;

26) „odporność oprogramowania" oznacza zachowanie się oprogramowania w przypadku wprowadzenia nieoczekiwanych danych, awarii sprzętu komputerowego lub awarii zasilania, zarówno w samym systemie komputerowym, jak i w podłączonych urządzeniach;

27) „odporność na przeciążenie" oznacza zachowanie się systemu w przypadku większego niż zaplanowano dla normalnego działania systemu tempa wprowadzania danych, a zwłaszcza jego odporność na taką sytuację;

28) „poprawna i kompletna weryfikacja oprogramowania EATMN" oznacza wszelkie wymagania w zakresie bezpieczeństwa oprogramowania, które prawidłowo wskazują, jakie warunki muszą być spełnione przez składnik oprogramowania w ramach oceny i ograniczania ryzyka, oraz że spełnienie tych wymagań jest potwierdzone na poziomie wymaganym dla bezpieczeństwa oprogramowania;

29) „dane cyklu życia oprogramowania" oznaczają dane generowane w trakcie cyklu życia oprogramowania w celu planowania, kierowania, wyjaśniania, określania, rejestrowania lub potwierdzania czynności. Dane te umożliwiają zatwierdzanie procesów cyklu życia oprogramowania, systemu lub sprzętu oraz zmian wprowadzonych do oprogramowania, już po jego zatwierdzeniu;

30) „cykl życia oprogramowania" oznacza:

a) uporządkowany ogół procesów, które instytucja uznaje za wystarczający i odpowiedni do wyprodukowania oprogramowania;

b) okres czasu rozpoczynający się od decyzji o produkcji lub zmianie oprogramowania i kończący się z chwilą wycofania oprogramowania z użytku;

31) „wymóg bezpieczeństwa systemu" oznacza wymóg bezpieczeństwa odnoszący się do systemu funkcjonalnego.

Artykuł 3

Ogólne wymagania bezpieczeństwa

1. Jeśli instytucja zobowiązana jest do wdrożenia procesu oceny i ograniczania ryzyka zgodnie z obowiązującym prawem wspólnotowym lub krajowym, definiuje ona i wdraża system zapewnienia bezpieczeństwa oprogramowania, dotyczący konkretnie kwestii związanych z oprogramowaniem EATMN, włączając w to wszystkie działania operacyjne *on-line*, a w szczególności szybkie przejście lub zamianę urządzeń w czasie pracy.

2. Instytucja gwarantuje, co najmniej, że jej system zapewnienia bezpieczeństwa oprogramowania zapewnia dowody i argumenty potwierdzające, że:

a) wymagania bezpieczeństwa oprogramowania prawidłowo określają wymagania, jakie oprogramowanie musi spełnić, zapewniając tym samym spełnienie celów i wymagań bezpieczeństwa, zgodnie z procesem oceny i ograniczania ryzyka;

b) wszystkie wymagania bezpieczeństwa oprogramowania są możliwe do prześledzenia;

c) wdrożenie oprogramowania nie zawiera funkcji, które niekorzystnie wpływają na bezpieczeństwo;

d) oprogramowanie EATMN spełnia wymagania z poziomem ufności odpowiadającym stopniowi krytyczności oprogramowania;

e) gwarancje spełnienia ogólnych wymagań bezpieczeństwa, określonych w lit. a)–d), oraz ich dowody wynikają zawsze z następujących źródeł:

(i) znanej wersji wykonawczej oprogramowania;

(ii) znanego zakresu danych konfiguracyjnych,

(iii) znanego zestawu programów i ich opisów (włącznie ze specyfikacjami), użytych w produkcji aktualnej wersji oprogramowania.

3. Instytucja zapewnia krajowy organ nadzorujący, że spełnione zostały wymagania, o których mowa w ust. 2.

Artykuł 4

Wymagania dotyczące systemu zapewnienia bezpieczeństwa oprogramowania

Instytucja gwarantuje, co najmniej, że system zapewnienia bezpieczeństwa oprogramowania:

1) jest udokumentowany, szczególnie jako część ogólnej dokumentacji dotyczącej oceny i ograniczania ryzyka;

2) przydziela poziomy gwarantowania oprogramowania całemu oprogramowaniu operacyjnemu EATMN, zgodnie z wymogami określonymi w załączniku I;

3) zawiera gwarancje:

a) zasadności wymagań w zakresie bezpieczeństwa oprogramowania zgodnie z wymogami określonymi w załączniku II część A;

b) weryfikacji oprogramowania zgodnie z wymogami określonymi w załączniku II część B;

c) zarządzania konfiguracją oprogramowania zgodnie z wymogami określonymi w załączniku II część C;

d) śledzenia wymagań w zakresie bezpieczeństwa oprogramowania zgodnie z wymogami określonymi w załączniku II część D;

4) określa dokładność, z jaką mają być ustanawiane powyższe gwarancje; dokładność musi być określana dla każdego z poziomów gwarantowania oprogramowania i wzrastać wraz ze wzrostem poziomu krytyczności oprogramowania; w tym celu:

a) dokładność zapewniania bezpieczeństwa, w zależności od poziomu gwarantowania oprogramowania, powinna być zróżnicowana pod względem:

(i) kryteriów wymaganych do niezależnego osiągnięcia;

(ii) kryteriów wymaganych do osiągnięcia;

(iii) kryteriów niewymaganych;

b) zapewnienia odpowiadające każdemu z poziomów gwarantowania oprogramowania muszą dawać dostateczną pewność, że oprogramowanie EATMN może być używane z dopuszczalnym bezpieczeństwem;

5) wykorzystuje zwrotne informacje wynikające z doświadczeń uzyskiwanych podczas użytkowania oprogramowania EATMN, w celu potwierdzenia, że system zapewnienia bezpieczeństwa oprogramowania i przypisane poziomy gwarantowania są właściwe. W tym celu skutki każdej usterki oprogramowania lub jego awarii, zgłoszone zgodnie z wymaganiami dotyczącymi sprawozdawczości i oceny zdarzeń związanych z bezpieczeństwem, porównuje się ze skutkami określonymi dla danego systemu zgodnie ze schematem klasyfikacji stopnia ciężkości, o którym mowa w sekcji 4 punktu 3.2.4 załącznika II do rozporządzenia (WE) nr 2096/2005.

Artykuł 5

Wymagania dotyczące zmian w oprogramowaniu i w szczególnych rodzajach oprogramowania

1. Odnośnie do zmian w oprogramowaniu lub w szczególnych rodzajach oprogramowania, takich jak COTS, oprogramowanie istniejące lub oprogramowanie poprzednio użytkowane, w odniesieniu do których nie można stosować pewnych wymagań określonych w art. 3 ust. 2 lit. d) lub e) lub w art. 4 ust. 2, 3, 4 lub 5, instytucja czuwa, aby system zapewnienia bezpieczeństwa oprogramowania zapewniał, poprzez zastosowanie innych środków wybranych i uzgodnionych z krajowym organem nadzorującym, poziom ufności odpowiadający właściwemu poziomowi bezpieczeństwa oprogramowania, jeśli takowy ustalono.

Środki te muszą zapewniać odpowiedni poziom pewności co do zgodności tego oprogramowania z celami i wymogami w zakresie bezpieczeństwa, określonymi w ramach procesu oceny i ograniczania ryzyka.

2. Ocenę środków, o których mowa w ust. 1, krajowy organ nadzorujący może zlecić uznanej organizacji lub notyfikowanemu organowi.

Artykuł 6

Zmiana do rozporządzenia (WE) nr 2096/2005

W załączniku II do rozporządzenia (WE) nr 2096/2005 dodaje się sekcję w brzmieniu:

„3.2.5. Sekcja 5

System zapewnienia bezpieczeństwa oprogramowania

W ramach stosowania systemu zarządzania bezpieczeństwem instytucja zapewniająca służby ruchu lotniczego wdraża system zapewnienia bezpieczeństwa oprogramowania zgodnie z rozporządzeniem Komisji (WE) nr 482/2008 z dnia 30 maja 2008 r. ustanawiającym system zapewnienia bezpieczeństwa oprogramowania do stosowania przez instytucje zapewniające służby żeglugi powietrznej oraz zmieniającym załącznik II do rozporządzenia (WE) nr 2096/2005 (*).

(*) Dz.U. L 141 z 31.5.2008, s. 5.”.

Artykuł 7

Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie stosuje się od dnia 1 stycznia 2009 r. do nowego oprogramowania EATMN, o którym mowa w art. 1 ust. 2 akapit pierwszy.

Niniejsze rozporządzenie stosuje się od dnia 1 lipca 2010 r. odnośnie do wszelkich zmian w oprogramowaniu systemów EATMN, o których mowa w art. 1 ust. 2 akapit pierwszy, działających na ten dzień.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich Państwach członkowskich.

Sporządzono w Brukseli, dnia 30 maja 2008 r.

W imieniu Komisji

Antonio TAJANI

Członek Komisji

ZAŁĄCZNIK I

Wymagania dotyczące poziomów gwarantowania oprogramowania, o których mowa w art. 4 pkt 2

1. Poziom gwarantowania oprogramowania określa relację między poziomem rygorystyczności poszczególnych elementów zapewnienia bezpieczeństwa a stopniem krytyczności oprogramowania EATMN z zastosowaniem schematu klasyfikacji stopnia ciężkości, o którym mowa w sekcji 4 punktu 3.2.4 załącznika II do rozporządzenia (WE) nr 2096/2005, w powiązaniu z prawdopodobieństwem wystąpienia określonych skutków negatywnych. Określa się przynajmniej cztery poziomy gwarantowania oprogramowania, przy czym poziom 1 jest najbardziej krytyczny.

2. Przydzielony poziom gwarantowania oprogramowania jest współmierny do najpoważniejszego skutku, jaki może wywołać usterka oprogramowania lub jego awaria, zgodnie z sekcją 4 punktu 3.2.4 załącznika II do rozporządzenia (WE) nr 2096/2005. W szczególności uwzględnia on ryzyko towarzyszące usterkom lub jego awariom oraz określone zabezpieczenia proceduralne i/lub na poziomie architektury oprogramowania.

3. Składnikom oprogramowania EATMN, w odniesieniu do których nie jest możliwe wykazanie ich niezależności od pozostałych składników, przydziela się poziom gwarantowania oprogramowania odpowiadający najbardziej krytycznym składnikom zależnym.

ZAŁĄCZNIK II

Część A: Wymagania dotyczące zapewnienia zasadności wymagań w zakresie bezpieczeństwa oprogramowania, o których mowa w art. 4 pkt 3 lit. a)

1. Wymagania w zakresie bezpieczeństwa oprogramowania określają funkcjonalne właściwości w trybie nominalnym i ograniczonym oprogramowania EATMN oraz, w zależności od przypadku, wydajność czasową, wydajność ogólną, dokładność, wykorzystanie zasobów docelowej platformy sprzętowej, odporność na nietypowe warunki operacyjne oraz tolerancję na przeciążenie.

2. Wymagania w zakresie bezpieczeństwa oprogramowania są kompletne i poprawne oraz wypełniają wymagania bezpieczeństwa systemowego.

Część B: Wymagania dotyczące zapewnienia weryfikacji oprogramowania, o których mowa w art. 4 pkt 3 lit. b)

1. Funkcjonalne właściwości oprogramowania EATMN, czas reakcji, wydajność, dokładność, stopień wykorzystania zasobów oprogramowania w sprzęcie komputerowym, odporność na nietypowe warunki operacyjne oraz tolerancję na przeciążenie są zgodne z wymogami dotyczącymi oprogramowania.

2. Oprogramowanie EATMN jest odpowiednio sprawdzane poprzez analizy i/lub testowanie i/lub równoważne metody, uzgodnione z upoważnioną władzą państwową.

3. Weryfikacja oprogramowania EATMN jest poprawna i kompletna.

Część C: Wymagania dotyczące zapewnienia zarządzania konfiguracją oprogramowania, o których mowa w art. 4 pkt 3 lit. c)

1. Istnieją procedury określania konfiguracji, śledzenia i rejestrowania statusu konfiguracji, pozwalające wykazać, że konfiguracja danych dotyczących cyklu życia oprogramowania pozostaje pod kontrolą przez cały okres oprogramowania EATMN.

2. Istnieją procedury zgłaszania problemów, ich śledzenia oraz określania działań naprawczych pozwalające wykazać, że podjęto środki mające na celu ograniczenie problemów związanych z bezpieczeństwem oprogramowania.

3. Istnieją procedury odzyskiwania i udostępniania, umożliwiające odtwarzanie i przedstawianie danych cyklu życia oprogramowania przez cały okres istnienia oprogramowania EATMN.

Część D: Wymagania dotyczące zapewnienia identyfikowalności wymagań w zakresie bezpieczeństwa oprogramowania, o których mowa w art. 4 pkt 3 lit. d)

1. Istnieje możliwość śledzenia każdego wymagania w zakresie bezpieczeństwa oprogramowania do tego poziomu projektowego, na którym wykazane zostaje jego spełnienie.

2. Istnieje możliwość śledzenia każdego wymagania w zakresie bezpieczeństwa oprogramowania, na każdym poziomie projektowym, na którym wykazane zostaje jego spełnienie, w powiązaniu z wymaganiem w zakresie bezpieczeństwa systemu.