DZIENNIK URZĘDOWY

AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO

Warszawa, dnia 3 września 2014 r.

Poz. 23

ZARZĄDZENIE NR 45
SZEFA AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO

z dnia 17 sierpnia 2012 r.

w sprawie certyfikacji urządzeń, narzędzi oraz środków przeznaczonych do ochrony informacji niejawnych

Na podstawie art. 19 ust. 3 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.[1)]) zarządza się, co następuje:

Przepisy ogólne

§ 1. 1. Zarządzenie określa tryb oraz sposób realizacji zadań Agencji Bezpieczeństwa Wewnętrznego, zwanej dalej „ABW", o których mowa w art. 50 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228), zwanej dalej „ustawą".

2. Przepisów zarządzenia nie stosuje się do procesów certyfikacji urządzeń, narzędzi lub środków, prowadzonych na potrzeby własne ABW.

§ 2. Ilekroć w zarządzeniu jest mowa o:

1) procesie certyfikacji - należy przez to rozumieć zespół czynności faktycznych oraz prawnych, mających na celu przeprowadzenie badań oraz dokonanie oceny bezpieczeństwa urządzenia, narzędzia lub środka przeznaczonego do ochrony informacji niejawnych, o których mowa w art. 50 ustawy, a także ewentualne wydanie odpowiedniego certyfikatu;

2) Jednostce Certyfikującej - należy przez to rozumieć komórkę organizacyjną Wydziału I Departamentu Bezpieczeństwa Teleinformatycznego ABW, właściwą w zakresie prowadzenia procesu certyfikacji;

3) porozumieniu - należy przez to rozumieć porozumienie w sprawie prowadzenia procesu certyfikacji urządzenia, narzędzia lub środka przeznaczonego do ochrony informacji niejawnych;

4) wymaganiach certyfikacyjnych - należy przez to rozumieć minimalne wymagania określone przez ABW dla urządzenia, narzędzia lub środka, przeznaczonego do ochrony informacji niejawnych, których spełnienie jest konieczne do uzyskania pozytywnych wyników oceny bezpieczeństwa;

5) zespołach badawczych - należy przez to rozumieć łącznie Laboratorium Ochrony Elektromagnetycznej, Laboratorium Ochrony Kryptograficznej oraz inne, właściwe merytorycznie, komórki organizacyjne Departamentu Bezpieczeństwa Teleinformatycznego ABW;

6) DBTI ABW - należy przez to rozumieć Departament Bezpieczeństwa Teleinformatycznego ABW.

Rodzaje certyfikatów

§ 3. 1. W ramach procesu certyfikacji wydawane są następujące rodzaje certyfikatów dla urządzeń, narzędzi lub środków przeznaczonych do ochrony informacji niejawnych:

1) dla urządzeń lub narzędzi kryptograficznych:

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2010 r. Nr 182, poz. 1228, Nr 238, poz. 1578 oraz z 2011 r. Nr 53, poz. 273, Nr 84, poz. 455, Nr 117, poz. 677 i Nr 230, poz. 1371.

a) certyfikat typu (oznaczony literą „T”) - wydawany dla określonego modelu urządzenia lub narzędzia, przeznaczonego do ochrony informacji niejawnych,

b) certyfikat zgodności (oznaczony literą „Z”) - wydawany dla egzemplarza urządzenia lub narzędzia przeznaczonego do ochrony informacji niejawnych, posiadającego ważny certyfikat typu,

c) certyfikat dla urządzenia lub narzędzia kryptograficznego przeznaczonego do ochrony informacji niejawnych o klauzuli „zastrzeżone” - wydawany dla urządzenia lub narzędzia kryptograficznego oraz obejmujący jego wszystkie egzemplarze;

2) dla środków ochrony elektromagnetycznej - certyfikat ochrony elektromagnetycznej, wydawany dla egzemplarza środka;

3) dla urządzenia lub narzędzia służącego do realizacji zabezpieczenia teleinformatycznego - certyfikat zabezpieczenia teleinformatycznego, wydawany dla urządzenia lub narzędzia służącego do realizacji zabezpieczenia, oraz obejmujący jego wszystkie egzemplarze.

2. Wzory certyfikatów, o których mowa w ust. 1, określa Dyrektor DBTI ABW.

3. Aktualne wzory certyfikatów, o których mowa w ust. 1, są publikowane na internetowej stronie podmiotowej Biuletynu Informacji Publicznej Agencji Bezpieczeństwa Wewnętrznego, zwanej dalej „BIP ABW”.

Zasady ważności certyfikatów

§ 4. 1. Zasady oraz okres ważności certyfikatów określane są w samych certyfikatach.

2. W przypadku urządzeń lub narzędzi kryptograficznych przeznaczonych do ochrony informacji niejawnych o klauzuli „poufne” lub wyższej, dopiero łączne posiadanie przez konkretny egzemplarz urządzenia lub narzędzia obydwu, jednocześnie ważnych certyfikatów wymienionych w § 3 ust. 1 pkt 1 lit. a i b, stanowi o możliwości zastosowania urządzenia lub narzędzia w systemie teleinformatycznym podlegającym akredytacji lub już akredytowanym.

3. Wygaśnięcie ważności certyfikatu typu, o którym mowa w § 3 ust. 1 pkt 1 lit. a, powoduje wygaśnięcie ważności certyfikatu zgodności, o którym mowa w § 3 ust. 1 pkt 1 lit. b.

Wymagania certyfikacyjne

§ 5. 1. Wymagania certyfikacyjne stanowiące informacje niejawne ABW udostępnia podmiotom ubiegającym się o przeprowadzenie procesu certyfikacji, na zasadach i pod warunkiem spełnienia wymogów określonych w ustawie. Wymagania certyfikacyjne niebędące informacjami niejawnymi mogą być publikowane na BIP ABW.

2. Zastosowanie wymagań certyfikacyjnych stanowi niezbędny element procesu certyfikacji oraz odbywa się na każdym jego etapie.

Rodzaje wniosków o wszczęcie procesu certyfikacji

§ 6. 1. W celu przeprowadzenia procesu certyfikacji wnioskodawca składa w Jednostce Certyfikującej wypełniony właściwy wniosek:

1) dla urządzenia lub narzędzia kryptograficznego - wniosek WK-01;

2) dla środka ochrony elektromagnetycznej - wniosek WE-01 lub WS-01;

3) dla urządzenia lub narzędzia realizującego zabezpieczenie teleinformatyczne -wniosek WUN-01.

2. Wzory formularzy wniosków, o których mowa w ust. 1, określa Dyrektor DBTI ABW.

3. Aktualne wzory wniosków, o których mowa w ust. 1, publikowane są na internetowej stronie BIP ABW.

4. Do wniosku załącza się komplet załączników określonych we wzorze wniosku.

5. W uzasadnionych przypadkach, w zakresie procesu certyfikacji środków ochrony elektromagnetycznej dopuszcza się przyjęcie wniosku bez niektórych załączników, o których mowa w ust. 4, chyba, że uniemożliwiłoby to lub znacznie utrudniło prowadzenie procesu certyfikacji.

6. Wraz z wnioskiem są przekazywane do ABW egzemplarze urządzenia, narzędzia lub środka przeznaczonego do ochrony informacji niejawnych, w ilości określonej w porozumieniu, o którym mowa w § 7 ust. 4 pkt 6. Przekazywane egzemplarze służą do prowadzenia badań urządzenia, narzędzia lub środka przeznaczonego do ochrony informacji niejawnych, w trakcie których mogą ulec zniszczeniu - na co wnioskodawca wyraża zgodę.

7. Warunkiem wszczęcia procesu certyfikacji jest złożenie poprawnie wypełnionego wniosku wraz z kompletem pełnych załączników oraz egzemplarzami urządzenia, środka lub narzędzie. Fragmenty załączników (np. niepełna dokumentacja, czy niepełna instrukcja w języku polskim) nie stanowią załączników w rozumieniu ust. 4 - 6.

8. W przypadku stwierdzenia wystąpienia braków formalnych we wniosku, wnioskodawca będzie wezwany do ich uzupełnienia w terminie jednego miesiąca, z pouczeniem, że nieusunięcie braków spowoduje pozostawienie wniosku bez rozpoznania. Na potrzeby obliczania terminów, za dzień złożenia wniosku uważa się dzień złożenia poprawnie wypełnionego wniosku wraz z kompletem pełnych załączników lub dzień ostatecznego usunięcia braków.

9. Przyjęty wniosek spełniający wymagania, o których mowa w ust. 1-8, podlega rejestracji dokonywanej przez Jednostkę Certyfikującą.

Rozpoczęcie procesu certyfikacji

§ 7. 1. W nieprzekraczalnym terminie trzech miesięcy od dnia rejestracji wniosku, Jednostka Certyfikująca we współpracy z zespołami badawczymi dokonuje analizy przekazanych materiałów i przeprowadza wstępną ocenę urządzenia, narzędzia lub środka w celu ustalenia zasadności i zdolności do poddania go badaniom i ocenie bezpieczeństwa oraz określenia niezbędnych zasobów warunkujących przeprowadzenie tych czynności.

2. Na żądanie Jednostki Certyfikującej wnioskodawca do czasu zakończenia analizy materiałów, o której mowa w ust. 1:

1) przeprowadza prezentację urządzenia, narzędzia lub środka, w szczególności w celu przedstawienia zastosowanych w nim mechanizmów zabezpieczeń wyspecyfikowanych w dokumentacji bezpieczeństwa;

2) dostarcza dodatkową dokumentację dotyczącą urządzenia, narzędzia, środka lub specjalistyczną aparaturę dedykowaną, niezbędną do przeprowadzenia badań.

3. Dla rozpoczęcia procesu certyfikacji niezbędne jest uzyskanie przez wnioskodawcę pozytywnej oceny przekazanych materiałów.

4. W przypadku urządzeń lub narzędzi kryptograficznych oraz urządzeń lub narzędzi realizujących zabezpieczenie teleinformatyczne, dla rozpoczęcia procesu certyfikacji, po spełnieniu warunku, o którym mowa w ust. 3, niezbędne jest ponadto zawarcie odpowiedniego dla danego procesu certyfikacji pisemnego porozumienia określającego w szczególności:

1) przedmiot badań;

2) ustalenia dotyczące terminów prowadzonych czynności;

3) zasady dostarczenia urządzenia, narzędzia lub środka do badań;

4) w przypadku wniosku o certyfikat typu dla urządzenia lub narzędzia kryptograficznego przeznaczonego do ochrony informacji niejawnych o klauzuli „poufne” lub wyższej zasady:

   a) dostarczenia i bezpłatnego użyczenia niezbędnych narzędzi służących do implementacji algorytmu narodowego; kwestie te mogą także zostać uregulowane w odrębnej umowie,

   b) bezpłatnego przekazywania generatorów liczb losowych,

   c) deponowania egzemplarzy wzorcowych,

   d) udzielenia licencji na korzystanie z algorytmu narodowego,

   e) składania wniosków o udzielenie certyfikatu zgodności, dla egzemplarzy urządzenia lub narzędzia;

5) zasady naliczania opłat z tytułu prowadzonych czynności w ramach procesu certyfikacji;

6) ilość egzemplarzy urządzenia, narzędzia lub środka, niezbędnych do przeprowadzenia badań i dokonania oceny bezpieczeństwa;

7) warunki wydania i ważności certyfikatu;

8) w razie potrzeby - zasady przechowywania egzemplarzy kontrolnych urządzenia, narzędzia lub środka posiadającego certyfikat w depozycie DBTI ABW;

9) pozostałe obowiązki stron porozumienia związane z procesem certyfikacji.

5. Porozumienie ze strony ABW zawiera, z upoważnienia Szefa ABW, Dyrektor DBTI ABW.

6. W przypadku negatywnej oceny przekazanych przez wnioskodawcę materiałów Jednostka Certyfikująca odmawia rozpoczęcia badań. Informację o odmowie wraz z uzasadnieniem i pouczeniem o możliwości ponownego złożenia wniosku Dyrektor DBTI ABW przekazuje niezwłocznie wnioskodawcy.

Zasady prowadzenia czynności

§ 8. 1. Badania prowadzone są przez wyspecjalizowane w tym zakresie zespoły badawcze DBTI ABW lub zespoły zewnętrzne na warunkach określonych w przepisach odrębnych, którym Jednostka Certyfikująca zleca ich wykonanie.

2. Przebieg badań oraz oceny bezpieczeństwa podlegają dokumentowaniu.

3. Szczegółowe procedury postępowania Jednostki Certyfikującej oraz zespołów badawczych są określane przez Dyrektora DBTI ABW.

4. Po wykonaniu badań zespoły badawcze, o których mowa w ust. 1, w ciągu jednego miesiąca opracowują sprawozdania lub raporty z badań.

Generatory danych losowych

§ 9. 1. Wykorzystywane w urządzeniach lub narzędziach kryptograficznych generatory danych losowych podlegają badaniom oraz ocenie bezpieczeństwa wykonywanym w procesie certyfikacji.

2. Warunkiem uzyskania certyfikatu zgodności jest potwierdzenie przez Jednostkę Certyfikującą poprawności funkcjonowania egzemplarza generatora danych losowych zainstalowanego w urządzeniu lub narzędziu kryptograficznym, które podlega procesowi certyfikacji.

3. Po pozytywnym potwierdzeniu właściwości generatora Jednostka Certyfikująca sporządza wewnętrzne świadectwo dopuszczenia do eksploatacji egzemplarza generatora danych losowych, które przechowywane jest w dokumentacji Jednostki Certyfikującej. Świadectwa dopuszczenia do eksploatacji generatora danych losowych podpisuje Dyrektor DBTI ABW lub upoważniony przez niego funkcjonariusz DBTI ABW.

Dokonanie oceny bezpieczeństwa

§ 10. 1. Po zakończeniu badań Jednostka Certyfikująca kompletuje sprawozdania lub raporty z przeprowadzonych czynności oraz dokonuje ich analizy.

2. Po wykonaniu czynności, o których mowa w ust. 1, Jednostka Certyfikująca w terminie jednego miesiąca sporządza raport z certyfikacji, który stanowi podstawę do wydania certyfikatu, albo odmowy jego wydania.

3. Wyciąg z raportu z certyfikacji może być udostępniony wnioskodawcy na jego pisemny wniosek kierowany do Dyrektora DBTI ABW.

4. Wydawany certyfikat może określać szczegółowe wymagania jego ważności.

Egzemplarze wzorcowe

§ 11. 1. Po przeprowadzeniu procesu certyfikacji wnioskodawca przekazuje dwa dodatkowe egzemplarze urządzenia lub narzędzia do ABW, które przechowywane są jako egzemplarze wzorcowe.

2. Wymogu przekazywania egzemplarzy wzorcowych, o których mowa w ust. 1, nie stosuje się:

1) do środków ochrony elektromagnetycznej;

2) do urządzenia lub narzędzia kryptograficznego przeznaczonego do ochrony informacji niejawnych o klauzuli „zastrzeżone”;

3) do urządzenia lub narzędzia służącego do realizacji zabezpieczenia teleinformatycznego;

4) w przypadku prowadzenia certyfikacji mającej na celu wydanie certyfikatu zgodności dla urządzenia lub narzędzia, które posiada wydany przez ABW certyfikat typu; a także

5) w przypadku certyfikacji mającej na celu ponowne wydanie certyfikatu typu dla urządzenia lub narzędzia, które bądź posiada ważny certyfikat typu wydany przez ABW, bądź którego certyfikat typu wydany przez ABW utracił ważność z powodu upływu terminu, na który został wydany.

Wydawanie certyfikatów

§ 12. 1. O odmowie wydania certyfikatu Dyrektor DBTI ABW niezwłocznie informuje pisemnie wnioskodawcę, podając przyczyny odmowy.

2. Certyfikaty ochrony kryptograficznej - typu, certyfikaty ochrony kryptograficznej dla urządzenia lub narzędzia kryptograficznego przeznaczonego do ochrony informacji niejawnych o klauzuli „zastrzeżone” oraz certyfikaty dla urządzenia lub narzędzia realizującego zabezpieczenie teleinformatyczne wydaje Szef ABW.

3. Certyfikaty ochrony kryptograficznej - zgodności, oraz certyfikaty ochrony elektromagnetycznej, wydaje na podstawie odrębnego upoważnienia Dyrektor DBTI ABW.

4. Jednostka Certyfikująca prowadzi ewidencję certyfikatów wydanych przez ABW.

5. Wydanie certyfikatu następuje po dokonaniu opłat z tytułu przeprowadzonych badań i certyfikacji.

6. Informacja o wydanym certyfikacie ochrony kryptograficznej typu oraz certyfikacie dla urządzenia lub narzędzia kryptograficznego przeznaczonego do ochrony informacji niejawnych o klauzuli „zastrzeżone” publikowana jest na stronie BIP ABW.

Zapewnienie poufności informacji

§ 13. ABW zapewnia ochronę przekazanych przez wnioskodawcę w trakcie badań i certyfikacji informacji stanowiących tajemnice prawnie chronione.

Przepisy końcowe

§ 14. Traci moc zarządzenie nr 48 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 21 lipca 2011 r. w sprawie badań i certyfikacji urządzeń kryptograficznych, środków ochrony elektromagnetycznej i urządzeń realizujących zabezpieczenie teleinformatyczne, wykorzystywanych do ochrony informacji niejawnych, prowadzonych przez Departament Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego.

§ 15. Zarządzenie wchodzi w życie z dniem podpisania.

Szef
Agencji Bezpieczeństwa Wewnętrznego

gen. bryg. Krzysztof BONDARYK