Warszawa, dnia 3 sierpnia 2021 r.

Poz. 8

ZARZĄDZENIE NR 35
SZEFA AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO

z dnia 3 sierpnia 2021 r.

w sprawie certyfikacji przez Agencję Bezpieczeństwa Wewnętrznego 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 2020 r. poz. 27 i 2320) zarządza się, co następuje:

§ 1. 1. Zarządzenie określa sposób i tryb prowadzenia przez Agencję Bezpieczeństwa Wewnętrznego, zwaną dalej „ABW", certyfikacji, o której mowa w art. 50 ust. 1-3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. 2019 r. poz. 742), zwanej dalej „ustawą".

2. Zarządzenia nie stosuje się do certyfikacji prowadzonej na potrzeby ABW.

§ 2. Użyte w zarządzeniu określenia oznaczają:

1) produkt – przeznaczone do ochrony informacji niejawnych urządzenia lub narzędzia kryptograficzne, urządzenia lub narzędzia służące do realizacji zabezpieczenia teleinformatycznego lub środek ochrony elektromagnetycznej;

2) wersja produktu – odmianę produktu posiadającą ściśle określoną funkcjonalność, zapewniającą bezpieczeństwo produktu na określonym poziomie;

3) wnioskodawca – podmiot zainteresowany przeprowadzeniem przez ABW certyfikacji produktu, który złożył wniosek, o którym mowa w art. 50 ust. 3 ustawy;

4) wydanie produktu – odmianę wersji produktu, różniąca się cechami, które nie mają wpływu na podstawową funkcjonalność, ani poziom bezpieczeństwa produktu;

5) wymagania certyfikacyjne – minimalne wymagania określone przez ABW dla produktu, których spełnienie jest konieczne do uzyskania pozytywnych wyników oceny bezpieczeństwa, o których mowa w art. 50 ust. 4 ustawy;

6) algorytm typu A – algorytm kryptograficzny konstruowany pod nadzorem ABW, oceniony i dopuszczony do stosowania przez ABW, a także algorytm kryptograficzny oparty o gamę jednorazową;

7) algorytm typu A1 – algorytm kryptograficzny opracowany w wyniku personalizacji przez ABW algorytmu pierwotnego, oceniony i dopuszczony do stosowania przez ABW;

8) zespoły badawcze Departamentu I ABW – właściwe merytorycznie komórki organizacyjne Departamentu I ABW, przeprowadzające badania i ocenę bezpieczeństwa w ramach certyfikacji.

§ 3. 1. W ramach certyfikacji ABW wydaje następujące rodzaje certyfikatów:

1) dla urządzeń lub narzędzi kryptograficznych:

   a) certyfikat ochrony kryptograficznej „typu" (oznaczony literą „T") – wydawany dla określonego modelu urządzenia lub narzędzia kryptograficznego, przeznaczonego do ochrony informacji niejawnych o klauzuli „poufne" i wyższej. Certyfikat ten umożliwia produkcję egzemplarzy produktu danej wersji oraz jest niezbędny do uzyskania certyfikatów zgodności,

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

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

2) dla środków ochrony elektromagnetycznej, w tym kabin ekranujących i Sprzętowych Stref Ochrony Elektromagnetycznej, zwanych dalej „SSOE” – certyfikat ochrony elektromagnetycznej, wydawany dla określonego egzemplarza środka ochrony elektromagnetycznej lub SSOE;

3) dla urządzeń lub narzędzi służących do realizacji zabezpieczenia teleinformatycznego – certyfikat zabezpieczenia teleinformatycznego, wydawany dla urządzenia lub narzędzia służącego do realizacji zabezpieczenia teleinformatycznego, obejmujący jego wszystkie egzemplarze.

2. Wzory certyfikatów, o których mowa w ust. 1, określa dyrektor Departamentu I ABW.

§ 4. 1. Wymagania certyfikacyjne stanowiące informacje niejawne, ABW udostępnia wnioskodawcom na zasadach i pod warunkiem spełnienia wymogów określonych w ustawie.

2. Wymagania certyfikacyjne niebędące informacjami niejawnymi mogą być publikowane na stronie BIP ABW lub udostępniane indywidualnie.

3. Spełnianie wymagań certyfikacyjnych jest weryfikowane przez ABW na każdym etapie certyfikacji.

§ 5. 1. W celu rozpoczęcia certyfikacji, wnioskodawca składa do ABW wypełniony wniosek:

1) dla urządzeń lub narzędzi kryptograficznych:

a) WK-01-T – w celu uzyskania certyfikatu, o którym mowa w § 3 ust. 1 pkt 1 lit. a i c,

b) WK-01-Z – w celu uzyskania certyfikatu, o którym mowa w § 3 ust. 1 pkt 1 lit. b;

2) dla środków ochrony elektromagnetycznej:

a) WE-01 – w celu uzyskania certyfikatu, o którym mowa w § 3 ust. 1 pkt 2, z wyjątkiem badań kabin ekranujących oraz wyznaczenia SSOE,

b) WE-01-K – w celu uzyskania certyfikatu, o którym mowa w § 3 ust. 1 pkt 2, w zakresie badań kabin ekranujących,

c) WS-01 – w celu uzyskania certyfikatu, o którym mowa w § 3 ust. 1 pkt 2 w zakresie wyznaczenia SSOE;

3) WUN-01 – w celu uzyskania certyfikatu, o którym mowa w § 3 ust. 1 pkt 3.

2. Do wniosków, o których mowa w ust. 1, dołącza się:

1) określone we wniosku uzupełnione załączniki;

2) odpowiednią liczbę egzemplarzy produktu, co do których wnioskodawca wyraża zgodę na ewentualne zniszczenie.

3. W przypadku stwierdzenia braków formalnych we wniosku, o którym mowa w ust. 1, lub załącznikach, o których mowa w ust. 2, wzywa się wnioskodawcę do ich uzupełnienia w terminie jednego miesiąca od dnia doręczenia informacji o stwierdzeniu braków formalnych.

4. Nieusunięcie braków formalnych przez wnioskodawcę w terminie, o którym mowa w ust. 3, powoduje zwrot wniosku, o którym mowa w ust. 1, wraz z załącznikami, o których mowa w ust. 2, bez rozpatrzenia.

5. Za dzień rozpoczęcia certyfikacji uznaje się dzień złożenia poprawnie wypełnionego wniosku, o którym mowa w ust. 1, oraz załączników, o których mowa w ust. 2.

6. Wzory wniosków, o których mowa w ust. 1, określa dyrektor Departamentu I ABW oraz są one publikowane na stronie BIP ABW.

§ 6. 1. W terminie trzech miesięcy od dnia złożenia wniosku, o którym mowa w § 5 ust. 1, zespoły badawcze Departamentu I ABW dokonują analizy przekazanych materiałów i przeprowadzają wstępną ocenę produktu w celu ustalenia zasadności i zdolności do poddania go badaniom oraz określenia niezbędnych zasobów warunkujących przeprowadzenie tych czynności. W uzasadnionych przypadkach termin wskazany w zdaniu pierwszym może ulec zmianie.

2. W terminie, o którym mowa w ust. 1, wnioskodawca na wniosek ABW ustala:

1) szczegóły spotkania, mającego na celu prezentację produktu, w szczególności przedstawienie zastosowanych w nim mechanizmów zabezpieczeń wyspecyfikowanych w dokumentacji;

2) termin dostarczenia dodatkowej dokumentacji produktu lub dedykowanej aparatury specjalistycznej, niezbędnej do przeprowadzenia badań.

3. Realizacja badań i oceny bezpieczeństwa prowadzonych w ramach certyfikacji urządzeń lub narzędzi kryptograficznych oraz urządzeń lub narzędzi służących do realizacji zabezpieczenia teleinformatycznego, jest prowadzona na podstawie porozumienia zawieranego pomiędzy ABW a wnioskodawcą, określającego w szczególności:

1) przedmiot badań;

2) ustalenia dotyczące harmonogramu prowadzonych czynności;

3) zasady dostarczenia produktu do badań;

4) zasady dotyczące:

a) dostarczenia i bezpłatnego użyczenia niezbędnych narzędzi służących do implementacji algorytmu typu A lub algorytmu typu A1,

b) bezpłatnego przekazywania generatorów liczb losowych,

c) deponowania egzemplarzy wzorcowych, o których mowa w § 10,

d) udzielenia licencji na korzystanie z algorytmu typu A lub algorytmu typu A1,

e) składania wniosków o wydanie certyfikatu ochrony kryptograficznej „zgodności”, dla egzemplarzy badanego produktu

– w przypadku wniosku o wydanie certyfikatu ochrony kryptograficznej „typu”;

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

6) liczbę przekazanych egzemplarzy produktu do przeprowadzenia badań i przeprowadzenia oceny bezpieczeństwa;

7) liczbę przekazanych egzemplarzy wzorcowych, o których mowa w § 10, oraz ewentualne zasady ich przechowywania w Departamencie I ABW;

8) warunki wydania i ważności certyfikatu.

4. W przypadku negatywnej oceny materiałów przekazanych przez wnioskodawcę lub niedotrzymania terminu, o którym mowa w ust. 1, ABW może odmówić rozpoczęcia badań. Informację o odmowie rozpoczęcia badań wraz z uzasadnieniem i pouczeniem o możliwości ponownego złożenia wniosku, dyrektor Departamentu I ABW przekazuje niezwłocznie wnioskodawcy.

§ 7. 1. Badania prowadzone w ramach certyfikacji są przeprowadzane przez zespoły badawcze Departamentu I ABW, a w razie konieczności inne jednostki organizacyjne ABW. W indywidualnych przypadkach, dyrektor Departamentu I ABW może zlecić wykonanie badań podmiotom zewnętrznym, zgodnie z art. 50 ust. 6 ustawy.

2. Przebieg badań oraz oceny bezpieczeństwa podlega dokumentowaniu w postaci raportów lub sprawozdań.

3. Dyrektor Departamentu I ABW, określa szczegółowe procedury postępowania zespołów badawczych Departamentu I ABW w zakresie prowadzonych badań i oceny bezpieczeństwa, w tym badań, o których mowa w § 8 ust. 1.

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

2. Warunkiem uzyskania certyfikatu ochrony kryptograficznej „zgodności" jest potwierdzenie przez zespół badawczy Departamentu I ABW poprawności funkcjonowania egzemplarza generatora danych losowych zainstalowanego w urządzeniu lub narzędziu kryptograficznym, które podlega certyfikacji.

3. W celu uzyskania potwierdzenia, o którym mowa w ust. 2, wnioskodawca składa wypełniony wniosek WK-01-Z, o którym mowa w § 5 ust. 1 pkt 1 lit. b.

4. Po potwierdzeniu deklarowanych właściwości generatora, zespół badawczy Departamentu I ABW sporządza świadectwo dopuszczenia do eksploatacji egzemplarza generatora danych losowych. O wyniku tego badania niezwłocznie informuje się wnioskodawcę.

5. Świadectwo, o którym mowa w ust. 4, sporządza dyrektor Departamentu I ABW lub upoważniony przez niego funkcjonariusz ABW i jest przechowywane w dokumentacji Departamentu I ABW.

6. Wzór świadectwa, o którym mowa w ust. 4, określa dyrektor Departamentu I ABW.

§ 9. 1. Po zakończeniu badań i oceny bezpieczeństwa, kierownik zespołu badawczego Departamentu I ABW kompletuje sprawozdania lub raporty cząstkowe z przeprowadzonych prac oraz dokonuje ich analizy.

2. Po wykonaniu czynności, o których mowa w ust. 1, zespół badawczy Departamentu I ABW sporządza raport z certyfikacji, który stanowi podstawę do wydania lub odmowy wydania certyfikatu.

3. Wyciąg z raportu z certyfikacji, o którym mowa w ust. 2, może być udostępniony wnioskodawcy na jego pisemny wniosek skierowany do dyrektora Departamentu I ABW.

§ 10. 1. Po zakończeniu certyfikacji mającej na celu wydanie certyfikatu ochrony kryptograficznej „typu", o którym mowa w § 3 ust. 1 pkt 1 lit. a, wnioskodawca przekazuje do Departamentu I ABW certyfikowane produkty, które przechowywane są jako egzemplarze wzorcowe. Ich liczbę, szczegóły kompletacji i ewentualne warunki przechowywania w depozycie Departamentu I ABW określa porozumienie, o którym mowa w § 6 ust. 3.

2. Wymogu przekazywania egzemplarzy wzorcowych, o których mowa w ust. 1, nie stosuje się w przypadku certyfikacji mającej na celu ponowne wydanie certyfikatu ochrony kryptograficznej „typu" dla tego samego urządzenia lub narzędzia kryptograficznego lub w przypadku, o którym mowa w § 12 ust. 8.

3. Egzemplarze wzorcowe, o których mowa w ust. 1, mogą być zwrócone na wniosek wnioskodawcy, po upływie okresu ważności lub wygaśnięciu otrzymanego certyfikatu.

§ 11. 1. Certyfikacja kończy się wydaniem lub odmową wydania certyfikatu.

2. O odmowie wydania certyfikatu dyrektor Departamentu I ABW niezwłocznie informuje pisemnie wnioskodawcę, podając przyczyny odmowy.

3. Certyfikaty, o których mowa w § 3 ust. 1:

1) pkt 1 lit. a i c oraz pkt 3 – wydaje Szef ABW;

2) pkt 1 lit. b oraz pkt 2 – wydaje dyrektor Departamentu I ABW, na podstawie odrębnego upoważnienia Szefa ABW.

4. Departament I ABW prowadzi ewidencję certyfikatów wydanych przez ABW.

5. Wydanie certyfikatu następuje po dokonaniu opłat z tytułu przeprowadzonych badań i oceny bezpieczeństwa w ramach certyfikacji oraz wydania certyfikatu.

6. Informacje o wydanych certyfikatach, o których mowa w § 3 ust. 1 pkt 1 lit. a i c oraz pkt 3, są publikowane na stronie BIP ABW.

§ 12. 1. Certyfikat jest wydawany dla produktu wyszczególnionego w certyfikacie.

2. Warunki oraz okres ważności certyfikatu są określone w wydanym certyfikacie.

3. Certyfikat ochrony kryptograficznej „zgodności", o którym mowa w § 3 ust. 1 pkt 1 lit. b, jest wydawany dla wersji produktu posiadającej ważny certyfikat ochrony kryptograficznej „typu", o którym mowa w § 3 ust. 1 pkt 1 lit. a.

4. W przypadku urządzenia lub narzędzia kryptograficznego przeznaczonego do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej, łączne posiadanie przez określony egzemplarz produktu obu, jednocześnie ważnych certyfikatów wymienionych w § 3 ust. 1 pkt 1 lit. a i b, umożliwia stosowanie go w systemie teleinformatycznym podlegającym akredytacji lub już akredytowanym.

5. Certyfikaty ochrony kryptograficznej „zgodności" mogą być wydawane na okres ważności certyfikatu ochrony kryptograficznej „typu" wydanego dla danej wersji produktu.

6. W przypadku, gdy dla wersji produktu określonej w certyfikatach ochrony kryptograficznej „zgodności" zostanie wydany kolejny certyfikat ochrony kryptograficznej „typu", certyfikaty ochrony kryptograficznej „zgodności" wydane dla dotychczasowej wersji produktu zachowują ważność na zasadach określonych w certyfikacie.

7. W przypadku wprowadzenia w produkcie posiadającym ważny, wydany na określoną wersję certyfikat, o którym mowa w § 3 ust. 1 pkt 1 lit. a i c oraz pkt 3, zmian niemających wpływu na mechanizmy bezpieczeństwa ani podstawową funkcjonalność produktu, dopuszcza się możliwość objęcia wydanym certyfikatem ochrony kryptograficznej nowego wydania produktu.

8. Celem wystąpienia o objęcie certyfikatem nowego wydania produktu, o którym mowa w ust. 7, wnioskodawca jest obowiązany dostarczyć do ABW:

1) wniosek WK-01-T, o którym mowa w § 5 ust. 1 pkt 1 lit. a;

2) dokumentację zmian wprowadzonych w nowym wydaniu produktu z uwzględnieniem przyczyn ich wprowadzenia;

3) dokumentację stanowiącą załączniki, o których mowa w § 5 ust. 2 pkt 1, zaktualizowaną pod względem zmian wyszczególnionych w dokumentacji, o której mowa w pkt 2.

9. Produkt w nowym wydaniu podlega badaniom w zakresie wprowadzonych zmian i ich wpływu na zmianę funkcjonalności i poziom bezpieczeństwa.

10. Badania, o których mowa w ust. 9, są prowadzone w sposób określony w § 7.

11. Zgodę na objęcie lub odmowę objęcia certyfikatem produktu, o którym mowa w ust. 7, wydaje Szef ABW.

§ 13. 1. Wygaśnięcie certyfikatu następuje w przypadku:

1) utraty przez produkt zdolności do ochrony informacji niejawnych;

2) wprowadzenia w produkcie zmian niezgodnych z wydanym certyfikatem;

3) utraty przez producenta produktu zdolności zapewnienia właściwego procesu produkcji certyfikowanego produktu oraz stwierdzenia naruszenia przez niego zasad wynikających z nadanych uprawnień i licencji;

4) stwierdzenia nieprzestrzegania warunków certyfikatu.

2. Dyrektor Departamentu I ABW informuje niezwłocznie wnioskodawcę o wygaśnięciu certyfikatu.

3. O wygaśnięciu certyfikatu, o którym mowa w § 3 ust. 1 pkt 1 oraz pkt 3, wnioskodawca niezwłocznie informuje wszystkie podmioty, które w swoich akredytowanych systemach teleinformatycznych wdrożyły urządzenia lub narzędzia objęte tym certyfikatem.

§ 14. ABW zapewnia ochronę przekazanych przez wnioskodawcę w trakcie badań i certyfikacji informacji stanowiących tajemnicę prawnie chronioną.

§ 15. 1. W sprawach certyfikacji rozpoczętych, a niezakończonych przed dniem wejścia w życie zarządzenia, stosuje się przepisy niniejszego zarządzenia.

2. Porozumienia zawarte na podstawie zarządzenia uchylanego w § 16 stają się porozumieniami, o których mowa w § 6 ust. 3.

§ 16. Traci moc 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 (Dz. Urz. ABW poz. 23).

§ 17. Zarządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

Szef
Agencji Bezpieczeństwa Wewnętrznego

płk Krzysztof Wacławek