Warszawa, dnia 9 kwietnia 2026 r.

Poz. 5

ZARZĄDZENIE NR 20
SZEFA AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO

z dnia 9 kwietnia 2026 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 2025 r. poz. poz. 902 i 1366 oraz z 2026 r. poz. 26) zarządza się, co następuje:

§ 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. z 2025 r. poz. 1209), zwanej dalej „ustawą".

§ 2. Użyte w zarządzeniu określenia oznaczają:

1) algorytm kryptograficzny Typu A – niejawny algorytm kryptograficzny, skonstruowany pod nadzorem ABW lub Służby Kontrwywiadu Wojskowego, pozytywnie oceniony przez ABW i dopuszczony do stosowania przez ABW, znajdujący się pod ścisłym nadzorem ABW;

2) produkt – przeznaczone do ochrony informacji niejawnych urządzenie lub narzędzie kryptograficzne albo urządzenie lub narzędzie służące do realizacji zabezpieczenia teleinformatycznego;

3) system teleinformatyczny – system teleinformatyczny w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2024 r. poz. 1513);

4) środek ochrony elektromagnetycznej – rozwiązanie techniczne lub organizacyjne, wykorzystywane do zapewnienia ochrony elektromagnetycznej informacji niejawnych, przetwarzanych przez urządzenia i systemy teleinformatyczne;

5) wersja produktu – odmianę produktu posiadającą ściśle określoną funkcjonalność, zapewniającą zdolności do ochrony informacji niejawnych na określonym poziomie;

6) wnioskodawca – podmiot, który złożył wniosek, o którym mowa w art. 50 ust. 3 ustawy, ubiegający się o przeprowadzenie przez ABW certyfikacji produktu lub środka ochrony elektromagnetycznej;

7) wydanie produktu – odmianę wersji produktu, różniącą się cechami, które nie mają wpływu na podstawową funkcjonalność oraz na poziom ochrony informacji niejawnych zapewniany przez produkt;

8) zalecenia – określone przez ABW minimalne wymagania, obejmujące:

   a) zalecenia ochrony elektromagnetycznej – minimalne wymagania określone przez ABW dla środków ochrony elektromagnetycznej, których spełnienie jest konieczne do uzyskania pozytywnych wyników oceny bezpieczeństwa, o których mowa w art. 50 ust. 4 ustawy,

   b) zalecenia bezpieczeństwa kryptograficznego – określone przez ABW wymagania w zakresie bezpieczeństwa kryptograficznego dla produktów, których spełnienie jest konieczne do uzyskania pozytywnych wyników oceny bezpieczeństwa, o których mowa w art. 50 ust. 4 ustawy;

9) 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 określonej wersji urządzenia lub narzędzia kryptograficznego, przeznaczonego do ochrony informacji niejawnych do klauzuli „poufne” i wyższej. Certyfikat ten umożliwia produkcję egzemplarzy produktu wyłącznie 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 bezpieczeństwa 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. Zalecenia stanowiące informacje niejawne, ABW udostępnia wnioskodawcom z uwzględnieniem przepisów o ochronie informacji niejawnych.

2. Zalecenia lub wyciąg z zaleceń niebędące informacjami niejawnymi mogą być umieszczane w Biuletynie Informacji Publicznej na stronie podmiotowej ABW, zwanym dalej „BIP ABW”, lub udostępniane indywidualnie wnioskodawcy na jego uzasadniony wniosek.

3. Spełnianie wymagań, zawartych w zaleceniach lub wyciągu z zaleceń jest weryfikowane przez ABW na każdym etapie certyfikacji.

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

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 i obiektów 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 z wyjątkiem badań obiektów ekranujących,

c) WE-01-O – w celu uzyskania certyfikatu, o którym mowa w § 3 ust. 1 pkt 2, w zakresie badań obiektów ekranujących z wyjątkiem badań kabin ekranujących,

d) 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. Wzory wniosków, o których mowa w ust. 1, są określane przez dyrektora Departamentu I ABW oraz publikowane w BIP ABW.

3. Do wniosków, o których mowa w ust. 1 pkt 1 i 3 dołącza się egzemplarze produktu, jeśli są wymagane i co do których wnioskodawca wyraża zgodę na ewentualne zniszczenie. Sposób i termin ich przekazania ustala się z zespołem badawczym Departamentu I ABW.

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

5. Nieuzupełnienie braków formalnych przez wnioskodawcę w terminie, o którym mowa w ust. 4, albo wycofanie wniosku przez wnioskodawcę powoduje zwrot wniosku, wraz z załącznikami i egzemplarzami produktu, o których mowa w ust. 1 i 3, bez rozpatrzenia.

6. Za dzień rozpoczęcia certyfikacji uznaje się dzień złożenia poprawnie wypełnionego wniosku i przekazania załączników, o których mowa w ust. 1, oraz egzemplarzy produktów, o których mowa w ust. 3, albo dzień ostatecznego uzupełnienia braków formalnych, o których mowa w ust. 4.

§ 6. 1. W terminie trzech miesięcy od dnia złożenia wniosku, o którym mowa w § 5 ust. 1 pkt 1 lit. a lub pkt 3, zespoły badawcze Departamentu I ABW dokonują wstępnej oceny przekazanych materiałów, w celu ustalenia zasadności i zdolności do poddania produktu badaniom oraz określenia niezbędnych zasobów warunkujących przeprowadzenie tych czynności. W uzasadnionych przypadkach termin ten może ulec przedłużeniu.

2. Na żądanie ABW, w czasie dokonywania przez zespół badawczy Departamentu I ABW wstępnej oceny przekazanych materiałów, o którym mowa w ust. 1, wnioskodawca ustala z ABW:

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 na wniosek, o którym mowa w § 5 ust. 1 pkt 1 lit. a lub ust. 3, jest prowadzona na podstawie porozumienia zawartego 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 przez wnioskodawcę niezbędnych narzędzi służących do implementacji algorytmu typu A,

b) bezpłatnego przekazania przez wnioskodawcę generatorów liczb losowych,

c) zdeponowania egzemplarzy wzorcowych, o których mowa w § 13,

d) udzielenia licencji na korzystanie z algorytmu typu A,

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 oceny bezpieczeństwa;

7) liczbę przekazanych egzemplarzy wzorcowych, o których mowa w § 13, oraz ewentualnie zasady ich przechowywania w Departamencie I ABW.

4. W przypadku negatywnego wyniku wstępnej oceny materiałów albo niedotrzymania terminu, o którym mowa w ust. 1 lub 2, ABW może odmówić rozpoczęcia badań i oceny bezpieczeństwa.

5. Informację o odmowie rozpoczęcia badań, o której mowa w ust. 4, wraz z uzasadnieniem i pouczeniem o możliwości ponownego złożenia wniosku, przekazuje się niezwłocznie wnioskodawcy.

§ 7. 1. W terminie trzech miesięcy od dnia złożenia wniosku, o którym mowa w § 5 ust. 1 pkt 2, zespoły badawcze Departamentu I ABW dokonują wstępnej oceny przekazanych materiałów, w celu ustalenia zasadności i zdolności do poddania środka ochrony elektromagnetycznej badaniom oraz określenia niezbędnych zasobów warunkujących przeprowadzenie tych czynności. W uzasadnionych przypadkach termin ten może ulec przedłużeniu.

2. W czasie dokonywania przez zespół badawczy Departamentu I ABW wstępnej oceny przekazanych materiałów, o którym mowa w ust. 1, wnioskodawca ustala z ABW:

1) szczegóły realizacji wniosku, w szczególności termin realizacji badań oraz termin dostarczenia środka ochrony elektromagnetycznej;

2) termin dostarczenia dodatkowej dokumentacji środka ochrony elektromagnetycznej lub odpowiednio skonfigurowanego sprzętu lub oprogramowania, niezbędnych do przeprowadzenia badań.

3. W przypadku negatywnego wyniku wstępnej oceny materiałów albo niedotrzymania terminu, o którym mowa w ust. 1, ABW może odmówić rozpoczęcia badań i oceny bezpieczeństwa.

4. Informację o odmowie rozpoczęcia badań, o której mowa w ust. 3, wraz z uzasadnieniem i pouczeniem o możliwości ponownego złożenia wniosku, przekazuje się niezwłocznie wnioskodawcy.

§ 8. 1. Badania prowadzone w ramach certyfikacji są realizowane przez zespoły badawcze Departamentu I ABW, a w razie konieczności przez inne jednostki organizacyjne ABW. W indywidualnych przypadkach mogą zostać zlecone podmiotom zewnętrznym, zgodnie z art. 50 ust. 6 ustawy.

2. Przebieg badań oraz oceny bezpieczeństwa podlega dokumentowaniu.

3. W przypadku wydzielonych komponentów sprzętowych bądź programowych urządzeń lub narzędzi kryptograficznych, które zostały przebadane w ramach innego procesu certyfikacji, można odstąpić od ich ponownego badania z wyłączeniem badań funkcjonalnych.

4. Dyrektor Departamentu I ABW, z uwzględnieniem przepisów ustawy, określa szczegółowe procedury postępowania zespołów badawczych Departamentu I ABW w zakresie prowadzonych badań i oceny bezpieczeństwa, w tym badań, o których mowa w § 9 ust. 1.

§ 9. 1. Generatory danych losowych, wykorzystywane w urządzeniach lub narzędziach kryptograficznych, podlegają badaniom oraz ocenie bezpieczeństwa realizowanym w ramach certyfikacji.

2. W przypadku gdy jednym z komponentów urządzenia lub narzędzia kryptograficznego podlegającego certyfikacji jest generator danych losowych to warunkiem uzyskania certyfikatu ochrony kryptograficznej „zgodności", o którym mowa w § 3 ust. 1 pkt 1 lit. b, jest potwierdzenie przez zespół badawczy Departamentu I ABW poprawności funkcjonowania egzemplarza generatora danych losowych, zainstalowanego w tym urządzeniu lub narzędziu kryptograficznym.

3. W celu uzyskania potwierdzenia poprawności deklarowanych funkcjonalności generatora danych losowych, 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. Wnioskodawca jest niezwłocznie informowany o wynikach badań, o których mowa w ust. 1.

5. W Departamencie I ABW prowadzi się, w postaci elektronicznej, ewidencję generatorów danych losowych, o których mowa w ust. 1.

§ 10. 1. Po zakończeniu badań i oceny bezpieczeństwa, mającej na celu wydanie certyfikatu, o którym mowa w § 3 ust. 1 pkt 1 lit. a oraz pkt 3, kierownik zespołu badawczego Departamentu I ABW kompletuje sprawozdania lub raporty cząstkowe z przeprowadzonych prac oraz dokonuje ich analizy.

2. Po przeprowadzeniu analizy, o której 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.

§ 11. 1. Po zakończeniu badań i oceny bezpieczeństwa, mającej na celu wydanie certyfikatu ochrony kryptograficznej „zgodności", o którym mowa w § 3 ust. 1 pkt 1 lit. b, zespół badawczy Departamentu I ABW sporządza sprawozdanie z przeprowadzonych prac oraz dokonuje jego analizy.

2. Sprawozdanie, o którym mowa w ust. 1, stanowi podstawę do wydania lub odmowy wydania certyfikatu.

§ 12. Po zakończeniu badań i oceny bezpieczeństwa, mającej na celu wydanie certyfikatu ochrony elektromagnetycznej zespół badawczy Departamentu I ABW sporządza raport z przeprowadzonych prac oraz dokonuje jego analizy.

2. Raport, o którym mowa w ust. 1, stanowi podstawę do wydania lub odmowy wydania certyfikatu.

§ 13. 1. Po zakończeniu certyfikacji mającej na celu wydanie certyfikatu ochrony kryptograficznej „typu", o którym mowa w § 3 ust. 1 pkt 1 lit. a, na podstawie porozumienia, o którym mowa w § 6 ust. 3, wnioskodawca przekazuje do Departamentu I ABW certyfikowane produkty, które są przechowywane jako egzemplarze wzorcowe.

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 tej samej wersji urządzenia lub narzędzia kryptograficznego albo w przypadku wystąpienia o objęcie certyfikatem nowego wydania produktu, o którym mowa w § 16 ust. 1.

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

2. Certyfikat, o którym mowa w § 3 ust. 1:

1) pkt 1 lit. a i c oraz pkt 3 – wydaje lub odmawia jego wydania Szef ABW;

2) pkt 1 lit. b oraz pkt 2 – wydaje lub odmawia jego wydania dyrektor Departamentu I ABW, na podstawie upoważnienia udzielonego przez Szefa ABW.

3. O odmowie wydania certyfikatu informuje się pisemnie wnioskodawcę, podając przyczyny odmowy.

4. W Departamencie I ABW prowadzi się, w postaci elektronicznej, ewidencję certyfikatów wydanych przez ABW.

5. Wydany certyfikat przekazuje się wnioskodawcy po potwierdzeniu uiszczenia opłat, o których mowa w przepisach wykonawczych wydanych na podstawie art. 53 ust. 4 ustawy, z tytułu przeprowadzonych badań, oceny bezpieczeństwa oraz wydania certyfikatu.

6. W przypadku jednostek organizacyjnych, o których mowa w art. 53 ust. 2 ustawy, certyfikat przekazuje się bezpośrednio po jego wydaniu.

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

8. W odniesieniu do certyfikatów wydanych dla produktów certyfikowanych na potrzeby ABW, ust. 7 nie stosuje się.

§ 15. 1. Certyfikat jest wydawany dla produktu lub środka ochrony elektromagnetycznej wyszczególnionego w certyfikacie.

2. Certyfikat ochrony kryptograficznej, o którym mowa w § 3 ust. 1 pkt 1 lit. a i c zawiera w szczególności:

1) numer certyfikatu;

2) nazwę i wersję produktu;

3) informacje o producencie i wnioskodawcy;

4) poziom ochrony produktu;

5) warunki ważności certyfikatu, w tym warunki eksploatacyjne, jeśli są wymagane.

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. Stosowanie urządzenia lub narzędzia kryptograficznego, przeznaczonego do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej, w akredytowanym systemie teleinformatycznym albo systemie teleinformatycznym podlegającym akredytacji, dopuszczalne jest wyłącznie przy jednoczesnym posiadaniu przez określony egzemplarz produktu ważnych certyfikatów ochrony kryptograficznej „typu" i „zgodności", o których mowa w § 3 ust. 1 pkt 1 lit. a i b.

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

6. W przypadku wydania kolejnego certyfikatu ochrony kryptograficznej „typu” dla wersji produktu określonej w certyfikatach ochrony kryptograficznej „zgodności”, certyfikaty ochrony kryptograficznej „zgodności” wydane dla dotychczasowej wersji produktu zachowują ważność na zasadach określonych w certyfikacie.

7. Certyfikat ochrony elektromagnetycznej, o którym mowa w § 3 ust. 1 pkt 2, zawiera w szczególności:

1) numer certyfikatu;

2) informacje o środku ochrony elektromagnetycznej i wnioskodawcy;

3) warunki ważności certyfikatu, w tym warunki eksploatacyjne, jeśli są wymagane.

§ 16. 1. W przypadku wprowadzenia zmian w produkcie posiadającym ważny certyfikat, o którym mowa w § 3 ust. 1 pkt 1 lit. a i c oraz pkt 3, które nie mają wpływu na mechanizmy bezpieczeństwa, podstawową funkcjonalność produktu oraz treść certyfikatu, dopuszcza się możliwość objęcia obowiązującym certyfikatem produktu w nowym wydaniu, z zastrzeżeniem ust. 3.

2. W celu wystąpienia o objęcie certyfikatem produktu w nowym wydaniu, o którym mowa w ust. 1, 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 wyjaśnieniem przyczyn ich wprowadzenia;

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

3. Produkt w nowym wydaniu oraz dokumentacja, o której mowa w ust. 2 pkt 2 i 3 podlegają badaniom w zakresie wprowadzonych zmian i ich wpływu na zmianę funkcjonalności i poziom bezpieczeństwa.

4. Badania, o których mowa w ust. 3, są prowadzone w sposób określony w § 8.

5. Zgodę na objęcie lub odmowę objęcia certyfikatem nowego wydania produktu, o którym mowa w ust. 1, wydaje Szef ABW.

§ 17. 1. Utrata ważności certyfikatu ochrony kryptograficznej 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 do zapewnienia właściwego procesu produkcji certyfikowanego produktu oraz stwierdzenia naruszenia przez niego zasad wynikających z nadanych mu uprawnień i licencji;

4) stwierdzenia nieprzestrzegania warunków ważności certyfikatu.

2. Po potwierdzeniu informacji o zaistnieniu przesłanki, o której mowa w ust. 1, w Departamencie I ABW przeprowadza się analizę zagrożeń dla bezpieczeństwa informacji niejawnych przetwarzanych przez produkt objęty certyfikatem, o którym mowa w § 3 ust. 1 pkt 1 i 3.

3. W przypadku braku możliwości niezwłocznego usunięcia lub zminimalizowania skutków zidentyfikowanych zagrożeń dla bezpieczeństwa informacji niejawnych przetwarzanych przez certyfikowany produkt, Szef ABW albo dyrektor Departamentu I ABW, na podstawie upoważnienia udzielonego przez Szefa ABW, stwierdza utratę ważności certyfikatu. Do stwierdzenia utraty ważności certyfikatu stosuje się przepisy § 14 ust. 2.

4. O stwierdzeniu utraty ważności certyfikatu niezwłocznie informuje się wnioskodawcę.

5. O stwierdzeniu utraty ważności certyfikatu, o którym mowa w § 3 ust. 1 pkt 1 oraz pkt 3, wnioskodawca niezwłocznie informuje wszystkie podmioty, którym zostały przekazane urządzenia lub narzędzia objęte tym certyfikatem.

6. Certyfikat ochrony kryptograficznej, który utracił ważność, podlega zwrotowi do ABW.

§ 18. 1. Utrata ważności certyfikatu ochrony elektromagnetycznej, o którym mowa w § 3 ust. 1 pkt 2, następuje w przypadku:

1) nieprzestrzegania warunków ważności certyfikatu przez wnioskodawcę;

2) wycofania z użytkowania środka ochrony elektromagnetycznej.

2. W przypadku uzyskania informacji mających wpływ na ważność certyfikatu ochrony elektromagnetycznej, o którym mowa w ust. 1 pkt 1, w Departamencie I ABW przeprowadza się analizę zagrożeń dla bezpieczeństwa informacji niejawnych przetwarzanych przez środek ochrony elektromagnetycznej objęty certyfikatem, o którym mowa w § 3 ust. 2.

3. W przypadku braku możliwości niezwłocznego usunięcia lub zminimalizowania skutków zidentyfikowanych zagrożeń dla bezpieczeństwa informacji niejawnych przetwarzanych przez certyfikowany środek ochrony elektromagnetycznej, dyrektor Departamentu I ABW, na podstawie upoważnienia udzielonego przez Szefa ABW, może stwierdzić utratę ważności certyfikatu.

4. O utracie ważności certyfikatu niezwłocznie informuje się wnioskodawcę.

5. W przypadku wycofania z użytkowania środka ochrony elektromagnetycznej certyfikat ochrony elektromagnetycznej podlega zwrotowi do ABW.

§ 19. Do certyfikacji, o której mowa w art. 50 ust. 1-3 ustawy, prowadzonej na potrzeby ABW przepisy zarządzenia dotyczące w szczególności podpisywania porozumień, udostępniania licencji i składania wniosków przez jednostkę badawczą, stosuje się odpowiednio, z uwzględnieniem procedur, o których mowa w § 8 ust.4.

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

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

2. Porozumienia zawarte na podstawie zarządzenia uchylanego w § 22, pozostają w mocy do czasu zakończenia certyfikacji, której dotyczą.

§ 22. Traci moc 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 (Dz. Urz. ABW poz. 7).

§ 23. Zarządzenie wchodzi w życie po upływie jednego miesiąca od dnia ogłoszenia.

Szef
Agencji Bezpieczeństwa Wewnętrznego

płk Rafał Syrysko