Warszawa, dnia 14 października 2022 r.

Poz. 2098

ROZPORZĄDZENIE
MINISTRA OBRONY NARODOWEJ

z dnia 29 września 2022 r.

w sprawie trybu oceny i sposobu dopuszczania rozwiązań informatycznych, w których mają być przetwarzane informacje niejawne

Na podstawie art. 51 ust. 6 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742 oraz z 2022 r. poz. 655 i 1933) zarządza się, co następuje:

§ 1. Rozporządzenie określa tryb oceny i sposób dopuszczania rozwiązań informatycznych niebędących systemami teleinformatycznymi do przetwarzania informacji niejawnych.

§ 2. Ilekroć w rozporządzeniu jest mowa o:

1) dopuszczeniu rozwiązania informatycznego – należy przez to rozumieć formalne potwierdzenie realizacji wymogów określonych w rozporządzeniu w odniesieniu do rozwiązania informatycznego;

2) dostępności – należy przez to rozumieć właściwość zasobu określającą możliwość jego wykorzystania na żądanie, w założonym czasie, przez uprawniony podmiot;

3) gestorze rozwiązania informatycznego – należy przez to rozumieć jednostkę lub komórkę organizacyjną odpowiedzialną za realizację czynności związanych z oceną rozwiązania informatycznego planowanego do przetwarzania informacji niejawnych;

4) głównym użytkowniku – należy przez to rozumieć kierownika jednostki organizacyjnej, w której jest eksploatowane rozwiązanie informatyczne podlegające dopuszczeniu;

5) incydencie – należy przez to rozumieć incydent w rozumieniu art. 2 pkt 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863);

6) integralności – należy przez to rozumieć właściwość zasobu określającą, że nie został on zmodyfikowany w sposób nieuprawniony;

7) komponencie rozwiązania informatycznego – należy przez to rozumieć część rozwiązania informatycznego realizującą daną funkcjonalność w jego obrębie;

8) podatności – należy przez to rozumieć słabość zasobu lub zabezpieczenia, która może zostać wykorzystana przez zagrożenie;

9) poufności – należy przez to rozumieć właściwość określającą, że informacja nie jest udostępniana lub ujawniana nieuprawnionym do tego podmiotom;

10) przekazywaniu informacji – należy przez to rozumieć zarówno przekazywanie informacji na informatycznych nośnikach danych, na których zostały utrwalone, jak i w formie teletransmisji;

11) rozwiązaniu informatycznym – należy przez to rozumieć rozwiązanie informatyczne, o którym mowa w art. 2 pkt 19 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, zwanej dalej „ustawą”;

12) ryzyku – należy przez to rozumieć ryzyko w rozumieniu art. 2 pkt 12 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

13) SKW – należy przez to rozumieć Służbę Kontrwywiadu Wojskowego;

14) testach bezpieczeństwa – należy przez to rozumieć testy mające na celu weryfikację poprawności i skuteczności funkcjonowania zabezpieczeń, ustalenie ich aktualnego stanu oraz rekomendowanie skutecznych rozwiązań służących zapewnieniu odporności rozwiązania informatycznego oraz współpracujących z nim systemów teleinformatycznych na zagrożenia, w skład których wchodzą testy weryfikacyjne, podatnościowe oraz penetracyjne;

15) testach penetracyjnych – należy przez to rozumieć element testów bezpieczeństwa obejmujący zaplanowanie i przeprowadzenie kontrolowanego ataku mającego na celu praktyczną weryfikację poprawności i skuteczności funkcjonowania procedur i zabezpieczeń oraz opracowanie rekomendacji dotyczących skutecznych rozwiązań, które zwiększają poziom odporności rozwiązania informatycznego oraz współpracujących z nim systemów teleinformatycznych na zagrożenia;

16) testach podatnościowych – należy przez to rozumieć element testów bezpieczeństwa umożliwiający:

   a) identyfikację oraz ocenę wagi podatnych na zagrożenia słabych punktów w rozwiązaniu informatycznym oraz interfejsach współpracujących z nim systemów teleinformatycznych, w tym w wykorzystywanych w nich rozwiązaniach sprzętowych, programowych, infrastrukturalnych oraz organizacyjnych,

   b) dostarczanie gestorowi rozwiązania informatycznego informacji o rzeczywistych podatnościach zasobów niezbędnych do prawidłowego projektowania, wdrażania i optymalizacji jego zabezpieczeń, przy uwzględnieniu wyników szacowania ryzyka;

17) testach weryfikacyjnych – należy przez to rozumieć element testów bezpieczeństwa mający na celu weryfikację poprawności implementacji zabezpieczeń w rozwiązaniu informatycznym oraz w interfejsach współpracujących z nim systemów teleinformatycznych;

18) zabezpieczeniu – należy przez to rozumieć środki o charakterze fizycznym, technicznym lub proceduralnym zmniejszające ryzyko;

19) zagrożeniu – należy przez to rozumieć potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w rozwiązaniu informatycznym oraz we współpracujących z nim systemach teleinformatycznych.

§ 3. W ramach rozwiązań informatycznych dopuszcza się przetwarzanie informacji na poziomach taktycznym i operacyjnym, niezbędne do wykonania zadania realizowanego z wykorzystaniem danego rozwiązania informatycznego, w szczególności o krótkotrwałym charakterze przetwarzanych informacji niejawnych.

§ 4. W ramach trybu oceny za rozwiązania informatyczne niebędące systemem teleinformatycznym można uznawać wyłącznie sprzęt wojskowy lub sprzęt, który podlega procesowi pozyskiwania w ramach procedury pozyskiwania, zwany dalej „SpW”, oraz jego elementy.

§ 5. 1. Rozwiązania informatyczne ocenia się w zakresie wdrożenia spójnego zbioru zabezpieczeń służących zapewnieniu zachowania bezpieczeństwa informacji niejawnych przetwarzanych przy ich zastosowaniu, na podstawie właściwego doboru w danym rozwiązaniu informatycznym metod realizacji następujących celów bezpieczeństwa:

1) poufności informacji niejawnych;

2) integralności informacji niejawnych;

3) dostępności informacji niejawnych.

2. Realizując cele bezpieczeństwa:

1) wdraża się spójny zbiór zabezpieczeń w zakresie bezpieczeństwa osobowego, bezpieczeństwa fizycznego, bezpieczeństwa informatycznego, a także odpowiednie procedury związane z wykorzystywaniem rozwiązań informatycznych do określonych zastosowań;

2) ogranicza się zakres obszarów zastosowania rozwiązań informatycznych z uwzględnieniem sposobu i przypadków ich użycia;

3) ogranicza się dostęp do wykorzystania rozwiązań informatycznych tylko przez podmioty uprawnione w zakresie wynikającym z ich zadań oraz wyłącznie w zakresie niezbędnym do ich realizacji;

4) stosuje się wielopoziomową ochronę, polegającą na stosowaniu zabezpieczeń na różnych poziomach, w celu ograniczenia występowania przypadków, w których przełamanie pojedynczego zabezpieczenia skutkuje przełamaniem pozostałych;

5) wdraża się procedury wymiany informacji niejawnych z systemami teleinformatycznymi;

6) zapewnia się sprawowanie nadzoru nad poprawną eksploatacją rozwiązania informatycznego zgodnie z warunkami jego dopuszczenia.

3. Projektując zbiór zabezpieczeń, o których mowa w ust. 2, stosuje się, w zależności od możliwości technicznych oraz poziomu ryzyka ujawnienia, utraty lub naruszenia integralności informacji niejawnych, odpowiednio do zadań realizowanych przy wykorzystywaniu rozwiązań informatycznych:

1) zabezpieczenia realizujące kontrolę dostępu do zasobów rozwiązań informatycznych, w szczególności zapewnienie ochrony fizycznej ich komponentów;

2) warunki i sposób przydziału uprawnień do eksploatacji rozwiązań informatycznych;

3) procedury postępowania związane z wykorzystywaniem rozwiązań informatycznych, w tym w czasie wojny, w razie ogłoszenia stanu nadzwyczajnego, mobilizacji lub sytuacji kryzysowej;

4) środki zapewniające ochronę transmisji danych przed wykryciem, przechwyceniem lub zakłóceniem;

5) środki zapewniające ochronę elektromagnetyczną;

6) mechanizmy lub procedury dotyczące reagowania na incydenty;

7) inne niezbędne procedury i mechanizmy zabezpieczania informacji niejawnych przetwarzanych w ramach rozwiązania informatycznego.

4. Działania, o których mowa w ust. 3, opisuje się szczegółowo w dokumencie „Wymagania ochrony informacji niejawnych" opracowywanym dla danego rozwiązania informatycznego.

§ 6. 1. W celu zagwarantowania poufności i integralności informacji niejawnych przekazywanych przez komponenty rozwiązań informatycznych, w formie transmisji poza obszarami objętymi ochroną fizyczną, stosuje się ochronę kryptograficzną.

2. Doboru rozwiązań z zakresu ochrony kryptograficznej, o których mowa w ust. 1, dokonuje się z uwzględnieniem wyników procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych za pomocą rozwiązania informatycznego oraz opinii Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni.

§ 7. W celu zagwarantowania poufności informacji niejawnych przetwarzanych przy użyciu rozwiązań informatycznych, zagrożonych w wyniku elektromagnetycznej emisji ujawniającej, rozwiązania z zakresu ochrony elektromagnetycznej dobiera się z uwzględnieniem wyników procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych. W szczególnym przypadku rozwiązania informatyczne lub ich komponenty mogą podlegać badaniom poziomu ich emisyjności w celu zapewnienia właściwej ochrony elektromagnetycznej, z uwzględnieniem zaleceń.

§ 8. W celu zagwarantowania realizacji procesu wykrywania incydentów, a także zapewnienia niezwłocznego informowania odpowiednich osób o wykrytym incydencie, w dokumencie „Wymagania ochrony informacji niejawnych" stosuje się procedury reagowania na incydenty związane z przetwarzaniem informacji niejawnych za pomocą rozwiązań informatycznych.

§ 9. W celu zapewnienia właściwej ochrony informacji niejawnych przetwarzanych w ramach rozwiązania informatycznego na niejawnych wymiennych informatycznych nośnikach danych, które można wyodrębnić z rozwiązania informatycznego, stosuje się procedury właściwe dla ochrony materiału niejawnego w rozumieniu art. 2 pkt 4 ustawy, stosownie do najwyższej klauzuli przechowywanych informacji.

§ 10. 1. Rozwiązania informatyczne dopuszczone do przetwarzania informacji niejawnych mogą wymieniać informacje niejawne z systemami teleinformatycznymi posiadającymi akredytację bezpieczeństwa teleinformatycznego w rozumieniu przepisów ustawy z zastosowaniem wyłącznie procedur określonych w dokumencie „Wymagania ochrony informacji niejawnych", które zostały uwzględnione w dokumentacji szczególnych wymagań bezpieczeństwa oraz procedur bezpiecznej eksploatacji dla przedmiotowego systemu, wykonanymi według wymagań ustawy.

2. Wymianę informacji, o której mowa w ust. 1, realizuje się, zapewniając minimalizację wymienianych danych, stosownie do sytuacji i realizowanych zadań, oraz odpowiednio uwzględnia się wymaganie ograniczonego zaufania, o którym mowa w przepisach wydanych na podstawie art. 49 ust. 9 ustawy, z tym zastrzeżeniem, że potencjalnym źródłem zagrożeń może być zarówno inny system teleinformatyczny, jak i inne rozwiązanie informatyczne.

§ 11. Dopuszczenie rozwiązania informatycznego do przetwarzania informacji niejawnych realizuje się przed rozpoczęciem przetwarzania informacji niejawnych w ramach jego eksploatacji.

§ 12. 1. W celu dopuszczenia rozwiązań informatycznych do przetwarzania informacji niejawnych, w rozumieniu art. 51 ust. 3 ustawy, opracowuje się dokument „Wymagania ochrony informacji niejawnych".

2. Dokument „Wymagania ochrony informacji niejawnych" zawiera informacje o:

1) rodzajach oraz najwyższej klauzuli informacji niejawnych, które mogą być przetwarzane za pomocą rozwiązania informatycznego;

2) przeznaczeniu rozwiązania informatycznego;

3) podmiotach uprawnionych do eksploatacji rozwiązania informatycznego;

4) podmiocie sprawującym nadzór nad eksploatacją zgodną z warunkami określonymi w dokumencie „Wymagania ochrony informacji niejawnych”;

5) wymaganych środkach w zakresie bezpieczeństwa osobowego przed dopuszczeniem do pracy z wykorzystaniem rozwiązania informatycznego;

6) środkach ochrony fizycznej komponentów rozwiązania informatycznego;

7) rozwiązaniach w zakresie zapewnienia ochrony elektromagnetycznej;

8) stosowaniu ochrony kryptograficznej lub innych rozwiązań w zakresie bezpieczeństwa transmisji;

9) certyfikatach lub innych dokumentach potwierdzających ocenę bezpieczeństwa rozwiązania informatycznego lub jego komponentu wydanych przez krajowe władze bezpieczeństwa państwa członkowskiego NATO lub UE lub właściwy organ NATO lub UE;

10) ochronie nośników danych, w szczególności ich ochronie fizycznej;

11) procedurach wykorzystania rozwiązania informatycznego w stanach nadzwyczajnych, w tym w czasie wojny, w razie ogłoszenia stanu nadzwyczajnego, mobilizacji lub sytuacji kryzysowej;

12) niezbędnych szkoleniach dla podmiotów użytkujących rozwiązania informatyczne;

13) procedurach wymiany danych z systemami teleinformatycznymi posiadającymi akredytację bezpieczeństwa teleinformatycznego oraz systemami informacyjnymi, o których mowa w art. 2 pkt 14 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

14) procedurach reagowania na incydenty związane z eksploatacją rozwiązania informatycznego;

15) procedurach reagowania na incydenty związane z przetwarzaniem informacji niejawnych za pomocą rozwiązań informatycznych;

16) wynikach procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w ramach rozwiązania informatycznego;

17) przyjętych w ramach zarządzania ryzykiem sposobów osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa informacji niejawnych przetwarzanych w ramach rozwiązania informatycznego;

18) aspektach budowy, dostępnych trybów pracy, działania i eksploatacji rozwiązania informatycznego, które mają związek z bezpieczeństwem informacji niejawnych przetwarzanych w ramach rozwiązania informatycznego lub wpływają na ich bezpieczeństwo;

19) oświadczeniu zrealizowania procesu oceny bezpieczeństwa rozwiązania informatycznego zgodnie z wymogami niniejszego rozporządzenia;

20) wykazie zaleceń i wymagań dla głównego użytkownika;

21) innych danych niezbędnych do prawidłowego wdrożenia rozwiązania informatycznego oraz prawidłowej ochrony informacji niejawnych.

§ 13. Tryb oceny bezpieczeństwa rozwiązania informatycznego przeznaczonego do przetwarzania informacji niejawnych realizowany przez:

1) Szefa Sztabu Generalnego Wojska Polskiego, zwanego dalej „Szefem Sztabu Generalnego WP” – obejmuje czynności, o których mowa w § 14 pkt 2 i 3;

2) gestora rozwiązania informatycznego – obejmuje czynności, o których mowa w § 15.

§ 14. W zakresie czynności realizowanych w ramach trybu oceny rozwiązania informatycznego przeznaczonego do przetwarzania informacji niejawnych Szef Sztabu Generalnego WP podejmuje następujące czynności:

1) wyznacza, w formie rozkazu, gestora rozwiązania informatycznego oraz wyznacza lub wskazuje eksperckie jednostki wspierające;

2) akceptuje wyniki procesu szacowania ryzyka zrealizowanego przez gestora rozwiązania informatycznego oraz zapewnia właściwą organizację ochrony informacji niejawnych, związanej z eksploatacją rozwiązania informatycznego w Siłach Zbrojnych Rzeczypospolitej Polskiej, z uwzględnieniem wyników przedmiotowego procesu;

3) zatwierdza i przesyła do SKW dokument „Wymagania ochrony informacji niejawnych”;

4) nadzoruje realizację zadań przez gestora rozwiązania informatycznego;

5) informuje SKW, w formie pisemnej, o wycofaniu rozwiązania informatycznego z eksploatacji;

6) prowadzi wykaz rozwiązań informatycznych dopuszczonych do przetwarzania informacji niejawnych przez SKW.

§ 15. 1. W zakresie czynności realizowanych w ramach trybu oceny rozwiązania informatycznego przeznaczonego do przetwarzania informacji niejawnych gestor rozwiązania informatycznego, na etapie planowania, projektowania i pozyskania rozwiązania informatycznego:

1) analizuje kierunki zastosowania rozwiązania informatycznego w Siłach Zbrojnych Rzeczypospolitej Polskiej, w tym w czasie wojny, w razie ogłoszenia stanu nadzwyczajnego, mobilizacji lub sytuacji kryzysowej;

2) analizuje funkcjonalności zabezpieczeń dostarczanych przez dane rozwiązanie informatyczne, które mogą zostać zastosowane do zabezpieczenia poufności, integralności i dostępności informacji niejawnych;

3) przeprowadza proces wstępnego szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych z zastosowaniem rozwiązania informatycznego;

4) projektuje zbiór dodatkowych zabezpieczeń, z uwzględnieniem wymogów określonych w § 5 ust. 2 i 3 oraz z uwzględnieniem wyników realizacji czynności, o których mowa w pkt 1–3;

5) współpracuje z instytucjami odpowiedzialnymi za pozyskanie i wprowadzenie na wyposażenie Sił Zbrojnych Rzeczypospolitej Polskiej „SpW" zawierającego rozwiązania informatyczne lub ich komponenty;

6) współpracuje z eksperckimi jednostkami wspierającymi, o których mowa w § 14 pkt 1.

2. Na etapie, o którym mowa w ust. 1, gestor rozwiązania informatycznego może opracować i uzgodnić z SKW plan dopuszczenia rozwiązania informatycznego. Plan ten obejmuje zakres i harmonogram przedsięwzięć wymaganych do uzyskania dopuszczenia rozwiązania informatycznego do przetwarzania informacji niejawnych. Opracowanie planu możliwe jest w przypadkach rozpatrywania szczególnie skomplikowanych rozwiązań informatycznych.

3. Na etapie wdrażania rozwiązania informatycznego gestor rozwiązania informatycznego odpowiada za:

1) analizę funkcjonalności dodatkowych zabezpieczeń zastosowanych do wzmocnienia poziomu ochrony dostarczanych przez dane rozwiązanie informatyczne, które mogą zostać zastosowane do zabezpieczenia poufności, integralności i dostępności przetwarzanych informacji niejawnych;

2) przeprowadzenie procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych z zastosowaniem rozwiązania informatycznego, z uwzględnieniem przepisów ustawy;

3) opracowanie procedur wymiany informacji oraz stosowanie dodatkowych zabezpieczeń na styku z systemami teleinformatycznymi, z uwzględnieniem postanowień, o których mowa w § 10;

4) zaplanowanie i przeprowadzenie testów bezpieczeństwa we współpracy z Dowódcą Komponentu Wojsk Obrony Cyberprzestrzeni;

5) opracowanie dokumentu „Wymagania ochrony informacji niejawnych" dla danego rozwiązania informatycznego;

6) współpracę z eksperckimi jednostkami wspierającymi, o których mowa w § 14 pkt 1;

7) uzgodnienie dokumentu „Wymagania ochrony informacji niejawnych" z właściwym pełnomocnikiem do spraw ochrony informacji niejawnych oraz Dowódcą Komponentu Wojsk Obrony Cyberprzestrzeni.

4. Na etapie eksploatacji rozwiązania informatycznego gestor rozwiązania informatycznego odpowiada za:

1) nadzór nad utrzymywaniem zgodności eksploatacji rozwiązania informatycznego z dokumentem „Wymagania ochrony informacji niejawnych";

2) prowadzenie szkoleń w zakresie eksploatacji rozwiązania informatycznego zgodnie z dokumentem „Wymagania ochrony informacji niejawnych";

3) bieżące monitorowanie podatności, zagrożeń, poziomu ryzyka, oraz w miarę potrzeb wprowadzanie adekwatnych zmian w dokumencie „Wymagania ochrony informacji niejawnych";

4) konsultowanie, w przypadku dostrzeżenia takiej potrzeby, planowanych do wprowadzenia zmian z właściwym pełnomocnikiem do spraw ochrony informacji niejawnych lub Dowódcą Komponentu Wojsk Obrony Cyberprzestrzeni.

5. Na etapie wycofywania rozwiązania informatycznego gestor rozwiązania informatycznego odpowiada za koordynowanie przedsięwzięć związanych z wycofaniem z wyposażenia Sił Zbrojnych Rzeczypospolitej Polskiej rozwiązania informatycznego.

§ 16. Główny użytkownik, w ramach dopuszczenia rozwiązania informatycznego na etapie eksploatacji i wycofywania, odpowiada za przestrzeganie wymagań i zaleceń określonych w dokumencie „Wymagania ochrony informacji niejawnych".

§ 17. W zakresie czynności realizowanych w ramach trybu oceny rozwiązania informatycznego przeznaczonego do przetwarzania informacji niejawnych ekspercka jednostka wspierająca, o której mowa w § 14 pkt 1, jest obowiązana udzielać pomocy gestorowi w procesie oceny i dopuszczenia rozwiązania informatycznego do przetwarzania informacji niejawnych – zgodnie z zakresem posiadanych kompetencji.

§ 18. W celu dopuszczenia rozwiązania informatycznego do przetwarzania informacji niejawnych dokument „Wymagania ochrony informacji niejawnych" jest opracowywany przez gestora rozwiązania informatycznego, a następnie podlega uzgodnieniu z:

1) właściwym pełnomocnikiem do spraw ochrony informacji niejawnych – w zakresie zgodności z przepisami ustawy;

2) Dowódcą Komponentu Wojsk Obrony Cyberprzestrzeni – w zakresie zapewnienia odporności rozwiązania informatycznego na zagrożenia pochodzące z cyberprzestrzeni przy zastosowaniu rozwiązań w nim opisanych.

§ 19. W ramach trybu dopuszczenia rozwiązania informatycznego do przetwarzania informacji niejawnych uzgodniony dokument „Wymagania ochrony informacji niejawnych", podpisany przez gestora rozwiązania informatycznego, po zatwierdzeniu, Szef Sztabu Generalnego WP przesyła do SKW. W przypadku braku uzgodnień, o których mowa w § 18, dokument nie jest rozpatrywany.

§ 20. 1. SKW rozstrzyga w przedmiocie dopuszczenia rozwiązania informatycznego po otrzymaniu dokumentu „Wymagania ochrony informacji niejawnych". O dopuszczeniu rozwiązania informatycznego SKW informuje, w formie pisemnej, Szefa Sztabu Generalnego WP.

2. Rozstrzygnięcie w przedmiocie dopuszczenia rozwiązania informatycznego jest podejmowane bez zbędnej zwłoki, jednak nie później niż w ciągu 3 miesięcy od dnia otrzymania dokumentu „Wymagania ochrony informacji niejawnych".

3. W sprawach szczególnie skomplikowanych rozstrzygnięcie w przedmiocie dopuszczenia rozwiązania informatycznego jest podejmowane nie później niż w ciągu 6 miesięcy od dnia otrzymania dokumentu „Wymagania ochrony informacji niejawnych".

4. SKW, na podstawie wyników oceny bezpieczeństwa rozwiązania informatycznego, przy uwzględnieniu poziomu zagrożenia bezpieczeństwa informacji niejawnych, określa termin ważności dopuszczenia, a także może skrócić jego termin ważności, zawiesić dopuszczenie lub je cofnąć w każdym czasie. O wyniku rozstrzygnięcia informuje, w formie pisemnej, Szefa Sztabu Generalnego WP.

§ 21. Brak informacji o dopuszczeniu rozwiązania informatycznego, o której mowa w § 20 ust. 1, jest równoznaczny z brakiem dopuszczenia rozwiązania informatycznego do przetwarzania informacji niejawnych.

§ 22. 1. W ramach trybu dopuszczenia rozwiązań informatycznych do przetwarzania informacji niejawnych, po uzyskaniu dopuszczenia SKW, Szef Sztabu Generalnego WP umieszcza dane rozwiązanie w wykazie rozwiązań informatycznych dopuszczonych do przetwarzania informacji niejawnych.

2. Wykaz, o którym mowa w ust. 1, zawiera:

1) nazwę rozwiązania informatycznego;

2) maksymalną klauzulę tajności informacji niejawnych, do których przetwarzania rozwiązanie informatyczne zostało dopuszczone;

3) gestora rozwiązania informatycznego;

4) okres ważności dopuszczenia rozwiązania informatycznego;

5) inne dane niezbędne do prawidłowego wdrożenia rozwiązania informatycznego.

§ 23. 1. W przypadku wprowadzania zmian w dokumencie „Wymagania ochrony informacji niejawnych" w ramach trybu dopuszczania rozwiązań informatycznych do przetwarzania informacji niejawnych, przepisy § 15–20 stosuje się odpowiednio.

2. Aktualizacja dokumentu, o którym mowa w ust. 1, może odbywać się w formie aneksu.

§ 24. Rozporządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

Minister Obrony Narodowej: z up. *M. Wiśniewski*