BIP - Agencja Bezpieczeństwa Wewnętrznego

Aby informacje niejawne mogły być prawidłowo przetwarzane należy stosować środki bezpieczeństwa fizycznego odpowiednie do poziomu zagrożeń w celu uniemożliwienia osobom nieuprawnionym dostępu do tych informacji lub ich utraty.

Informacje niejawne mogą być przetwarzane w strefach ochronnych, do których wstęp powinny mieć tylko uprawnione osoby.

W jednostkach organizacyjnych, w których przetwarzane są informacje niejawne o klauzuli „tajne" lub „ściśle tajne" tworzy się kancelarie tajne.

Szczegółowe informacje na ten temat zawarto w odpowiedziach na następujące pytania:

Co to jest kancelaria tajna i czym się zajmuje?

Zgodnie z art. 42 ust. 4 ustawy kancelaria tajna to wyodrębniona komórka organizacyjna, w zakresie ochrony informacji niejawnych podległa pełnomocnikowi ochrony, obsługiwana przez pracowników pionu ochrony, odpowiedzialna za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów uprawnionym osobom.

Zgodnie z art. 43 ust. 1 ustawy organizacja pracy kancelarii tajnej zapewnia możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał o klauzuli "tajne" lub "ściśle tajne" pozostający w dyspozycji jednostki organizacyjnej oraz kto z tym materiałem się zapoznał.

⏶

Jakie informacje niejawne są przetwarzane w kancelariach tajnych?

Zgodnie z art. 2 pkt 5 ustawy przetwarzaniem informacji niejawnych są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie.

Zgodnie z art. 42 ust. 1 ustawy obowiązek utworzenia kancelarii tajnej, spoczywa jedynie na kierownikach jednostek organizacyjnych, w których są lub będą przetwarzane informacje niejawne oznaczone klauzulami „tajne” bądź „ściśle tajne”.

Zgodnie jednak z art. 42 ust. 5 ustawy kierownik jednostki organizacyjnej może wyrazić zgodę na przetwarzanie w kancelarii tajnej informacji niejawnych o klauzuli „poufne” lub „zastrzeżone”.

⏶

Czy kierownik jednostki organizacyjnej może nazwać komórkę organizacyjną odpowiedzialną za przetwarzanie informacji niejawnych o klauzuli tajności POUFNE - Kancelarią tajną? Czy też nazwa „Kancelaria tajna” jest zastrzeżona do stosowania jedynie dla komórek określonych w art. 42 ust. 1 ustawy?

W jednostce, w której przetwarzane są tylko i wyłącznie informacje niejawne o klauzuli

„zastrzeżone” i „poufne” nie powinna funkcjonować komórka organizacyjna pod nazwą kancelaria tajna. W rozumieniu ustawy kancelaria tajna funkcjonuje w jednostkach przetwarzających informacje „ściśle tajne” lub „tajne”. Niezasadne określenie mianem kancelarii tajnej w/w komórki organizacyjnej mogłoby zatem spowodować problemy praktyczne, skutkujące przesyłaniem informacji niejawnych o klauzuli „tajne” lub „ściśle tajne” do jednostki organizacyjnej, która nie ma możliwości przetwarzania informacji o klauzuli wyższej niż „poufne”. Należy także mieć na względzie, że w art. 43 ust. 2, 3 i 6 ustawodawca posłużył się różnymi terminami komórek organizacyjnych dla obsługi dokumentów „ściśle tajnych” i „tajnych” (w tym przypadku jest to „kancelaria tajna”) oraz „poufnych” (mówi się o „innej niż kancelaria tajna komórce”).

Czy w kancelariach tajnych można przetwarzać informacje niejawne o klauzuli „poufne” lub „zastrzeżone”?

Zgodnie z art. 42 ust. 5 ustawy kierownik jednostki organizacyjnej może wyrazić zgodę na przetwarzanie w kancelarii tajnej informacji niejawnych o klauzuli „poufne” lub „zastrzeżone”.

Zgodnie z art. 43 ust. 2 i art. 44 ustawy, jeżeli jednostka organizacyjna przetwarza lub będzie przetwarzała materiały niejawne oznaczone maksymalnie klauzulą „poufne”, to funkcję kancelarii tajnej może spełniać inna komórka organizacyjna, pod warunkiem, że jej organizacja zapewni możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał niejawny pozostający w dyspozycji jednostki organizacyjnej.

O sposobie i trybie przetwarzania informacji niejawnych w podległej jednostce (jednostkach) zadecyduje kierownik jednostki organizacyjnej, zatwierdzając sporządzone przez pełnomocnika ochrony stosowne procedury wynikające z art. 43 ust. 3 ustawy.

Kiedy należy utworzyć kancelarię tajną?

Zgodnie z art. 2 pkt 5 ustawy przetwarzaniem informacji niejawnych są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie.

Zgodnie z art. 42 ust. 1 ustawy obowiązek utworzenia kancelarii tajnej, spoczywa jedynie na kierownikach jednostek organizacyjnych, w których są lub będą przetwarzane informacje niejawne oznaczone klauzulami „tajne” bądź „ściśle tajne”.

Zgodnie jednak z art. 42 ust. 5 ustawy kierownik jednostki organizacyjnej może wyrazić zgodę na przetwarzanie w kancelarii tajnej informacji niejawnych o klauzuli „poufne” lub „zastrzeżone”.

Czy kierownik jednostki organizacyjnej może utworzyć więcej niż jedną kancelarię tajną?

Zgodnie z art. 42 ust. 2 ustawy w przypadku uzasadnionym względami organizacyjnymi kierownik jednostki organizacyjnej może utworzyć więcej niż jedną kancelarię tajną.

Czy jedna kancelaria tajna może obsługiwać więcej niż jedną jednostkę organizacyjną?

Zgodnie z art. 42 ust. 3 ustawy w uzasadnionych przypadkach istnieje możliwość utworzenia kancelarii tajnej obsługującej więcej niż jedną jednostkę organizacyjną.

Warunkami skorzystania z takiego rozwiązania będzie:

- porozumienie zainteresowanych kierowników jednostek organizacyjnych w zakresie zasad funkcjonowania wspólnej kancelarii;
- uzyskanie zgody ABW lub SKW - zgoda taka będzie uzależniona od oceny poziomu skuteczności zastosowanych rozwiązań organizacyjnych i środków ochrony.

Porozumienie kierowników jednostek organizacyjnych, dotyczące organizacji kancelarii tajnej obsługującej kilka jednostek organizacyjnych, nie dotyczy udostępniania systemu teleinformatycznego organizowanego przez kierownika jednostki organizacyjnej osobom z innej jednostki organizacyjnej. Możliwość udostępniania systemu TI organizowanego przez kierownika jednostki organizacyjnej osobom z innej jednostki organizacyjnej wymaga odpowiedniego opracowania/aktualizacji dokumentacji bezpieczeństwa danego systemu TI oraz jej zatwierdzenia w ramach procesu akredytacji, o której mowa w art. 48 ustawy.

⏶

Jak wygląda procedura wyrażenia zgody przez ABW na utworzenie kancelarii tajnej obsługującej dwie lub więcej jednostek organizacyjnych?

W przypadku występowania okoliczności, o których mowa w art. 42 ust. 3 ustawy obowiązuje następujący tryb postępowania:

1. Przesłanie do ABW wniosku w przedmiotowej sprawie wraz z uzasadnieniem oraz podaniem nazw i adresów zainteresowanych podmiotów.
2. Do wniosku należy dołączyć podpisane porozumienie zainteresowanych kierowników jednostek organizacyjnych, zawierające rozwiązania w zakresie organizacji i funkcjonowania wspólnej kancelarii tajnej oraz nadzoru i odpowiedzialności kierowników jednostek organizacyjnych i pełnomocników ochrony.
3. Biorąc pod uwagę lokalizację wspólnej kancelarii tajnej, wniosek wraz z zawartym porozumieniem, należy przesłać odpowiednio do Departamentu Ochrony Informacji Niejawnych ABW lub do właściwej terytorialnie delegatury ABW.
4. Stanowisko ABW w postaci udzielenia lub nieudzielenia zgody w przedmiotowej sprawie zostanie przekazane wszystkim zainteresowanym kierownikom jednostek organizacyjnych.

W celu ograniczenia prowadzenia korespondencji, jednostki występujące o wydanie zgody na utworzenie wspólnej kancelarii tajnej powinny przekazać do ABW jeden egzemplarz wniosku i porozumienia.

Wzór porozumienia w sprawie utworzenia kancelarii tajnej krajowej

Wzór porozumienia w sprawie utworzenia kancelarii tajnej krajowej oraz kancelarii tajnej międzynarodowej

⏶

Kto powołuje kierowników oddziałów kancelarii tajnych?

Zgodnie z § 2 ust. 1 pkt 3b rozporządzenia Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. z 2017. poz. 1558) oddziałem kancelarii tajnej kieruje osoba wyznaczona przez pełnomocnika ochrony spośród pracowników pionu ochrony.

Czy kierownik kancelarii tajnej może być pełnomocnikiem ochrony?

Zgodnie z art. 42 ust. 4 ustawy kancelaria tajna podlega pełnomocnikowi ochrony. Kierujący kancelarią kierownik podlega zatem bezpośrednio pełnomocnikowi ochrony i ta podległość służbowa uniemożliwia jednoczesne bycie pełnomocnikiem ochrony i kierownikiem kancelarii tajnej.

Czy i kogo trzeba informować o utworzeniu lub likwidacji kancelarii tajnej?

Zgodnie z art. 42 ust. 6 ustawy kierownik jednostki organizacyjnej informuje odpowiednio Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego o fakcie utworzenia lub likwidacji kancelarii tajnej, z określeniem klauzuli tajności przetwarzanych w niej informacji niejawnych.

Ten obowiązek informacyjny pozwoli na bieżące uaktualniane wykazu kancelarii tajnych funkcjonujących odpowiednio w tzw. sferze cywilnej lub wojskowej.

Gdzie powinny być przetwarzane informacje niejawne o klauzuli „poufne” lub „zastrzeżone”?

Zgodnie z art. 43 ust. 2 i art. 44 ustawy, jeśli jednostka organizacyjna przetwarza lub będzie przetwarzała materiały niejawne oznaczone maksymalnie klauzulą „poufne”, to funkcję kancelarii tajnej może spełniać inna komórka organizacyjna, pod warunkiem, że jej organizacja zapewni możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał niejawny pozostający w dyspozycji jednostki organizacyjnej.

Zgodnie z art. 43 ust. 3 ustawy o sposobie i trybie przetwarzania informacji niejawnych o klauzuli „poufne” w podległej jednostce (jednostkach) zadecyduje kierownik jednostki organizacyjnej, zatwierdzając sporządzone przez pełnomocnika ochrony stosowne procedury.

Zgodnie z art. 43 ust. 5 ustawy kierownik jednostki organizacyjnej zatwierdza, opracowaną przez pełnomocnika ochrony, instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego.

Co to jest pion ochrony?

Zgodnie z art. 15 ust. 2 ustawy pion ochrony to wyodrębniona i podlegająca pełnomocnikowi ochrony komórka organizacyjna do spraw ochrony informacji niejawnych. W pionie ochrony zatrudnieni są pracownicy pionu ochrony, którzy podlegają pełnomocnikowi ochrony.

Obowiązek powołania pionu ochrony i zatrudnienia pełnomocnika ochrony, który będzie nim kierował obowiązuje niezależnie od klauzuli przetwarzanych w jednostce organizacyjnej informacji niejawnych.

Co ważne, ustawa wprowadza wyjątki od obowiązku utworzenia pionu ochrony oraz powołania pełnomocnika ochrony:

- zgodnie z art. 54 ust. 3 i ust. 5 ustawy, w przypadku przedsiębiorcy prowadzącego działalność jednoosobowo i osobiście powołanie pełnomocnika ochrony oraz utworzenie pionu ochrony nie jest wymagane, z wyjątkiem ubiegania się o świadectwo potwierdzające zdolność do ochrony informacji niejawnych o klauzuli będącej zagranicznym odpowiednikiem klauzuli „tajne" lub „poufne", stosowanym przez organizacje międzynarodowe;
- zgodnie z art. 54 ust. 10 ustawy, w przypadku przedsiębiorcy zamierzającego wykonywać umowy związane z dostępem do informacji niejawnych o klauzuli „zastrzeżone", nie ma wymogu zatrudnienia pełnomocnika ochrony, ale nie ma wówczas możliwości przetwarzania informacji niejawnych w użytkowanych przez niego obiektach;
- zgodnie z art. 60 ust. 1 ustawy, w przypadku postępowania bezpieczeństwa przemysłowego trzeciego stopnia powołanie pełnomocnika ochrony oraz utworzenie pionu ochrony nie jest wymagane. W takiej sytuacji zwykłe postępowania sprawdzające oraz szkolenie pracowników przedsiębiorcy może przeprowadzić pełnomocnik ochrony jednostki zlecającej wykonanie umowy (art. 60 ust. 2). Powołanie pełnomocnika i utworzenie pionu ochrony jest jednak konieczne, jeśli przedsiębiorca ubiega się o wydanie świadectwa bezpieczeństwa przemysłowego III stopnia potwierdzającego zdolność do ochrony informacji niejawnych międzynarodowych o klauzulach będących odpowiednikami klauzul „poufne" lub „tajne".

W jaki sposób należy wyodrębnić pion ochrony w małych jednostkach organizacyjnych, żeby spełnione zostały wymogi art 15 ust 2 ustawy?

Wyodrębnienie komórki organizacyjnej w postaci pionu ochrony, wymagane expressis verbis przez art. 15 ust. 2 ustawy, powinno przybrać postać indywidualnej i konkretnej normy prawnej wynikającej z przepisu o charakterze organizacyjno-prawnym i zawartej w akcie prawa wewnętrznego jednostki - regulaminu organizacyjnego, zarządzenia, decyzji lub polecenia służbowego na piśmie. Norma zawarta w takim akcie prawnym powinna określać zakres działania, zadania, obowiązki, kompetencje i uprawnienia oraz podległość osób wchodzących w skład pionu ochrony. Co ważne wyodrębnienie w ten sposób pionu ochrony nie musi mieć w przypadku małych jednostek organizacyjnych charakteru strukturalnego, budżetowego czy finansowego. Nie musi mieć także charakteru kadrowego, ani etatowego. Nie wymaga ono (stworzenie normy wyodrębniającej komórkę organizacyjną w postaci pionu ochrony) żadnych dodatkowych nakładów finansowych, ani stworzenia nowej struktury w postaci wydziału, oddziału, samodzielnego referatu, sekcji czy wieloosobowego stanowiska pracy. Wystarczy, jeżeli wyodrębnienie to będzie miało charakter wyłącznie normatywny, prawny, oparty wyłącznie na kryteriach merytorycznych, umożliwiających skuteczne wydawanie poleceń służbowych, podejmowanie działań, wykonywanie zadań, realizowanie kompetencji pełnomocnika wobec pionu ochrony.

Zastosowanie takiego rozwiązania nie powoduje generowania dodatkowych zbędnych w

przypadku małych jednostek organizacyjnych kosztów związanych z powołaniem pionu ochrony jako odrębnej komórki organizacyjnej, co jest zgodne z założeniami i intencjami projektodawców ustawy.

Kto może być pracownikiem pionu ochrony?

Zgodnie z art. 16 ustawy pracownikiem pionu ochrony może być osoba, która posiada:

- obywatelstwo polskie, z wyjątkiem pracowników pionu ochrony zatrudnionych u przedsiębiorców;
- odpowiednie poświadczenie bezpieczeństwa lub upoważnienie do klauzuli „zastrzeżone”;
- zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych.

Jak należy zorganizować pion ochrony, jeżeli w jednostce przetwarzane są informacje niejawne o klauzuli „poufne”?

Zgodnie z art. 15 ust. 2 i art. 43 ust. 3 ustawy organizacja pionu ochrony w jednostkach organizacyjnych, w których przetwarzane są informacje niejawne o klauzuli „poufne” opiera się na zatwierdzonym przez kierownika jednostki organizacyjnej, a opracowanym przez pełnomocnika ochrony sposobie i trybie przetwarzania informacji niejawnych.

Zgodnie z art. 43 ust. 4 ustawy pełnomocnik ochrony jednostki organizacyjnej, w której przetwarzane są informacje niejawne o klauzuli „poufne” lub wyższej opracowuje także dokumentację określającą poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą. Dokumentacja ta podlega zatwierdzeniu przez kierownika jednostki organizacyjnej.

W skład pionu ochrony jednostek organizacyjnych, w których przetwarzane są informacje niejawne o klauzuli „poufne” mogą wchodzić następujące osoby:

- pełnomocnik ochrony oraz jego zastępcy;
- pracownicy piony ochrony;
- inspektor bezpieczeństwa teleinformatycznego.

Co ważne, ustawa wprowadza wyjątki od obowiązku utworzenia pionu ochrony oraz powołania pełnomocnika ochrony:

- zgodnie z art. 54 ust. 3 i ust. 5 ustawy, w przypadku przedsiębiorcy prowadzącego działalność jednoosobowo i osobiście powołanie pełnomocnika ochrony oraz utworzenie pionu ochrony nie jest wymagane, z wyjątkiem ubiegania się o świadectwo potwierdzające zdolność do ochrony informacji niejawnych o klauzuli będącej zagranicznym odpowiednikiem klauzuli „tajne” lub „poufne”, stosowanym przez organizacje międzynarodowe;
- zgodnie z art. 54 ust. 10 ustawy, w przypadku przedsiębiorcy zamierzającego wykonywać umowy związane z dostępem do informacji niejawnych o klauzuli „zastrzeżone”, nie ma wymogu zatrudnienia pełnomocnika ochrony, ale nie ma wówczas możliwości

przetwarzania informacji niejawnych w użytkowanych przez niego obiektach;

- zgodnie z art. 60 ust. 1 ustawy, w przypadku postępowania bezpieczeństwa przemysłowego trzeciego stopnia powołanie pełnomocnika ochrony oraz utworzenie pionu ochrony nie jest wymagane. W takiej sytuacji zwykłe postępowania sprawdzające oraz szkolenie pracowników przedsiębiorcy może przeprowadzić pełnomocnik ochrony jednostki zlecającej wykonanie umowy (art. 60 ust. 2). Powołanie pełnomocnika i utworzenie pionu ochrony jest jednak konieczne, jeśli przedsiębiorca ubiega się o wydanie świadectwa bezpieczeństwa przemysłowego III stopnia potwierdzającego zdolność do ochrony informacji niejawnych międzynarodowych o klauzulach będących odpowiednikami klauzul „poufne" lub „tajne".

Jak należy zorganizować pion ochrony, jeżeli w jednostce przetwarzane są tylko informacje niejawne o klauzuli „zastrzeżone"?

Zgodnie z art. 15 ust. 2 ustawy organizacja pionu ochrony w jednostkach organizacyjnych, w których przetwarzane są informacje niejawne o klauzuli „zastrzeżone", nie różni się zasadniczo od organizacji pionu ochrony jednostek, w których przetwarzane są informacje „poufne".

Różnice dotyczą jedynie zadań pełnomocników ochrony w obu jednostkach.

Zgodnie z art. 43 ust. 5 ustawy w przypadku przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone" pełnomocnik ochrony zobowiązany jest do sporządzenia instrukcji dotyczącej sposobu i trybu przetwarzania tych informacji oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony.

W skład pionu ochrony jednostek organizacyjnych, w których przetwarzane są informacje niejawne o klauzuli „zastrzeżone" mogą wchodzić następujące osoby:

- pełnomocnik ochrony oraz jego zastępcy;
- pracownicy piony ochrony;
- inspektor bezpieczeństwa teleinformatycznego.

Co ważne, ustawa wprowadza wyjątki od obowiązku utworzenia pionu ochrony oraz powołania pełnomocnika ochrony:

- zgodnie z art. 54 ust. 3 i ust. 5 ustawy, w przypadku przedsiębiorcy prowadzącego działalność jednoosobowo i osobiście powołanie pełnomocnika ochrony oraz utworzenie pionu ochrony nie jest wymagane, z wyjątkiem ubiegania się o świadectwo potwierdzające zdolność do ochrony informacji niejawnych o klauzuli będącej zagranicznym odpowiednikiem klauzuli „tajne" lub „poufne", stosowanym przez organizacje międzynarodowe;
- zgodnie z art. 54 ust. 10 ustawy, w przypadku przedsiębiorcy zamierzającego wykonywać umowy związane z dostępem do informacji niejawnych o klauzuli „zastrzeżone", nie ma wymogu zatrudnienia pełnomocnika ochrony, ale nie ma wówczas możliwości przetwarzania informacji niejawnych w użytkowanych przez niego obiektach;
- zgodnie z art. 60 ust. 1 ustawy, w przypadku postępowania bezpieczeństwa przemysłowego trzeciego stopnia powołanie pełnomocnika ochrony oraz utworzenie pionu ochrony nie jest wymagane. W takiej sytuacji zwykłe postępowania sprawdzające oraz

szkolenie pracowników przedsiębiorcy może przeprowadzić pełnomocnik ochrony jednostki zlecającej wykonanie umowy (art. 60 ust. 2). Powołanie pełnomocnika i utworzenie pionu ochrony jest jednak konieczne, jeśli przedsiębiorca ubiega się o wydanie świadectwa bezpieczeństwa przemysłowego III stopnia potwierdzającego zdolność do ochrony informacji niejawnych międzynarodowych o klauzulach będących odpowiednikami klauzul „poufne" lub „tajne".

Co to jest strefa ochronna?

Zgodnie z art. 46 pkt 1 ustawy w celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych o klauzuli „poufne" lub wyższej należy w szczególności zorganizować strefy ochronne.

W opinii Agencji Bezpieczeństwa Wewnętrznego, strefa ochronna to obszar np.: wydzielona części budynku lub cały budynek, a także pomieszczenie wyposażone lub zabezpieczone w odpowiednie środki bezpieczeństwa fizycznego, w którym można przetwarzać informacje niejawne.

Pojęcie „strefa ochronna" zastępuje dotychczasowe pojęcia „strefa administracyjna", „strefa bezpieczeństwa" i „specjalna strefa bezpieczeństwa". Zadania, które spełniały wymienione strefy zostały przejęte przez strefy ochronne, zabezpieczone w środki bezpieczeństwa fizycznego adekwatne do klauzuli przetwarzanych informacji niejawnych oraz poziomu zagrożeń nieuprawnionego ich ujawnienia lub utraty.

Do dnia 2 stycznia 2011 r. obowiązek zabezpieczenia informacji niejawnych oznaczonych klauzulą „poufne" lub wyższą był realizowany przez zorganizowanie pomieszczenia kancelarii tajnej wyposażonego w odpowiednie środki ochrony fizycznej. Obecnie to strefy ochronne zorganizowane w sposób uwzględniający klauzulę tajności przetwarzanych dokumentów, jak i poziom zagrożenia, będąc wyposażonymi w środki bezpieczeństwa fizycznego mają za zadanie zapewnić ochronę materiałów niejawnych. Natomiast zadaniem kancelarii tajnej – jako komórki organizacyjnej – jest przede wszystkim dbanie o rejestrację i obieg dokumentów.

Gdzie można odbywać posiedzenia niejawne?

Stosownie do przepisów § 5 ust. 1 rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych, informacje niejawne o klauzuli ,,poufne" lub wyższej są przetwarzane w strefie ochronnej I lub II. W związku z przyjętą w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych definicją ,,przetwarzania informacji niejawnych", zawierającą w sobie dokonywanie wszelkich operacji w odniesieniu do informacji niejawnych, we wskazanych strefach ochronnych, tj. w I lub w II, można przeprowadzać rozmowy o charakterze niejawnym (w tym posiedzenia niejawne). Strefy takie muszą zostać zorganizowane w sposób wskazany w cytowanym przepisie rozporządzenia. Wśród kryteriów tworzenia przedmiotowych stref nie ma obowiązku zabezpieczenia tych stref przed podsłuchem.

Jeżeli natomiast kierownik jednostki organizacyjnej, w której odbywać się będą posiedzenia niejawne uzna, że informacje niejawne przetwarzane w trakcie takiego posiedzenia powinny być dodatkowo chronione przed podsłuchem, powinien wówczas zorganizować specjalną strefę ochronną stosownie do dyspozycji przepisu § 5 ust. 1 pkt 4 wspomnianego rozporządzenia. Taka

strefa, poza wymogami wynikającymi z cyt. rozporządzenia, powinna być wyposażona w stałe elementy techniczne uniemożliwiające podsłuch.

Ponadto przepisy rozporządzenia w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych w treści § 5 ust. 4, dają możliwość utworzenia ,,tymczasowej strefy ochronnej" (I, II lub specjalnej) w celu odbycia posiedzenia niejawnego. W związku z brakiem określenia w przywołanym przepisie prawa wymogów co do utworzenia przedmiotowych stref należy stosować kryteria tworzenia poszczególnych stref, które wskazane zostały we właściwych przepisach rozporządzenia. Jedynie w przypadku utworzenia tymczasowo specjalnej strefy ochronnej w związku z § 5 ust. l pkt 4 cyt. rozporządzenia obligatoryjnie będzie wymagana ochrona takiej strefy przed podsłuchem. Przepisy bowiem § 5 ust. 1 pkt l i pkt 2 odnoszące się do kryteriów tworzenia, odpowiednio strefy ochronnej I i II nie określają wymogu ochrony takich stref przed podsłuchem.

W przypadku posiedzeń niejawnych obejmujących w swoim przedmiocie informacje o klauzuli „zastrzeżone" nie ma obowiązku organizowania ich w strefach ochronnych. Zgodnie bowiem z art. 46 cyt. ustawy obowiązek zorganizowania stref ochronnych dotyczy wyłącznie informacji niejawnych o klauzuli „poufne" lub wyższej. W takim przypadku należy stosować przepisy § 7 ust. 4 cyt. rozporządzenia wskazującego wymogi przetwarzania informacji o klauzuli „zastrzeżone".

Poniżej zamieszczono treść zarządzenia Szefa ABW ws. zasad wykonywania przez ABW badań antypodsłuchowych oraz wzór wniosku o przeprowadzenie takich badań w ramach ochrony informacji niejawnych.

Zarządzenie nr 21 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 19 kwietnia 2016 r. w sprawie wykonywanie badań antypodsłuchowych przez Agencję Bezpieczeństwa Wewnętrznego.

Zarządzenie nr 115 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 16 października 2018 r. zmieniające zarządzenie w sprawie wykonywanie badań antypodsłuchowych przez Agencję Bezpieczeństwa Wewnętrznego.

Zarządzenie nr 45 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 13 czerwca 2024 r. zmieniające zarządzenie w sprawie wykonywanie badań antypodsłuchowych przez Agencję Bezpieczeństwa Wewnętrznego.

Wniosek o przeprowadzenie badań antypodsłuchowych w ramach ochrony informacji niejawnych

Czym są środki bezpieczeństwa fizycznego?

W opinii Agencji Bezpieczeństwa Wewnętrznego bezpieczeństwo fizyczne informacji niejawnych to system powiązanych ze sobą przedsięwzięć organizacyjnych, osobowych, technicznych i fizycznych służących ochronie tych informacji przed nieuprawnionym dostępem lub utratą. Kompleksowe podejście do bezpieczeństwa fizycznego informacji niejawnych wymaga wzajemnego uzupełniania się przyjętych rozwiązań. Na elementy składowe systemu służącego ochronie informacji niejawnych w szczególności składają się:

- działania organizacyjne – opracowanie planów, instrukcji, regulaminów i procedur;
- ochrona osobowa (ochrona czynna) - zorganizowanie wewnętrznej służby ochrony lub skorzystanie z usług koncesjonowanej agencji ochrony;

- ochrona bierna – wydzielenie, zorganizowanie i wdrożenie zabezpieczeń architektoniczno-budowlanych w postaci: ogrodzeń, zapór, bram, przegród, a w szczególności ścian i stropów stref chronionych, przed nieuprawnionym wtargnięciem;
- strefy ochronne - wyznaczenie, zorganizowanie i zabezpieczenie obszarów podlegających kontroli wejścia, wyjścia oraz kontroli przebywania (obustronna kontrola dostępu);
- elektroniczne – zabezpieczenie i nadzór nad odpowiednimi strefami ochronnymi przy wykorzystaniu systemów włamania i napadu, systemów kontroli dostępu, systemów telewizji dozorowej CCTV, systemów sygnalizacji pożaru, systemów zasilania awaryjnego i innych zintegrowanych elektronicznych systemów bezpieczeństwa;
- mechaniczne – zastosowanie do zabezpieczenia odpowiednich stref ochronnych technicznych środków ochrony w postaci: tripodów, śluz, bramek magnetycznych, certyfikowanych: drzwi, krat, żaluzji, zamków, kłódek, szaf matalowych.

Co to znaczy wyposażenie i urządzenia, którym przyznano certyfikaty?

Zgodnie z art. 46 pkt 4 ustawy jednostki organizacyjne dysponujące informacjami niejawnymi o klauzuli „poufne” lub wyższej są zobligowane do stosowania wyposażenia i urządzeń, którym na podstawie odrębnych przepisów przyznano certyfikaty.

W opinii Agencji Bezpieczeństwa Wewnętrznego pojęcia „urządzenia” lub „wyposażenie” oznaczają m.in. szafy metalowe służące do przechowywania materiałów niejawnych lub systemy alarmowe oraz dozorowe służące do ochrony informacji, a także systemy teleinformatyczne służące do przetwarzania informacji niejawnych.

Certyfikacje wyrobów służących ochronie informacji niejawnych przeprowadzają jednostki posiadające akredytację Polskiego Centrum Akredytacji. Urządzenia wyprodukowane, zakupione i zamontowane w okresie ważności certyfikatu zachowują ważność przez cały okres eksploatacji. Urządzenie traci certyfikat w przypadku dokonania zmian konstrukcyjnych lub w przypadku zmiany przepisów. Wyroby, na które wydano certyfikat zgodności, podlegają oznakowaniu potwierdzającemu zgodność wyrobu z zasadniczymi wymaganiami.

Zgodnie z art. 50 ustawy Departament Bezpieczeństwa Teleinformatycznego ABW w ramach realizacji zadań w zakresie bezpieczeństwa systemów teleinformatycznych przeprowadza certyfikacje środków (wyrobów) w zakresie:

- ochrony elektromagnetycznej;
- ochrony kryptograficznej.

Certyfikacja środków ochrony bezpieczeństwa teleinformatycznego prowadzona jest według polskich i europejskich norm i kryteriów oceny. Wyroby spełniające określone wymagania mogą uzyskać:

- certyfikat ochrony elektromagnetycznej;
- certyfikat ochrony kryptograficznej.

Certyfikat ochrony potwierdza, że wyrób spełnia określone odpowiednią normą wymagania i może być wykorzystywany do ochrony informacji niejawnych przetwarzanych w systemach teleinformatycznych.

Jak określać poziom zagrożeń?

Zgodnie z art. 45 ustawy jednostki organizacyjne, w których są przetwarzane informacje niejawne, stosują środki bezpieczeństwa fizycznego odpowiednie do poziomu zagrożeń w celu uniemożliwienia osobom nieuprawnionym dostępu do takich informacji.

W opinii Agencji Bezpieczeństwa Wewnętrznego przez poziom zagrożenia nieuprawnionego ujawnienia lub utraty informacji niejawnych, należy rozumieć wpływ szeregu czynników, mogących mieć istotne znaczenie dla bezpieczeństwa przetwarzanych w jednostce organizacyjnej informacji niejawnych. Określając poziom zagrożeń w szczególności należy uwzględnić:

- klauzulę tajności i liczbę dokumentów niejawnych pozostających w dyspozycji jednostki organizacyjnej;
- lokalizację pomieszczeń, w których będą przetwarzane informacje niejawne;
- liczbę osób mających dostęp do informacji niejawnych w danej jednostce organizacyjnej;
- działanie sił natury.

Określenie poziomu zagrożenia w połączeniu z klauzulami przetwarzanych informacji niejawnych wskazują klasę strefy ochronnej, w której mogą być przetwarzane informacje niejawne oraz środki bezpieczeństwa fizycznego niezbędne do zabezpieczenia tej strefy.

Zgodnie z art. 45 ust. 3 ustawy w uzasadnionych przypadkach przy określaniu poziomu zagrożeń uwzględnia się wskazania ABW lub SKW.

Szczegółowy sposób określania poziomu zagrożeń oraz doboru środków bezpieczeństwa fizycznego reguluje rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz.U. z 2012 r. poz. 683).

Metadane

Data publikacji : 27.12.2010
Data modyfikacji : 05.11.2024
Rejestr zmian

Podmiot udostępniający informację:
Agencja Bezpieczeństwa Wewnętrznego

Osoba wytwarzająca/odpowiadająca za informację:
Administrator BIP

Osoba udostępniająca informację:
Administrator BIP

Osoba modyfikująca informację:
Administrator BIP