ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO

Środki bezpieczeństwa fizycznego (1/7)

Jednostki organizacyjne, w których przetwarzane są informacje niejawne, stosują **środki bezpieczeństwa fizycznego** odpowiednie do poziomu zagrożeń w celu uniemożliwienia osobom nieuprawnionym dostępu do takich informacji, w szczególności chroniące przed:

1) działaniem obcych służb specjalnych;
2) zamachem terrorystycznym lub sabotażem;
3) kradzieżą lub zniszczeniem materiału;
4) próbą wejścia osób nieuprawnionych do pomieszczeń, w których przetwarzane są informacje niejawne;
5) nieuprawnionym dostępem do informacji o wyższej klauzuli tajności niewynikającym z posiadanych uprawnień.

Środki bezpieczeństwa fizycznego (2/7)

Zakres stosowania środków bezpieczeństwa fizycznego uzależnia się od **poziomu zagrożeń** związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą (w rozporządzeniu przyjęto określenie *„poziom zagrożeń związanych z utratą poufności, integralności lub dostępności informacji niejawnych).*

Środki bezpieczeństwa fizycznego stosuje się we wszystkich **pomieszczeniach i obszarach**, w których są przetwarzane informacje niejawne (wyjątek: przetwarzanie informacji niejawnych w części mobilnej zasobów systemu TI).

Środki bezpieczeństwa fizycznego (3/7)

System środków bezpieczeństwa fizycznego obejmuje stosowanie rozwiązań organizacyjnych, wyposażenia i urządzeń służących ochronie informacji niejawnych oraz elektronicznych systemów pomocniczych wspomagających ochronę informacji niejawnych.

W zależności od poziomu zagrożeń stosuje się odpowiednią kombinację następujących środków bezpieczeństwa fizycznego:

Środki bezpieczeństwa fizycznego (4/7)

1) **personel bezpieczeństwa** – osoby przeszkolone, nadzorowane, a w razie konieczności posiadające odpowiednie uprawnienie do dostępu do informacji niejawnych, wykonujące czynności związane z fizyczną ochroną informacji niejawnych, w tym kontrolę dostępu do pomieszczeń lub obszarów, w których przetwarzane są informacje niejawne, nadzór nad systemem dozoru wizyjnego, a także reagowanie na alarmy lub sygnały awaryjne;

2) **bariery fizyczne** – środki chroniące granice miejsca, w którym przetwarzane są informacje niejawne, w szczególności ogrodzenia, ściany, bramy, drzwi i okna;

Środki bezpieczeństwa fizycznego (5/7)

3) **szafy i zamki** – stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem;

4) **system kontroli dostępu** – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne, stosowany w celu zagwarantowania uzyskiwania dostępu do pomieszczenia lub obszaru, w którym przetwarzane są informacje niejawne, wyłącznie przez osoby posiadające odpowiednie uprawnienia;

Środki bezpieczeństwa fizycznego (6/7)

5) **system sygnalizacji włamania i napadu** – elektroniczny system pomocniczy stosowany w celu realizacji procedur ochrony informacji niejawnych oraz podwyższenia poziomu bezpieczeństwa, który dają bariery fizyczne, a w pomieszczeniach i budynkach zastępujący lub wspierający personel bezpieczeństwa;

6) **system dozoru wizyjnego** – elektroniczny system pomocniczy stosowany w celu bieżącego monitorowania ochronnego lub sprawdzania incydentów bezpieczeństwa i sygnałów alarmowych przez personel bezpieczeństwa;

Środki bezpieczeństwa fizycznego (7/7)

7) **system kontroli osób i przedmiotów** – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne polegające na zwracaniu się o dobrowolne poddanie się kontroli lub udostępnienie do kontroli rzeczy osobistych, a także przedmiotów wnoszonych lub wynoszonych – stosowany w celu zapobiegania próbom nieuprawnionego wnoszenia na chroniony obszar rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego wynoszenia informacji niejawnych z budynków lub obiektów.

Strefy ochronne (1/8)

W celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych o klauzuli **„poufne” lub wyższej** należy w szczególności:

1) zorganizować strefy ochronne;
2) wprowadzić system kontroli wejść i wyjść ze stref ochronnych;
3) określić uprawnienia do przebywania w strefach ochronnych;
4) stosować wyposażenie i urządzenia służące ochronie informacji niejawnych, którym przyznano certyfikaty.

Strefy ochronne (2/8)

Tworzy się następujące strefy ochronne:

1) **strefę ochronną I** – obejmującą pomieszczenie lub obszar, w których informacje niejawne o klauzuli „poufne” lub wyższej są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru umożliwia uzyskanie bezpośredniego dostępu do tych informacji.

Pomieszczenie lub obszar spełniają następujące wymagania:

a) wyraźnie wskazana w planie ochrony najwyższa klauzula tajności przetwarzanych informacji niejawnych;

b) wyraźnie określone i zabezpieczone granice;

Strefy ochronne (3/8)

c) wprowadzony system kontroli dostępu zezwalający na wstęp osób, które posiadają odpowiednie uprawnienie do dostępu do informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby albo wykonywania czynności zleconych;

d) w przypadku konieczności wstępu osób innych niż te, o których mowa w lit. c, przetwarzane informacje niejawne zabezpiecza się przed możliwością dostępu do nich tych innych osób oraz zapewnia się nadzór osoby uprawnionej lub równoważne mechanizmy kontrolne;

e) wstęp możliwy jest wyłącznie ze strefy ochronnej.

Strefy ochronne (4/8)

2) **strefę ochronną II** – obejmującą pomieszczenie lub obszar, w którym informacje niejawne o klauzuli „poufne” lub wyższej są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru nie umożliwia uzyskania bezpośredniego dostępu do tych informacji.

Pomieszczenie lub obszar spełniają następujące wymagania:

a) wyraźnie określone i zabezpieczone granice;

Strefy ochronne (5/8)

b) wprowadzony system kontroli dostępu zezwalający na wstęp osób, które posiadają odpowiednie uprawnienie do dostępu do informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby albo wykonywania czynności zleconych;

c) w przypadku konieczności wstępu osób innych, niż te, o których mowa powyżej, przetwarzane informacje niejawne zabezpiecza się przed możliwością dostępu do nich tych osób oraz zapewnia się nadzór osoby uprawnionej lub równoważne mechanizmy kontrolne;

d) wstęp możliwy jest wyłącznie ze strefy ochronnej.

Strefy ochronne (6/8)

3) **strefę ochronną III** – obejmującą pomieszczenie lub obszar wymagający wyraźnego określenia granic, w obrębie których jest możliwe kontrolowanie osób i pojazdów;

4) **specjalną strefę ochronną** – umiejscowioną w obrębie strefy ochronnej I lub strefy ochronnej II, chronioną przed podsłuchem, spełniającą dodatkowo następujące wymagania:

   a) strefę wyposaża się w system sygnalizacji włamania i napadu;

   b) strefa pozostaje zamknięta, gdy nikogo w niej nie ma;

Strefy ochronne (7/8)

c) w przypadku posiedzenia niejawnego strefa jest chroniona przed wstępem osób nieupoważnionych do udziału w tym posiedzeniu;

d) strefa podlega regularnym inspekcjom przeprowadzanym według zaleceń ABW albo SKW, nie rzadziej niż raz w roku oraz po każdym nieuprawnionym wejściu do strefy lub podejrzeniu, że takie wejście mogło mieć miejsce;

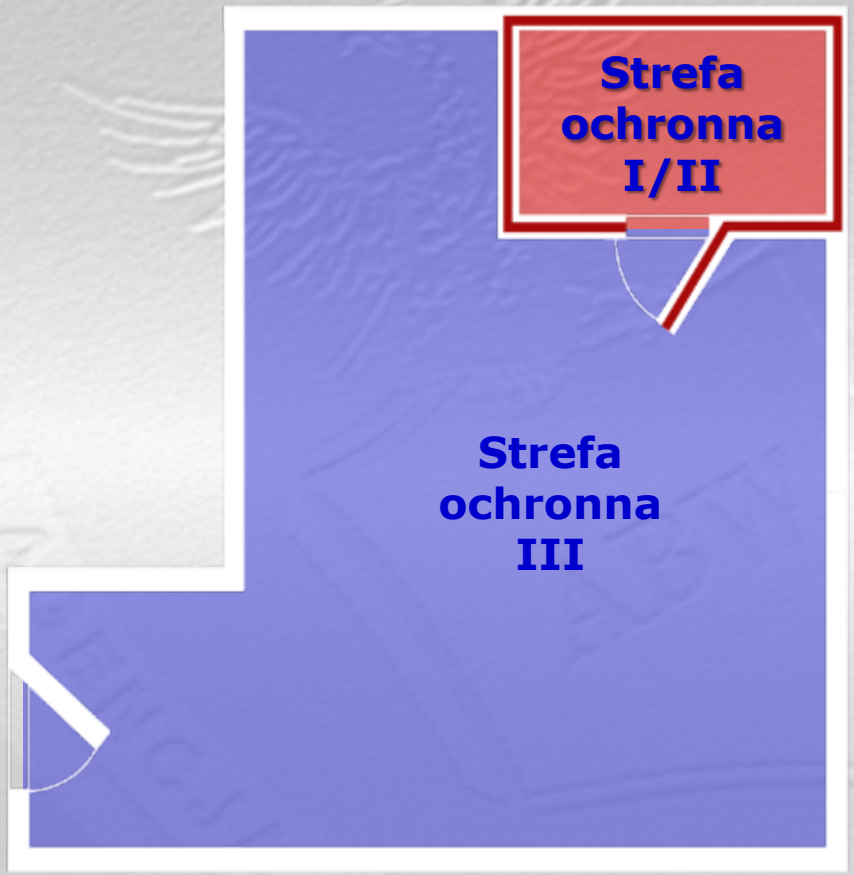
e) w strefie nie mogą znajdować się linie komunikacyjne, telefony, inne urządzenia komunikacyjne ani sprzęt elektryczny lub elektroniczny, których umieszczenie nie zostało zaakceptowane w sposób określony w procedurach bezpieczeństwa.

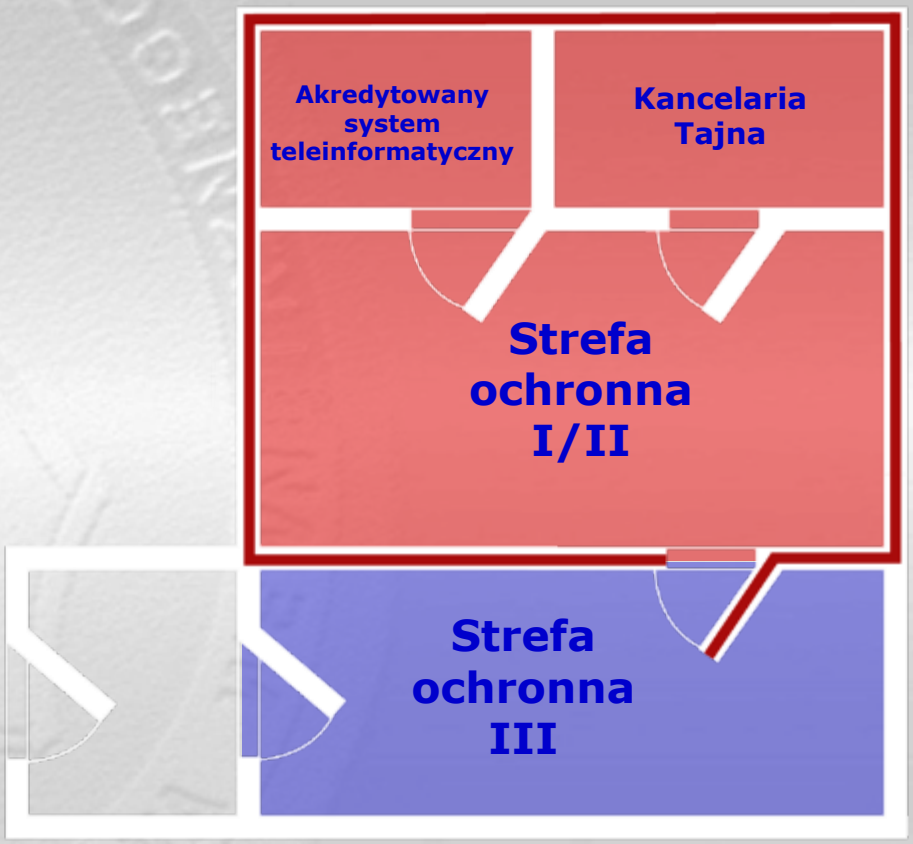
Strefy ochronne (8/8)

W strefie ochronnej I lub w strefie ochronnej II można utworzyć **pomieszczenie wzmocnione**. Konstrukcja pomieszczenia powinna zapewniać ochronę równoważną ochronie zapewnianej przez odpowiednie szafy przeznaczone do przechowywania informacji niejawnych o tej samej klauzuli tajności. W pomieszczeniu wzmocnionym dopuszczalne jest przechowywanie informacji niejawnych **poza odpowiednimi szafami**.

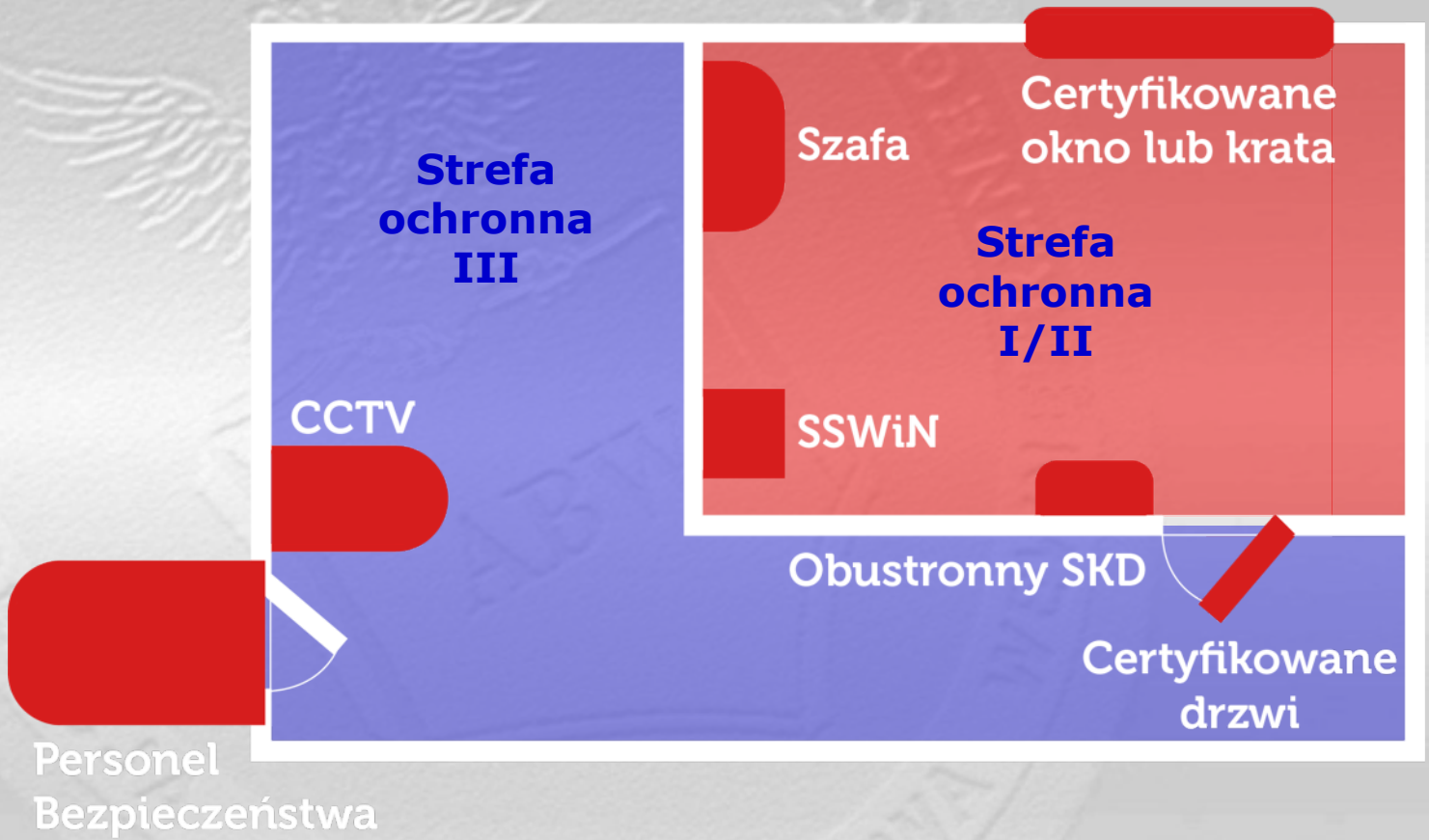
Strefę ochronną I, strefę ochronną II lub specjalną strefę ochronną można utworzyć **tymczasowo w strefie ochronnej III w celu odbycia posiedzenia niejawnego**.

Strefy ochronne – przykłady





Strefy ochronne – przykłady



Akty wykonawcze regulujące kwestię środków bezpieczeństwa fizycznego

Kryteria tworzenia stref ochronnych oraz rodzaje (katalog) środków bezpieczeństwa fizycznego wymienionych w rozporządzeniu Rady Ministrów z dnia 29 maja 2012 roku w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych **obowiązują wszystkie jednostki organizacyjne niezależnie od statusu.**

Zakres i dobór odpowiednich środków nie obowiązują jednostek organizacyjnych, do których zastosowanie mają przepisy właściwych zarządzeń wydanych w trybie art. 47 ust. 3 ustawy.

Przetwarzanie informacji niejawnych (1/4)

Informacje niejawne o klauzuli **„ściśle tajne” przetwarza się** w strefie ochronnej I lub w strefie ochronnej II i **przechowuje się** w szafie metalowej spełniającej co najmniej wymagania klasy odporności na włamanie S2, określone w Polskiej Normie PN-EN 14450 lub nowszej, lub w pomieszczeniu wzmocnionym, z zastosowaniem jednego z poniższych środków uzupełniających:

1) **stała ochrona lub kontrola** w nieregularnych odstępach czasu przez pracownika personelu bezpieczeństwa posiadającego odpowiednie poświadczenie bezpieczeństwa, w szczególności z wykorzystaniem systemu dozoru wizyjnego z obowiązkową rejestracją w rozdzielczości nie mniejszej niż 400 linii telewizyjnych i przechowywaniem zarejestrowanego zapisu przez czas nie krótszy niż 30 dni;

2) **system sygnalizacji włamania i napadu** obsługiwany przez personel bezpieczeństwa z wykorzystaniem systemu dozoru wizyjnego, o którym mowa w pkt. 1.

Przetwarzanie informacji niejawnych (2/4)

Informacje niejawne o klauzuli **„tajne” przetwarza się** w strefie ochronnej I lub w strefie ochronnej II i **przechowuje się** w szafie metalowej spełniającej co najmniej wymagania klasy odporności na włamanie S1, określone w Polskiej Normie PN-EN 14450 lub nowszej, lub w pomieszczeniu wzmocnionym.

Przetwarzanie informacji niejawnych (3/4)

Informacje niejawne o klauzuli **„poufne”:**

1) **przetwarza się** w strefie ochronnej I, II lub III;

2) **przechowuje się** w strefie ochronnej I lub w strefie ochronnej II w szafie metalowej lub w pomieszczeniu wzmocnionym.

Informacje niejawne o klauzuli **„zastrzeżone” przetwarza się** w pomieszczeniu lub obszarze wyposażonych w system kontroli dostępu i **przechowuje się** w szafie metalowej, pomieszczeniu wzmocnionym lub zamkniętym na klucz meblu biurowym.

Przetwarzanie informacji niejawnych (4/4)

Przetwarzanie informacji niejawnych o klauzuli **„poufne” lub wyższej w systemach teleinformatycznych** odbywa się w strefie ochronnej I lub w strefie ochronnej II, w warunkach uwzględniających wyniki procesu szacowania ryzyka.

Przetwarzanie informacji niejawnych o klauzuli **„zastrzeżone” w systemach teleinformatycznych** odbywa się w pomieszczeniu lub obszarze wyposażonych w system kontroli dostępu, w warunkach uwzględniających wyniki procesu szacowania ryzyka.

Postępowanie w sytuacjach zagrożenia dla informacji niejawnych (1/4)

Postępowanie w sytuacjach zagrożenia dla informacji niejawnych powinno mieć na celu **zapobieżenie naruszeniu przepisów o ochronie tych informacji**, w tym w szczególności zapobieżenie ujawnieniu, utracie lub ich zniszczeniu.

Rodzaj i skala zagrożeń związanych z nieuprawnionym dostępem lub utratą informacji niejawnych powinny zostać uwzględnione przy określaniu **poziomu zagrożeń** (art. 45 ustawy).

Postępowanie w sytuacjach zagrożenia dla informacji niejawnych (2/4)

Postępowanie w sytuacjach zagrożenia dla informacji niejawnych powinno mieć przede wszystkim charakter zapobiegawczy oraz polegać ma na przeciwdziałaniu zaistnienia sytuacji zagrożenia dla takich informacji.

Kierownik jednostki organizacyjnej powinien zatwierdzić, opracowaną przez pełnomocnika ochrony, procedurę postępowania w sytuacjach zagrożenia dla informacji niejawnych. Z przedmiotową procedurą powinni zostać zapoznani wszyscy pracownicy mający dostęp do informacji niejawnych.

Postępowanie w sytuacjach zagrożenia dla informacji niejawnych (3/4)

W przypadku **stwierdzenia naruszenia przepisów o ochronie informacji niejawnych** pełnomocnik ochrony powinien:

- ✓ niezwłocznie zawiadomić kierownika jednostki organizacyjnej;
- ✓ niezwłocznie podjąć działania wyjaśniające (niezbędne jest opracowanie szczegółowej instrukcji, wytycznych postępowania wyjaśniającego);
- ✓ podjąć działania ograniczające negatywne skutki naruszenia przepisów;
- ✓ niezwłocznie zawiadomić, w przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych o klauzuli „poufne” lub wyższej, również odpowiednio ABW lub SKW.

(art. 17 ustawy)

Postępowanie w sytuacjach zagrożenia dla informacji niejawnych (4/4)

O naruszeniu przepisów dotyczących ochrony informacji niejawnych należy **niezwłocznie powiadomić pełnomocnika ochrony.**

Postępowanie w przypadku ujawnienia informacji niejawnych

W przypadku stwierdzenia zaistnienia uzasadnionego podejrzenia popełnienia przestępstwa ujawnienia informacji niejawnych (art. 265 oraz art. 266 k.k.) istnieje obowiązek **niezwłocznego zawiadomienia właściwego organu ścigania** (prokuratura lub ABW).

(art. 304 k.p.k.)

Postępowanie w sytuacjach zagrożenia dla informacji niejawnych lub w przypadku ich ujawnienia

Procedura postępowania zarówno w sytuacjach zagrożenia dla informacji niejawnych jak i w przypadku naruszenia przepisów o ich ochronie (zwłaszcza ujawnieniu), powinna być opracowana dla konkretnej jednostki organizacyjnej w sposób zindywidualizowany.

Przedmiotowa procedura powinna mieć rangę aktu prawa wewnętrznego obowiązującego w danej jednostce organizacyjnej, np. w postaci załącznika do planu ochrony informacji niejawnych.

Podsumowanie

- Wymagane jest zorganizowanie co najmniej 2 stref ochronnych (wyjątek materiały „zastrzeżone”).
- Stosowanie środków bezpieczeństwa fizycznego odpowiednich do poziomu zagrożeń.
- Niezwłoczna reakcja na każde naruszenie przepisów o ochronie informacji niejawnych.