ZARZĄDZENIE Nr 24
PROKURATORA GENERALNEGO

z dnia 28 maja 2013 r.

w sprawie doboru i stosowania środków bezpieczeństwa fizycznego informacji niejawnych w powszechnych jednostkach organizacyjnych prokuratury

Na podstawie art. 47 ust. 3 ustawy z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* (Dz. U. z 2010 r. Nr 182 , poz.1228), zarządza się, co następuje:

Rozdział 1

Postanowienia ogólne

§ 1. Zarządzenie określa szczególny sposób doboru i stosowania środków bezpieczeństwa fizycznego informacji niejawnych w powszechnych jednostkach organizacyjnych prokuratury.

§ 2. Określenia użyte w zarządzeniu oznaczają:

1) ustawa - ustawę z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* (Dz. U. z 2010 r. Nr 182 , poz.1228);
2) rozporządzenie w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych – rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. *w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych* (Dz. U. Nr 115, poz. 683);
3) kancelaria - kancelarię tajną w Prokuraturze Generalnej lub w powszechnych jednostkach organizacyjnych prokuratury;
4) oddział kancelarii - oddział kancelarii tajnej w powszechnych jednostkach organizacyjnych prokuratury;
5) kierownik kancelarii - pracownika pionu ochrony, który organizuje i koordynuje pracę osób zatrudnionych w kancelarii, zgodnie z określonym zakresem zadań i obowiązków;
6) pracownik kancelarii - pracownika pionu ochrony zatrudnionego w kancelarii;
7) osoba upoważniona - osobę posiadającą odpowiednie poświadczenie bezpieczeństwa, upoważniające do dostępu do informacji niejawnych oznaczonych odpowiednią klauzulą tajności i przeszkoloną w zakresie ochrony informacji niejawnych oraz prokuratorów i asesorów prokuratorskich pełniących czynności prokuratorskie i inne osoby, których dostęp do informacji niejawnych regulują odrębne przepisy;
8) strefa ochronna - strefę, o której mowa w § 5 rozporządzenia w sprawie środków bezpieczeństwa fizycznego stosowanych *do* zabezpieczania informacji niejawnych;
9) system alarmowy — system spełniający wymagania Polskiej Normy;
10) pomieszczenie wzmocnione - pomieszczenie lub zespół pomieszczeń zlokalizowane w strefie ochronnej I lub w strefie ochronnej II, służące do ochrony informacji niejawnych przechowywanych w Prokuraturze Generalnej lub powszechnych jednostkach organizacyjnych prokuratury;
11) pomieszczenie wydzielone — pomieszczenie lub zespół pomieszczeń, w którym zainstalowano serwery sieciowe, terminale sieci teleinformatycznych, autonomiczne stanowiska komputerowe, a także ich elementy aktywne lub pasywne, w szczególności routery, switche, modemy, panele światłowodowe, służące do ochrony informacji niejawnych przetwarzanych w jednostce organizacyjnej;

12) pomieszczenie specjalne - pomieszczenie lub zespół pomieszczeń przeznaczone do prowadzenia narad, odpraw, konferencji, prezentacji multimedialnych oraz wideokonferencji, związanych z przetwarzaniem informacji o klauzulach „Tajne" i „ Ściśle tajne";
13) normy – normy, o których mowa w rozporządzeniu Rady Ministrów z dnia 29 maja 2012 r. *w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych* (Dz. U. Nr 115, poz. 683);
14) posterunek – wyznaczone miejsce, w którym pełni straż wyznaczona osoba, tj. personel bezpieczeństwa, strażnik.

Rozdział 2

Dobór środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń i zakres ich stosowania

§ 3. 1. W ramach systemu bezpieczeństwa fizycznego informacji niejawnych stosuje się środki bezpieczeństwa fizycznego zapewniające ochronę informacji niejawnych w strefach ochronnych.

2. W celu doboru adekwatnych środków bezpieczeństwa fizycznego określa się poziom zagrożeń związanych z utratą poufności, integralności lub dostępności informacji niejawnych, zwany dalej „poziomem zagrożeń".

3. Poziom zagrożeń określa się dla pomieszczenia lub obszaru, w którym przetwarzane są informacje niejawne.

4. Poziom zagrożeń określa się jako wysoki, średni albo niski.

5. W celu określenia poziomu zagrożeń przeprowadza się analizę, w której uwzględnia się wszystkie istotne czynniki mogące mieć wpływ na bezpieczeństwo informacji niejawnych, w szczególności:
1) klauzule tajności przetwarzanych informacji niejawnych;
2) postać i liczbę informacji niejawnych;
3) sposób przechowywania informacji niejawnych;
4) otoczenie i strukturę budynków lub stref, w których przetwarzane są informacje niejawne;
5) liczbę osób mających lub mogących mieć dostęp do informacji niejawnych, a także posiadane przez nich uprawnienia oraz uzasadnioną potrzebę dostępu do informacji niejawnych;
6) szacowane zagrożenie ze strony obcych służb specjalnych oraz zagrożenie sabotażem, zamachem terrorystycznym, kradzieżą lub inną działalnością przestępczą uzyskane od Policji i innych instytucji zgodnie z rozporządzeniem w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych.

§ 4. W zależności od poziomu zagrożeń określonego w wyniku przeprowadzenia analizy, pomieszczenia lub obszary, w których są przetwarzanie informacje niejawne o klauzuli „Ściśle tajne", „Tajne" lub „Poufne", tj. w szczególności kancelarie, czytelnie, pomieszczenia wydzielone powinny spełniać następujące warunki bezpieczeństwa fizycznego:

1. Poziom zagrożenia wysoki

1) usytuowanie w budynku o konstrukcji murowanej, betonowej lub innej o podobnych właściwościach (parametrach) konstrukcyjnych, z wejściem ze strefy ochronnej;

2) oddzielone od innych pomieszczeń stałymi przegrodami budowlanymi o rozwiązaniach konstrukcyjno-materiałowych zapewniających bezpieczeństwo pożarowe i bezpieczeństwo konstrukcji, pozbawionymi zbędnych otworów, a w przypadku, gdy ściany zewnętrzne lub stropy stanowią granicę strefy ochronnej, powinny być wykonane z materiałów niepalnych i spełniać wymagania w zakresie klasy odporności pożarowej oraz nośności granicznej odpowiadającej co najmniej konstrukcji murowanej z cegły grubości nie mniejszej niż 15 cm lub materiału o podobnej wytrzymałości;

3) wyposażone w drzwi wejściowe spełniające wymagania klasy RC 3 określone w Polskiej Normie PN-EN 1627, posiadające element samozatrzaskowy uniemożliwiający pozostawienie pomieszczenia otwartego, samozamykacz oraz wyposażone w zamek mechaniczny spełniający co najmniej wymagania klasy 4 określone w Polskiej Normie PN-EN 12209 lub elektroniczny szyfrowy co najmniej klasy B w Polskiej Normie PN-EN 1300, odporne na manipulację przez eksperta;

4) wyposażone w okna spełniające co najmniej wymagania klasy RC 3 określone w Polskiej Normie PN-EN 1627 lub zabezpieczone, stalowymi kratami zewnętrznymi lub wewnętrznymi z prętów lub innymi zabezpieczeniami posiadającymi odporność na włamanie nie mniejszą niż krata. Powyższe zabezpieczenia nie są niezbędne, jeżeli dolne krawędzie okien znajdują się na wysokości przynajmniej 5,5 m nad gruntem lub innym elementem budynku (np. balkonem lub balustradą) i nie można uzyskać do nich dostępu z dachu lub z wykorzystaniem znajdującego się w pobliżu elementu (rynna, drabina, drzewo) ułatwiającego potencjalny dostęp i penetrację, Przy tym rozwiązaniu dopuszcza się zastosowanie okien spełniających co najmniej wymagania klasy RC 2 określone w Polskiej Normie PN-EN 1627.
Okna pomieszczenia kancelarii, oraz pomieszczeń wydzielonych powinny być zabezpieczone przed podglądem z zewnątrz poprzez zastosowanie np. rolet, żaluzji, verticali lub szyb zabezpieczonych folią;

5) objęte bezpośrednią ochroną fizyczną w postaci posterunku lub okresowym patrolowaniem terenu wokół budynku nie rzadziej niż raz w dzień i dwa razy w nocy;

6) objęte kontrolą dostępu, z tym że:

a) instalowane elektroniczne systemy kontroli dostępu powinny spełniać wymagania techniczne i organizacyjne co najmniej w klasie rozpoznania 3, a w klasie dostępu B - określone w normie PN-EN 50133-1, wstęp kontrolowany jest przez odpowiednią barierę, system obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru,

b) dopuszcza się zastosowanie elektronicznego systemu kontroli dostępu, spełniającego co najmniej wymagania systemu w klasie rozpoznania 2, a w klasie dostępu B określone w normie PN-EN 50133-1, jeżeli wstęp kontrolowany jest przez odpowiednią barierę i system obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru,

c) w przypadku braku elektronicznego systemu kontroli dostępu, prowadzona jest książkowa ewidencja wejścia/ wyjścia do/z kontrolowanego pomieszczenia lub obszaru, wymagana jest identyfikacja osoby wchodzącej do strefy oraz obecność personelu bezpieczeństwa. Dane z ewidencji są przechowywane co najmniej z okresu ostatnich 12 miesięcy;

7) wyposażone w system alarmowy, z tym że:
a) powinien on sygnalizować nieuprawnione otwarcie drzwi wejściowych i okien, ruch w pomieszczeniach oraz próby napadu,
b) powinien spełniać wymagania techniczne i organizacyjne - określone w normie PN-EN 50131-1 stopnia 3;

8) wyposażone w miarę możliwości w system dozoru wizyjnego, który powinien spełniać wymagania techniczne i organizacyjne stopnia 3 określone w normie PN-EN 50132-1, z tym że:
a) powinien on rejestrować obraz drzwi wejściowych i osób wchodzących do tych pomieszczeń,
b) rejestracja powinna umożliwiać identyfikację osób,
c) zarejestrowany zapis należy przechowywać przez czas nie krótszy niż 30 dni.

2. Poziom zagrożenia średni

1) usytuowanie w budynku o konstrukcji zgodnie z wymaganiami określonymi w ust. 1 pkt. 1;

2) oddzielone od innych pomieszczeń zgodnie z wymaganiami określonymi w ust. 1 pkt. 2;

3) wyposażone w drzwi wejściowe spełniające wymagania klasy RC 2 określone w Polskiej Normie PN-EN 1627, posiadające element samozatrzaskowy uniemożliwiający pozostawienie pomieszczenia otwartego, samozamykacz oraz wyposażone w zamek mechaniczny spełniający co najmniej wymagania klasy 3 określone w Polskiej Normie PN-EN 12209 lub elektroniczny szyfrowy co najmniej klasy A w Polskiej Normie PN-EN 1300, odporne na manipulację przez eksperta;

4) wyposażone w okna spełniające co najmniej wymagania klasy RC 2 określone w Polskiej Normie PN-EN 1627 lub zabezpieczone, stalowymi kratami zewnętrznymi lub wewnętrznymi z prętów lub innymi zabezpieczeniami posiadającymi odporność na włamanie nie mniejszą niż krata. Powyższe zabezpieczenia nie są niezbędne, jeżeli dolne krawędzie okien znajdują się na wysokości przynajmniej 5,5 m nad gruntem lub innym elementem budynku (np. balkonem lub balustradą) i nie można uzyskać do nich dostępu z dachu lub z wykorzystaniem znajdującego się w pobliżu elementu (rynna, drabina, drzewo) ułatwiającego potencjalny dostęp i penetrację, Przy tym rozwiązaniu dopuszcza się zastosowanie okien spełniających co najmniej wymagania klasy RC 1 określone w Polskiej Normie PN-EN 1627.
Okna pomieszczenia kancelarii, oraz pomieszczeń wydzielonych powinny być zabezpieczone przed podglądem z zewnątrz poprzez zastosowanie np. rolet, żaluzji, verticali lub szyb zabezpieczonych folią;

5) objęte bezpośrednią ochroną fizyczną określoną w ust. 1 pkt 5;

6) objęte kontrolą dostępu określoną w ust. 1 pkt 6;

7) wyposażone w system alarmowy, z tym że:
   a) powinien sygnalizować nieuprawnione otwarcie drzwi wejściowych i okien, ruch w pomieszczeniach oraz próby napadu,
   b) instalowane systemy alarmowe powinny spełniać wymagania techniczne i organizacyjne stopnia 2 określone w normie PN-EN 50131-1.

8) wyposażone w miarę możliwości w system dozoru wizyjnego, który powinien spełniać wymagania techniczne i organizacyjne stopnia 2 określone w normie PN-EN 50132-1, z tym że:
   a) powinien on rejestrować obraz drzwi wejściowych i osób wchodzących do tych pomieszczeń,
   b) rejestracja powinna umożliwiać identyfikację osób,
   c) zarejestrowany zapis należy przechowywać przez czas nie krótszy niż 30 dni.

3. Poziom zagrożenia niski

1) usytuowanie w budynku spełniającym wymagania określone w ust. 1 pkt. 1;

2) oddzielone od innych pomieszczeń zgodnie z wymaganiami określonymi w ust. 1 pkt 2;

3) wyposażone w drzwi wejściowe spełniające wymagania klasy RC 2 określone w Polskiej Normie PN-EN 1627, posiadające element samozatrzaskowy uniemożliwiający pozostawienie pomieszczenia otwartego, samozamykacz oraz wyposażone w zamek mechaniczny spełniający co najmniej wymagania klasy 2 określone w Polskiej Normie PN-EN 12209 lub elektroniczny szyfrowy co najmniej klasy A w Polskiej Normie PN-EN 1300, odporne na manipulację przez eksperta;

4) wyposażone w okna spełniające wymagania określone w ust. 2 pkt 4;

5) objęte bezpośrednią ochroną fizyczną w postaci posterunku lub okresowym patrolowaniem terenu wokół budynku nie rzadziej niż raz w nocy;

6) objęte kontrolą dostępu, określoną w ust. 1 pkt 6;

7) wyposażone w system alarmowy, z tym że:
   a) powinien sygnalizować nieuprawnione otwarcie drzwi wejściowych i okien oraz próby napadu,
   b) instalowane systemy alarmowe powinny spełniać wymagania techniczne i organizacyjne stopnia 1 określone w normie PN-EN 50131-1;

8) wyposażone w miarę możliwości w system dozoru wizyjnego, który powinien spełniać wymagania techniczne i organizacyjne stopnia 1 określone w normie PN-EN 50132-1, z tym że:
   a) powinien on rejestrować obraz drzwi wejściowych i osób wchodzących do tych pomieszczeń,
   b) rejestracja powinna umożliwiać identyfikację osób,
   c) zarejestrowany zapis należy przechowywać przez czas nie krótszy niż 30 dni.

4. Pomieszczenia specjalne powinny spełniać następujące warunki:
   1) wymagania dla strefy zabezpieczonej technicznie określone w rozporządzeniu w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych;
   2) szczegółowe wymagania w zakresie zabezpieczenia przed podsłuchem i podglądem oraz stosowania odpowiednich środków bezpieczeństwa fizycznego dla każdego z pomieszczeń określa ABW w oparciu o zalecenia;
   3) zakaz wnoszenia przez osoby biorące udział w spotkaniu (naradzie, odprawie, konferencji) z wykorzystaniem prezentacji multimedialnych, wideo oraz spotkań realizowanych w ramach wideokonferencji wszelkich urządzeń elektronicznych służących do rejestracji i przekazywania obrazu lub głosu;
   4) prowadzenie przez ABW okresowych badań przeciwpodsłuchowych pomieszczenia oraz doraźnie w miarę potrzeb przed naradą, odprawą, konferencją, prezentacją multimedialną, wideokonferencją, a także po każdorazowym nieuprawnionym wejściu do strefy, podejrzeniu, że takie wejście mogło mieć miejsce oraz sprzętu będącego na wyposażeniu pomieszczenia który powrócił po naprawie lub konserwacji.

5. W przypadku pomieszczenia wzmocnionego środki bezpieczeństwa fizycznego należy stosować odpowiednio do określonego poziomu zagrożeń.

6. Konstrukcja pomieszczenia, o którym mowa w ust. 5 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.

7. Część kancelarii przeznaczoną do wydawania i udostępniania dokumentów niejawnych odgradza się barierą fizyczną od części przeznaczonej do przechowywania materiałów niejawnych oraz wykonywania pracy przez personel tej komórki.

8. W pomieszczeniach lub obszarach, o których mowa w ust. 1-5 instaluje się system sygnalizacji przeciwpożarowej.

9. Pomieszczenia lub obszary, o których mowa w ust. 1-4, odpowiednio do potrzeb, wyposaża się w nw. urządzenia do przechowywania dokumentów niejawnych:
   1) szafy metalowe spełniające co najmniej wymagania klasy odporności na włamanie S 1, określone w Polskiej Normie PN-EN 14450 lub nowszej i zabezpieczone zamkiem klasy B, określonym w Polskiej Normie PN-EN 1300 do przechowywania dokumentów zawierających informacje niejawne oznaczonych klauzulą „Ściśle tajne", a także „Tajne", „Poufne" i „Zastrzeżone";
   2) szafy metalowe zamykane na klucz, charakteryzujące się umiarkowaną odpornością na nieuprawnione próby otwarcia, zabezpieczone zamkiem typu 1 lub 2 z Kategorii K1S2, do przechowywania dokumentów zawierających informacje niejawne oznaczonych klauzulą „Poufne" i „Zastrzeżone";
   3) szafy - meble biurowe zamykane na klucz, niewyposażone w żadne szczególne funkcje zabezpieczające, ale charakteryzujące się umiarkowaną odpornością na nieuprawnione próby otwarcia, zabezpieczone zamkiem, do przechowywania dokumentów zawierających informacje niejawne oznaczonych klauzulą „Zastrzeżone".

10. W przypadku okien dodatkowo chronionych przez rozsuwane lub otwierane kraty, należy je zabezpieczyć kłódką klasy nie niższej niż 3 wg normy PN-EN 12320.

11. Pomieszczenia zlokalizowane poza strefą ochronną I lub II, w których przetwarzane są informacje niejawne, wyposaża się, odpowiednio do potrzeb, bez względu na poziom zagrożeń, w określone w ust. 9 urządzenia do przechowywania materiałów niejawnych.

12. W pomieszczeniach lub obszarach stanowiących strefę ochronną I, dopuszcza się przechowywanie materiałów niejawnych poza urządzeniami do przechowywania materiałów niejawnych.

§ 5. 1. Analizę poziomu zagrożeń pomieszczeń lub obszarów, o których mowa w § 4 ust. 1-5 prowadzi się każdorazowo przed ich uruchomieniem oraz w przypadku istotnych zmian czynników mogących mieć wpływ na ochronę informacji, jak również zmiany środków bezpieczeństwa fizycznego.

2. W przypadku wzrostu poziomu zagrożenia kierownicy jednostek (komórek) organizacyjnych wzmacniają system bezpieczeństwa fizycznego wykorzystując dostępne środki ochrony, a w szczególności stałą ochronę fizyczną do czasu powrotu do stanu pierwotnego, bądź wyeliminowania czynnika powodującego wzrost zagrożenia.

3. W szczególnie uzasadnionych przypadkach uniemożliwiających spełnienie któregokolwiek z warunków, o których mowa w § 4 ust. 1-4, zgodę na zastosowanie alternatywnych środków bezpieczeństwa udziela kierownik jednostki organizacyjnej.

§ 6. 1. Po zakończeniu pracy kierownicy kancelarii lub wyznaczeni przez nich pracownicy pionu ochrony, zamykają i zabezpieczają urządzenia do przechowywania dokumentów niejawnych oraz zabezpieczają pomieszczenia służbowe.

2. Zasady zdawania, przechowywania i wydawania kluczy użytku bieżącego do pomieszczeń służbowych i urządzeń, o których mowa w ust. 1, określa plan ochrony informacji niejawnych, o którym mowa w art. 15 ust. 1 pkt 5 ustawy.

3. Klucze zapasowe, kody dostępu oraz kody systemu alarmowego do pomieszczeń lub obszarów, o których mowa w § 4 ust. 1-5, a także znajdujących się w nich urządzeń do przechowywania dokumentów lub nośników informacji niejawnych, umieszczone w odpowiednio oznaczonych, zabezpieczonych i zaewidencjonowanych kopertach, przechowuje pełnomocnik ochrony lub kierownik jednostki organizacyjnej.

4. Zabrania się zapisywania przez użytkowników kodów dostępu, z zastrzeżeniem ust. 3 oraz wynoszenia poza teren jednostki organizacyjnej kluczy, o których mowa w ust. 2 i 3.

5. Każdorazowe użycie kluczy zapasowych do pomieszczeń lub obszarów odnotowuje się w stosownych ewidencjach.

6. Kody dostępu, o których mowa w ust. 3 zmienia się:
   1) w urządzeniach i zamkach nowo instalowanych, co najmniej raz w roku;
   2) po każdej zmianie składu osób znających kod, jeżeli kod nie jest wprowadzony indywidualnie;
   3) w przypadku zaistnienia podejrzenia, że osoba nieuprawniona mogła poznać kod;
   4) gdy zamek poddano konserwacji lub naprawie.

§ 7. 1. Przetwarzanie informacji niejawnych .o klauzuli "Poufne" lub wyższej w systemach teleinformatycznych odbywa się w strefie ochronnej I lub strefie ochronnej II , w warunkach uwzględniających wyniki procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy.

2. Przekazywanie informacji, o których mowa w ust. 1, odbywa się w strefie ochronnej, na podstawie wyników procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy.

3. Przetwarzanie informacji niejawnych o klauzuli "Zastrzeżone" w systemach teleinformatycznych odbywa się w pomieszczeniu lub obszarze wyposażonym w system kontroli dostępu, w warunkach uwzględniających wyniki procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy.

4. Serwery, systemy zarządzania siecią, kontrolery sieciowe i inne newralgiczne elementy systemów teleinformatycznych umieszcza się, z uwzględnieniem wyników procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy, w następujący sposób:
   1) w strefie ochronnej w przypadku przetwarzania informacji niejawnych o klauzuli "Zastrzeżone";
   2) w strefie ochronnej I lub w strefie ochronnej II, w przypadku przetwarzania informacji niejawnych o klauzuli "Poufne" lub wyższej.

5. Przetwarzanie informacji niejawnych w części mobilnej zasobów systemu teleinformatycznego odbywa się na podstawie wyników procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy, w sposób określony w dokumentacji bezpieczeństwa systemu teleinformatycznego.

Rozdział 3

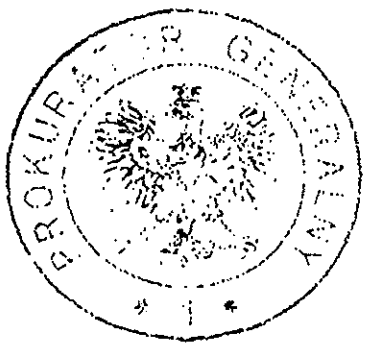
Przepisy przejściowe i końcowe

§ 8. Ustalenia zarządzenia dotyczą odpowiednio oddziału kancelarii.

§ 9. Środki ochrony fizycznej wynikające z poziomu zagrożeń należy dostosować do dnia 3 lipca 2015 roku.

§ 10. Certyfikaty i tabliczki znamionowe przyznane wyposażeniu i urządzeniom służącym ochronie informacji niejawnych, wydane przed dniem wejścia w życie rozporządzenia, zachowują ważność.

§ 11. Zarządzenie wchodzi w życie z dniem podpisania.



Andrzej Seremet