# 26

## WYTYCZNE
## MINISTRA OBRONY NARODOWEJ

z dnia 23 stycznia 2007 r.

**w sprawie ochrony informacji niejawnych oraz obiektów wojskowych w jednostkach organizacyjnych podporządkowanych Ministrowi Obrony Narodowej lub przez niego nadzorowanych w 2007 r.**

Na podstawie § 2 pkt 6 i 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426), w celu zwiększenia skuteczności ochrony informacji niejawnych oraz obiektów wojskowych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, polecam:

**1. W zakresie postępowań sprawdzających i szkolenia**:

1) do końca marca wdrożyć w podległych jednostkach organizacyjnych znowelizowane decyzje Ministra Obrony Narodowej regulujące funkcjonowanie resortowego systemu ochrony informacji niejawnych;
2) kierować sukcesywnie na szkolenia uzupełniające, prowadzone przez Służbę Kontrwywiadu Wojskowego, pełnomocników ochrony jednostek organizacyjnych, którzy ukończyli szkolenie specjalistyczne przed 2002 rokiem;
3) przeszkolić do końca roku kierowników i pracowników bibliotek tajnych oraz kancelarii prowadzących ewidencję i przechowujących materiały planowania operacyjnego, planowania mobilizacyjnego i gotowości bojowej, którzy nie posiadają zaświadczenia o ukończeniu szkolenia specjalistycznego, o którym mowa w § 3 ust. 9 zarządzenia Nr 25/MON Ministra Obrony Narodowej z dnia 17 listopada 2005 r. w sprawie szczególnego sposobu organizacji kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych (Dz. Urz. MON Nr 21, poz. 203);
4) zorganizować szkolenie uzupełniające dla kierowników i pracowników kancelarii tajnych, którzy ukończyli szkolenie specjalistyczne przed dniem wejścia w życie ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631, z późn. zm.);
5) organizować szkolenia uzupełniające, połączone z rozliczeniem z realizacji zadań merytorycznych, dla pełnomocników ochrony z podległych jednostek organizacyjnych;
6) każde ćwiczenie i trening sztabowy poprzedzać wydaniem przez pełnomocnika ochrony jednostki organizacyjnej wytycznych w sprawie ochrony informacji niejawnych podczas ćwiczenia oraz przeszkoleniem osób uczestniczących w ćwiczeniu w zakresie ochrony informacji niejawnych;
7) informować pełnomocnika ochrony bezpośrednio nadrzędnej jednostki organizacyjnej o organizowanych przez siebie szkoleniach specjalistycznych i uzupełniających dla pracowników pionów ochrony; angażować przedstawicieli Służby Kontrwywiadu Wojskowego, Departamentu Ochrony Informacji Niejawnych oraz pionów ochrony bezpośrednio nadrzędnych jednostek organizacyjnych do prowadzenia zajęć szkoleniowych;
8) kierować osoby wyznaczane na stanowiska pełnomocników ochrony od szczebla dywizji wzwyż, przed objęciem obowiązków służbowych, na krótkotrwałe praktyki w pionach ochrony bezpośrednio nadrzędnych jednostek organizacyjnych;

9) uzupełniać na bieżąco oraz systematycznie analizować wykazy stanowisk i prac zleconych, z którymi może łączyć się dostęp do informacji niejawnych oraz osób dopuszczonych do pracy lub służby na tych stanowiskach pod kątem aktualności tych wykazów, a także rozliczać z materiałów niejawnych oraz wstrzymywać dostęp do informacji niejawnych osobom, których poświadczenia bezpieczeństwa tracą ważność;
10) wnioski o wszczęcie kolejnych postępowań sprawdzających wobec osób zatrudnionych na stanowiskach, z którymi może się łączyć dostęp do informacji niejawnych, składać co najmniej 6 miesięcy przed upływem terminów ważności posiadanych przez te osoby poświadczeń bezpieczeństwa;
11) stosownie do zaleceń pokontrolnych Biura Bezpieczeństwa NATO, wystąpić do Służby Kontrwywiadu Wojskowego o wydanie certyfikatów bezpieczeństwa NATO osobom zatrudnionym na stanowiskach, z którymi może się łączyć dostęp do informacji niejawnych NATO oznaczonych klauzulą „Poufne" lub wyższą.

**2. W zakresie bezpieczeństwa teleinformatycznego:**

1) poprzez systematyczny nadzór służbowy wyeliminować przypadki przetwarzania informacji niejawnych, zwłaszcza podczas ćwiczeń poza miejscem stałej dyslokacji, w systemach i sieciach teleinformatycznych nie posiadających akredytacji bezpieczeństwa teleinformatycznego;
2) prowadzić ewidencję systemów i sieci teleinformatycznych funkcjonujących w podległych jednostkach organizacyjnych, w tym sprzętu w wykonaniu specjalnym, a także nadzorować gospodarkę materiałową tym sprzętem;
3) na podstawie prowadzonej ewidencji przygotowywać dla kierowników jednostek organizacyjnych, w nakazanych przepisami terminach, wnioski do Szefa Służby Kontrwywiadu Wojskowego o przeprowadzenie audytów recertyfikacyjnych pomieszczeń wydzielonych, w których są przetwarzane informacje niejawne, a także badań kontrolnych elektromagnetycznej emisji ujawniającej zestawów komputerowych klasy „Tempest", Bezpiecznych Stanowisk Komputerowych i kabin ekranujących;
4) systematycznie prowadzić w jednostce organizacyjnej bieżącą kontrolę zgodności funkcjonowania systemów i sieci teleinformatycznych z ich Szczególnymi Wymaganiami Bezpieczeństwa oraz sposobu przestrzegania przez użytkowników zasad zawartych w Procedurach Bezpiecznej Eksploatacji;
5) w ramach szkolenia uzupełniającego systematycznie szkolić użytkowników systemów i sieci teleinformatycznych, w których są wytwarzane, przetwarzane lub przesyłane informacje niejawne, a także co najmniej raz w roku organizować szkolenie uzupełniające dla administratorów systemów i sieci teleinformatycznych z podległych jednostek organizacyjnych;
6) nadzorować deklasyfikację, wycofywanie oraz niszczenie elektronicznych nośników cyfrowych, na których zapisano informacje niejawne;
7) stosować, we wszystkich systemach i sieciach teleinformatycznych, w których są przetwarzane, wytwarzane, przechowywane i przesyłane informacje niejawne, oprogramowanie antywirusowe i na bieżąco je aktualizować;
8) wdrożyć w podległych jednostkach organizacyjnych przepisy decyzji Nr 488/MON Ministra Obrony Narodowej z dnia 30 listopada 2006 r. w sprawie wprowadzenia do użytku w resorcie obrony narodowej „Tymczasowej instrukcji organizacji obiegu informacji niejawnych o klauzuli „Zastrzeżone" w resortowej sieci teleinformatycznej MIL-WAN".

**3. W zakresie nadzoru nad ochroną informacji niejawnych:**

1) w terminie do 15 października poinformować pełnomocnika ochrony bezpośrednio nadrzędnej jednostki organizacyjnej o planowanych przez siebie do realizacji na rok następny kontrolach problemowych;
2) informować pełnomocnika bezpośrednio nadrzędnej jednostki organizacyjnej o stwierdzanych w czasie kontroli faktach utraty dokumentów niejawnych oraz naruszeniach przepisów o ochronie informacji niejawnych;
3) podczas kontroli problemowych, prowadzonych w podległych jednostkach organizacyjnych, wyrywkowo sprawdzać stan faktyczny dokumentów niejawnych pobranych przez wykonawców, zwłaszcza materiałów zawierających informacje stanowiące tajemnicę państwową;
4) w czasie kontroli rocznej za rok 2007 dokonać przeglądu wytworzonych w jednostce organizacyjnej dokumentów zawierających informacje stanowiące tajemnicę służbową, którym upływa okres ochrony pod kątem jego ewentualnego przedłużenia;
5) nadzorować przebieg kontroli rocznej i półrocznej stanu ochrony informacji niejawnych w jednostce organizacyjnej;
6) w protokołach, meldunkach i notatkach z kontroli każdorazowo formułować konkretne wnioski oraz skierowane do określonych osób terminowe zadania (zalecenia) zawierające sposób usunięcia stwierdzonych nieprawidłowości;
7) wyniki działalności kontrolnej wykorzystywać szeroko w działalności profilaktycznej i szkoleniowej oraz do wypracowywania procedur zmierzających do usprawnienia systemu ochrony informacji niejawnych w jednostce organizacyjnej;
8) w ocenach stanu ochrony informacji niejawnych za 2006 r. sformułować dla komórek wewnętrznych jednostki organizacyjnej oraz osób funkcyjnych zadania zmierzające do wyeliminowania występujących w jednostce nieprawidłowości oraz udoskonalenia obowiązującego systemu ochrony informacji niejawnych.

**4. W zakresie bezpieczeństwa przemysłowego**:

1) uczestniczyć każdorazowo przy zawieraniu przez jednostkę organizacyjną umów dotyczących zlecenia przedsiębiorcy, jednostce naukowej lub badawczo-rozwojowej zadań związanych z dostępem do informacji niejawnych; określać w instrukcjach bezpieczeństwa przemysłowego szczegółowy sposób ochrony przez przedsiębiorcę przekazywanych informacji, w tym także ochrony materiałów wytworzonych przez niego w trakcie realizacji umowy oraz skutki jakie poniesie przedsiębiorca w przypadku niezapewnienia bezpieczeństwa przekazywanym mu informacjom;
2) materiały niejawne przekazywać przedsiębiorcom z chwilą ustalenia, że posiadają oni zdolność do zapewnienia bezpieczeństwa informacjom niejawnym, które zostaną im udostępnione w ramach realizacji umowy. Należy kontrolować okresowo, w czasie obowiązywania umowy, sposób ochrony przekazywanych dokumentów niejawnych.

**5. W zakresie funkcjonowania kancelarii tajnych i innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych**:

1) zaplanować środki finansowe na wykonanie zabezpieczeń oraz wyposażenie pomieszczeń kancelarii, bibliotek i kancelarii mobilizacyjnych tak, aby do końca 2008 roku osiągnąć standardy wynikające z przepisów zarządzenia Nr 25/MON Ministra Obrony Narodowej z dnia 17 listopada 2005 r. w sprawie szczególnego sposobu organizacji kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych;
2) rozważyć możliwość zorganizowania kancelarii tajnej wraz z punktem obsługi dokumentów zagranicznych, na bazie istniejącej kancelarii zagranicznej, w jednostkach organizacyjnych, w których kancelarie tajne nie spełniają wymaganych standardów w zakresie zabezpieczenia fizycznego i elektronicznego;
3) materiały niejawne innych jednostek organizacyjnych obsługiwanych przez kancelarię tajną jednostki organizacyjnej, jeżeli nie są one dyslokowane w tej samej strefie administracyjnej, udostępniać wyłącznie w pomieszczeniach kancelarii tajnej;
4) przekazać do właściwego archiwum lub odpowiednio wybrakować materiały archiwalne i niearchiwalne, które są nieprzydatne dla prowadzenia praktycznej działalności przez jednostkę organizacyjną.

**6. W zakresie ochrony obiektów jednostek organizacyjnych resortu**:

1) wdrożyć w podległych jednostkach organizacyjnych rozporządzenie Ministra Obrony Narodowej w sprawie szczegółowych zadań pełnomocników ochrony oraz szczególnych wymagań w zakresie ochrony fizycznej jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, a także przejąć zadania związane z ochroną obiektów wojskowych jednostek organizacyjnych;
2) nadzorować na bieżąco realizację planów ochrony obiektów wojskowych oraz aktualizować je stosownie do pojawiających się zagrożeń i potrzeb;
3) realizować proces budowy, rozbudowy oraz modernizacji systemów ochrony technicznej obiektów wojskowych uwzględniając obowiązujące parametry funkcjonalne i wymagania taktyczno-użytkowe dla systemów i urządzeń alarmowych, a także wymogi w zakresie dokumentacji projektowo-kosztorysowej i procedury przetargowe;
4) dążyć do zwiększenia udziału wart cywilnych oraz specjalistycznych uzbrojonych formacji ochronnych przedsiębiorców w ochronie fizycznej obiektów jednostek organizacyjnych;
5) organizować, co najmniej raz w roku, szkolenia instruktażowo-metodyczne z ochrony obiektów, podczas których prezentować przykładowe działanie sił ochronnych, a także wykorzystanie systemów i urządzeń alarmowych oraz systemów kontroli dostępu. Do prowadzenia zajęć angażować przedstawicieli Służby Kontrwywiadu Wojskowego, Departamentu Ochrony Informacji Niejawnych oraz pionów ochrony bezpośrednio nadrzędnych jednostek organizacyjnych;
6) raz na kwartał organizować dla całego stanu osobowego szkolenia instruktażowo-metodyczne z pozorowanym naruszeniem systemu ochrony w celu doskonalenia procedur postępowania sił ochronnych i stanów osobowych w zakresie przeciwdziałania zagrożeniom ze strony zorganizowanych grup przestępczych i terrorystycznych;
7) sporządzić, zgodnie z wzorcem określonym przez Departament Ochrony Informacji Niejawnych, oraz przesłać do 30 maja bieżącego roku do szczebla bezpośrednio nadrzędnego sprawozdanie z ochrony obiektów jednostki organizacyjnej za rok 2006, a także zestawienie zbiorcze do weryfikacji wartości pieniężnych norm rzeczowych na eksploatację systemów i urządzeń alarmowych oraz zestawienie ilościowo-jakościowe specjalistycznego sprzętu ochrony obiektów;
8) systematycznie nadzorować i kontrolować stan ochrony obiektów wojskowych w podległych jednostkach organizacyjnych; wyniki kontroli wykorzystywać do podnoszenia skuteczności funkcjonujących systemów ochrony.

7. Wytyczne podlegają ogłoszeniu w Dzienniku Urzędowym Ministra Obrony Narodowej.

Minister Obrony Narodowej: *R. Sikorski*