Sebastian Kaleta

Rola i znaczenie kancelarii tajnych dla ochrony informacji niejawnych w resorcie obrony narodowej

Kultura Bezpieczeństwa. Nauka-Praktyka-Refleksje nr 20, 238-249

2015

Kultura Bezpieczeństwa
Nauka – Praktyka – Refleksje
Nr 20, 2015 (238–249)

ROLA I ZNACZENIE KANCELARII TAJNYCH DLA OCHRONY INFORMACJI NIEJAWNYCH W RESORCIE OBRONY NARODOWEJ

THE ROLE AND THE IMPORTANCE OF SECRET OFFICES FOR THE PROTECTION OF CLASSIFIED INFORMATION IN THE MINISTRY OF NATIONAL DEFENSE

SEBASTIAN KALETA
Akademia Obrony Narodowej

Abstract

The disclosure of classified information can contribute to causing threat to national security. In order to prevent such situations in the Ministry of National Defense a specialized, full-time organizational units called protection sections have been appointed. Protection sections consists of secret offices which are responsible for recording, storage, circulation, publishing and archiving of classified information.

The article also highlights the key threats to classified information, and discusses the organization of secret offices in the Ministry of National Defense. The idea of "instruments of protection" have been presented to ensure the safety for both offices and for the information which is being processed.

Key words

secret office, protection of classified information, physical security measures, personal security, personnel training, control

Abstrakt

Ujawnienie informacji niejawnych może przyczynić się do spowodowania zagrożenia dla bezpieczeństwa państwa. W celu przeciwdziałania takim sytuacjom w resorcie obrony narodowej powołano wyspecjalizowane, etatowe komórki organizacyjne zwane pionami ochrony. W skład pionów ochrony wchodzą kancelarie tajne, które są odpowiedzialne za rejestrowanie, przechowywanie, obieg, wydawanie i archiwizację informacji niejawnych. W artykule wskazano główne zagrożenia dla informacji niejawnych oraz omówiono organizację kancelarii tajnych w resorcie obrony narodowej. Przedstawiono także „instrumenty ochrony" służące zapewnieniu bezpieczeństwa zarówno kancelariom jak i informacjom w nich przetwarzanym.

Słowa kluczowe

kancelaria tajna, ochrona informacji niejawnych, środki bezpieczeństwa fizycznego, bezpieczeństwo osobowe, szkolenie personelu, kontrola.

Ochrona informacji niejawnych[1] jest jednym z najistotniejszych elementów mających bezpośredni wpływ na bezpieczeństwo państwa. Świadome czy też niekontrolowane działanie, skutkujące ujawnieniem informacji niejawnych, szczególnie tych o najwyższych klauzulach tajności, „ściśle tajne"[2] czy

[1] Informacje niejawne – to informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania – art. 1.1 *Ustawy o ochronie informacji niejawnych* (Dz. U. z 2010 r., nr 182, poz.1228).

[2] Na podstawie art. 5.1 *Ustawy o ochronie informacji niejawnych* informacjom niejawnym nadaje się klauzulę „ściśle tajne" jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że: zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej; zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej; zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej; osłabi gotowość obronną Rzeczypospolitej Polskiej.

też „ tajne”[3] może się przyczynić do powstania zagrożeń dla najwyższych wartości każdego państwa, jakimi niewątpliwie są niepodległość, suwerenność czy integralność terytorialna. Dlatego też do priorytetów działalności podmiotów odpowiedzialnych za zapewnienie ochrony tymże informacjom, należy udoskonalanie istniejących bądź tworzenie nowych systemów[4] ochrony informacji niejawnych.

Autor niniejszego artykułu chciałby zwrócić uwagę na jeden z elementów struktury organizacyjnej pionów ochrony informacji niejawnych, mianowicie na kancelarie tajne. Sprawnie funkcjonująca kancelaria tajna jest w stanie zapewnić efektywną wymianę informacji pomiędzy uprawnionymi wykonawcami. Jednocześnie stanowi ona fizyczną barierę, która uniemożliwia dostęp do informacji wykonawcom nieupoważnionym.

Celem niniejszego artykułu jest przedstawienie znaczenia kancelarii tajnych resortu obrony narodowej dla zachowania bezpieczeństwa informacji w nich przetwarzanych oraz standardów mających zapewnić to bezpieczeństwo.

Miejsce kancelarii tajnych określa ustawa o ochronie informacji niejawnych. Art. 14 ust.1 określa, iż za ochronę informacji, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony jest odpowiedzialny kierownik jednostki organizacyjnej, w której te informacje są przetwarzane. Na kierowniku jednostki organizacyjnej, w której są przetwarzane informacje niejawne o klauzuli „tajne” lub „ściśle tajne”, ciąży obowiązek utworzenia kancelarii tajnej, czyli wyodrębnionej komórki organizacyjnej, w zakresie informacji niejawnych podległej pełnomocnikowi ochrony, obsługiwanej przez pracowników ochrony, która jest odpo-

[3] Zgodnie z art. 5.2 *Ustawy o ochronie informacji niejawnych* informacjom niejawnym nadaje się klauzulę „tajne” jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że: uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej; pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi; zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej; utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione; w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości; przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej.

[4] System (stgr. *σύστημα systema* – rzecz złożona) – obiekt fizyczny lub abstrakcyjny, w którym można wyodrębnić zespół lub zespoły elementów wzajemnie powiązanych w układy, realizujących jako całość funkcję nadrzędną lub zbiór takich funkcji (funkcjonalność).

wiedzialna za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów uprawnionym osobom.

Kierownik jednostki zadanie to realizuje wraz z pełnomocnikiem ochrony, który jest odpowiedzialny za m.in. zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego. Natomiast pełnomocnik ochrony zadanie to realizuje przy pomocy wyodrębnionej i podległej mu komórki organizacyjnej do spraw ochrony informacji niejawnych – pionu ochrony[5].

O fakcie utworzenia bądź likwidacji kancelarii tajnej kierownik jednostki organizacyjnej informuje zgodnie z ustawą Służbę Kontrwywiadu Wojskowego, określając jednocześnie klauzule tajności informacji niejawnych, które będą w niej przetwarzane. W gestii kierownika jednostki leży wydanie zgody na przetwarzanie w kancelarii tajnej informacji o niższych klauzulach tj. „zastrzeżone" i „poufne".

Kierownik jednostki akceptuje następujące projekty dokumentów regulujących ochronę informacji niejawnych w jednostce organizacyjnej. Są to opracowane przez pełnomocnika ochrony dokumenty określające:
- poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą;
- sposób i tryb przetwarzania informacji niejawnych o klauzuli „poufne" w podległych komórkach organizacyjnych,
- sposób i tryb przetwarzania informacji niejawnych o klauzuli „zastrzeżone" oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony;
- plan ochrony informacji niejawnych w jednostce organizacyjnej, w tym postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne" i „ściśle tajne" w razie wprowadzenia stanu nadzwyczajnego;
- decyzji (rozkazu) kierownika jednostki organizacyjnej w sprawie organizacji systemu przepustkowego w jednostce organizacyjnej.[6]

W celu skutecznej ochrony informacji niejawnych w jednostkach organizacyjnych stosuje się środki bezpieczeństwa fizycznego, które obejmują przedsięwzięcia organizacyjne, ochronę fizyczną i ochronę techniczną.

---

[5] Art. 15 ust. 1 Ustawy o ochronie informacji niejawnych.

[6] Rozporządzenie Ministra Obrony Narodowej z dnia 19 grudnia 2013 r. w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych (Dz. U. z 2013 r., nr 0, poz. 1660, § 5.1).

Jednostki organizacyjne, w których są przetwarzane informacje niejawne, mają obowiązek stosowania środków bezpieczeństwa fizycznego odpowiedniego do poziomu zagrożeń w celu uniemożliwienia osobom nieuprawnionym dostępu do takich informacji, w szczególności przed : działaniem obcych służb specjalnych, zamachem terrorystycznym lub sabotażem, kradzieżą lub zniszczeniem materiału oraz próbą wejścia osób nieuprawnionych do pomieszczeń, w których są przetwarzane informacje niejawne oraz nieuprawnionym dostępem do informacji o wyższej klauzuli tajności niewynikającym z posiadanych uprawnień.

Zakres stosowania środków bezpieczeństwa fizycznego uzależnia się od poziomu zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą.

W celu określenia poziomu zagrożeń należy przeprowadzić analizę uwzględniającą wszystkie istotne czynniki mogące mieć wpływ na bezpieczeństwo informacji niejawnych, w szczególności:

- klauzule tajności przetwarzanych informacji niejawnych,
- postać i ilość informacji niejawnych,
- sposób przechowywania informacji niejawnych,
- otoczenie i strukturę budynków lub stref, w których są przetwarzane informacje niejawne,
- liczbę osób mających lub mogących mieć dostęp do informacji niejawnych, a także posiadane przez nich uprawnienia oraz uzasadnioną potrzebę dostępu do informacji niejawnych,
- szacowane zagrożenie ze strony obcych służb specjalnych oraz zagrożenie sabotażem, zamachem terrorystycznym, kradzieżą lub inną działalnością przestępczą uzyskane od Służby Kontrwywiadu Wojskowego, Żandarmerii Wojskowej, Policji i innych instytucji.[7]

Aby uniemożliwić osobom nieuprawnionym dostęp do informacji niejawnych należy zorganizować strefy ochronne, wprowadzić system kontroli wejść i wyjść ze stref ochronnych, określić uprawnienia do przebywania w tych strefach oraz stosować tylko certyfikowane wyposażenie i urządzenia służące ochronie tych informacji.

[7] §5 Zarządzenia Nr 57/MON Ministra Obrony Narodowej z dnia 16 grudnia 2011 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych, sposobi i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego.

Strefa ochronna I obejmuje pomieszczenia lub obszar, w którym informacje niejawne są przetwarzane w taki sposób, że wstęp do tych pomieszczeń wiąże się z uzyskaniem bezpośredniego dostępu do informacji.

Strefa ochronna II obejmuje pomieszczenia lub obszar, w którym informacje niejawne są przetwarzane w taki sposób, że wstęp do tych pomieszczeń nie umożliwia uzyskania bezpośredniego dostępu do informacji.

W strefach tych przetwarza się informacje niejawne o klauzuli „ściśle tajne" i „tajne" a przebywać w nich mogą osoby, które posiadają stałe lub okresowe upoważnienia.

Natomiast strefa ochronna III to pomieszczenia lub obszar, który wymaga wyraźnego wskazania granic, a ruch osób i pojazdów odbywa się pod kontrolą. W jednostkach funkcję taką sprawują biura przepustek. W strefie III mogą być przetwarzane informacje do klauzuli „poufne" włącznie, bez możliwości przetwarzania w systemach teleinformatycznych informacji o klauzuli „poufne". W strefie tej przebywają osoby z nadanymi stałymi lub okresowymi uprawnieniami do dostępu, a interesanci mogą poruszać się wyłącznie pod nadzorem osoby uprawnionej.

Kancelarie tajne powinny być, w miarę możliwości rozmieszczone w zespołach pomieszczeń składających się z co najmniej trzech pomieszczeń z przeznaczeniem na:
- pokój pracy dla personelu,
- pomieszczenia magazynowe służące do przechowywania materiałów niejawnych,
- pomieszczenia przeznaczone do zapoznawania się wykonawców z dokumentami niejawnymi.[8]

Dokumenty niejawne należy przechowywać w certyfikowanych szafach stalowych:
- szafa stalowa klasy C – służy do przechowywania dokumentów niejawnych o klauzuli „ściśle tajne",
- szafa stalowa klasy B – służy do przechowywania dokumentów niejawnych o klauzuli „tajne",
- szafa stalowa klasy A – służy do przechowywania dokumentów niejawnych o klauzuli „poufne".

Dokumenty niejawne o klauzuli „zastrzeżone" przechowuje się np. w szafach drewnianych lub biurkach zamykanych na klucz.

[8] Ibidem § 3 pkt. 23.

Kancelarie tajne wyposaża się, stosownie do potrzeb, w urządzenia do niszczenia dokumentów niejawnych. Urządzenia te muszą spełniać wymogi normy DIN 32757.[9]

Personel kancelarii udostępnia wykonawcom, których pomieszczenia znajdują się poza strefą ochronną, materiały o klauzuli „ściśle tajne", „tajne" i poufne" w pomieszczeniu do tego przeznaczonym, jednocześnie zakładając „Kartę zapoznania się z dokumentem" i dołączając ją do dokumentu. W ten sposób powstaje ścisła ewidencja osób zapoznających się z dokumentami oznaczonymi najwyższą klauzulą tajności. Należy dodać, iż dokumenty są udostępniane poszczególnym wykonawcom tylko na podstawie dekretacji[10] kierownika jednostki organizacyjnej. Znajduje tu zastosowanie zasada „need to know", czyli wiedzy niezbędnej np. posiadanie poświadczenia bezpieczeństwa o klauzuli „ściśle tajne" nie upoważnia do wglądu we wszystkie dokumenty oznaczone tą klauzulą, a jedynie w te niezbędne do wykonywania obowiązków na zajmowanym stanowisku służbowym.

Wymiana informacji niejawnych pomiędzy kancelariami tajnymi jednostek organizacyjnych odbywa się w dwojaki sposób:

1. Za pomocą podmiotów zwanych „przewoźnikami" np.:
- poczty specjalnej podległej ministrowi właściwemu do spraw wewnętrznych, zapewniającej przewóz materiałów na terytorium RP;
- komórki organizacyjnej urzędu obsługującego ministra właściwego do spraw zagranicznych, zapewniającej przewóz materiałów za granicę i poza granicami RP,
- właściwej jednostki organizacyjnej podległej Ministrowi Obrony Narodowej lub Szefowi Kontrwywiadu Wojskowego,
- przedsiębiorców uprawnionych do wykonywania działalności pocztowej tzw. „operatorów pocztowych",
- przedsiębiorców uprawnionych do wykonywania działalności w zakresie ochrony osób i mienia,
- przedsiębiorców uprawnionych do wykonywania działalności w zakresie usług transportowych.
2. Za pomocą sieci teleinformatycznych przystosowanych do przesyłania informacji niejawnych (które uzyskały akredytację bezpieczeństwa teleinformatycznego).

[9] Ibidem § 3 pkt. 13.

[10] Decyzja nr 385/MON Ministra Obrony Narodowej z dnia 17 grudnia 2013 r. w sprawie wprowadzenia do użytku „Instrukcji o zasadach pracy biurowej w resorcie obrony narodowej".

Wyznaczanie na stanowiska kierownika i kancelisty odbywa się spośród osób posiadających poświadczenie bezpieczeństwa odpowiednie dla klauzuli dokumentów przetwarzanych w kancelarii, odbyte przeszkolenie w zakresie ochrony informacji niejawnych oraz szkolenie specjalistyczne, potwierdzone stosownymi zaświadczeniami. W stosunku do kandydatów na stanowisko w kancelarii tajnej, a więc osób, które w przyszłości będą posiadały dostęp do informacji niejawnych o klauzuli „ściśle tajne" i „tajne" Służba Kontrwywiadu Wojskowego na wniosek kierownika jednostki organizacyjnej lub osoby uprawnionej do obsady stanowiska przeprowadza poszerzone postępowanie sprawdzające.

Sprawdzeniu podlegają m.in.:
- uczestnictwo, współpraca lub popieranie przez kandydata działalności szpiegowskiej, terrorystycznej, sabotażowej wymierzonej przeciwko Rzeczypospolitej Polskiej,
- autentyczność informacji zawartych przez kandydata w ankiecie bezpieczeństwa osobowego mających znaczenie dla ochrony informacji niejawnych,
- wystąpienia w związku z osobą sprawdzaną okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji,
- niewłaściwe postępowanie z informacjami niejawnymi.

Ponadto poszerzone postępowanie sprawdzające może swym zasięgiem objąć:
- rozmowę z przełożonymi osoby sprawdzanej,
- przeprowadzenie wywiadu w miejscu zamieszkania osoby sprawdzanej;
- sprawdzenie stanu i obrotów na rachunku bankowym oraz zadłużenia osoby sprawdzanej, w szczególności wobec Skarbu Państwa.

Czynności te mają na celu ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy. W przypadku pozytywnego wyniku postępowania kończy się ono wydaniem poświadczenia bezpieczeństwa dostępu do informacji niejawnych o klauzuli „ściśle tajne" na okres 5 lat, a do informacji niejawnych o klauzuli „tajne" na okres 7 lat.

Kandydaci na stanowiska w kancelariach tajnych objęci są szkoleniem specjalistycznym. Celem szkoleń specjalistycznych jest przygotowanie osób do wykonywania zadań służbowych. Natomiast pracownicy kancelarii tajnych objęci są szkoleniem specjalistycznym uzupełniającym, którego celem jest uzupełnienie wiedzy specjalistycznej. Szkolenie to ponawiane jest po pięciu latach.

Szkolenie w zakresie informacji niejawnych przeprowadza się w celu zapoznania z:
- przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności karnej, dyscyplinarnej i służbowej za ich naruszenie, w szczególności za nieuprawnione ujawnienie informacji niejawnych,
- zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub służby, z uwzględnieniem zasad zarządzania ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowania ryzyka,
- sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia,

Szkolenia mają uchronić pracowników kancelarii przed popełnianiem m.in. następujących błędów:
- złe prowadzenie ewidencji kancelaryjnej oraz brak nadzoru nad wytwarzaniem, ewidencjonowaniem, przechowywaniem i zabezpieczaniem dokumentów,
- nieprzestrzegania zasad wydawania, rozliczania i obiegu dokumentów niejawnych, a także zasad kopertowania, adresowania i ekspedycji przesyłek,
- nieprzestrzeganiu zasad niszczenia dokumentów niejawnych[11],
- udostępniania materiałów niejawnych osobom nieuprawnionym (odbywa się na podstawie aktualnego wykazu osób upoważnionych do dostępu do informacji niejawnych).

W jednostkach i komórkach organizacyjnych resortu obrony narodowej przeprowadza się kontrole ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji. Realizuje się w celu:
- ustalenia stanu faktycznego realizacji zadań w zakresie ochrony informacji niejawnych i oceny przestrzegania przepisów wydanych w tym zakresie,
- określenia przyczyn i skutków ewentualnych naruszeń przepisów o ochronie informacji niejawnych oraz wskazania osób za to odpowiedzialnych,
- wskazania sposobów umożliwiających usunięcie stwierdzonych nieprawidłowości,
- sformułowania i przedłożenia przełożonym wniosków oraz zaleceń dotyczących doskonalenia systemu ochrony informacji niejawnych.

Kontrole realizuje się w formie kontroli bieżących, kontroli okresowych ewidencji, materiałów i obiegu dokumentów, tzw. „kontroli okresowych"

[11] P. Pietkowski, *Wybrane problemy bezpieczeństwa informacji niejawnych w instytucjach państwowych(na przykładzie resortu obrony narodowej)*, [w:] *Ochrona informacji niejawnych i biznesowych*. Materiały III Kongresu. Katowice 2007, s. 123.

oraz kontroli stanu zabezpieczenia informacji niejawnych. Najistotniejszą z perspektywy kancelarii tajnej jest przeprowadzana corocznie kontrola okresowa, którą przeprowadza się za dany rok kalendarzowy w pierwszym kwartale roku następnego. Jest to podstawowa forma sprawdzenia ewidencji, materiałów i obiegu dokumentów niejawnych w jednostce organizacyjnej i swoim zakresem przedmiotowym obejmuje sprawdzenie stanu przestrzegania zasad postępowania z materiałami niejawnymi w kancelariach tajnych. Polega na:

- szczegółowym sprawdzeniu stanu faktycznego materiałów niejawnych przechowywanych w kancelariach tajnych i innych komórkach, w których są przetwarzane materiały niejawne oraz porównaniu ze stanem ewidencyjnym z wyłączeniem teczek akt postępowań sprawdzających.
- sprawdzeniu przestrzegania zasad przetwarzania materiałów niejawnych.
- sprawdzeniu przestrzegania obowiązku dokumentowania faktu zapoznania się z informacjami niejawnymi oznaczonymi klauzulą „ściśle tajne" i „tajne"[12].

Podsumowanie

Resort obrony narodowej jest dobrze przygotowany do ochrony informacji niejawnych i posiada w tej materii bardzo bogate doświadczenie. Znajduje to odzwierciedlenie w organizacji i funkcjonowaniu kancelarii tajnych. Przykładem jest stałe i systematyczne dostosowywanie przepisów do zmieniającej się rzeczywistości. Poza aktami typu rozporządzenia, zarządzenia, decyzje wydawanymi na szczeblu ministerialnym, również na poziomie inspektoratów ukazują się m.in. wytyczne uszczegóławiające i dystrybuowane do jednostek podporządkowanych np. w postaci instrukcji zawierających opracowane wzory dokumentów. Ułatwia to pracę personelowi kancelarii i zmniejsza możliwość własnej interpretacji nie zawsze jednoznacznych aktów prawnych.

W zakresie bezpieczeństwa teleinformatycznego podejmowane są działania mające na celu stałe monitorowanie potencjalnych zagrożeń oraz dążenie do doskonalenia zabezpieczeń sieci teleinformatycznych przetwarzających informacje niejawne.

[12] Załącznik nr 2 do Decyzji nr 61/MON Ministra Obrony Narodowej z dnia 5 marca 2013 r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz w komórkach organizacyjnych Ministerstwa Obrony Narodowej (DZ. Urz. Min. Obr. Nar. Poz. 86).

Standardy dotyczące ochrony fizycznej wdrażane są na bieżąco zgodnie z obowiązującymi aktami normatywnymi.

Położony jest duży nacisk w zakresie teoretycznego i praktycznego przygotowania pracowników kancelarii do wykonywania obowiązków.

Temat dotyczący organizacji i funkcjonowania kancelarii tajnych jest bardzo obszerny. Z tego względu trudno ująć go w sposób wyczerpujący w jednym opracowaniu. Jednak na podstawie przedstawionych aktów prawnych można wysnuć wniosek, iż kancelarie tajne resortu obrony narodowej są dobrze przygotowane i spełniają swoją funkcję w zakresie ochrony informacji niejawnych.

Należy również podkreślić, iż ochrona informacji niejawnych nie jest procesem polegającym jedynie na jednorazowym wprowadzeniu mechanizmów zabezpieczających. Jest procesem ciągłym, wymagającym nieustannych modyfikacji, którego celem jest dążenie do osiągnięcia doskonałości w zakresie zapewnienia maksymalnej ochrony informacjom niejawnym.

Bibliografia

1. Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. (Dz. U. z 2010 r., Nr 182, poz. 1228).
2. Rozporządzenie Ministra Obrony Narodowej z dnia 19 grudnia 2013 r. w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych (Dz. U. z 2013 r., nr 0, poz. 1660).
3. Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. z 2011 r., nr 271, poz.1603).
4. *Ochrona informacji niejawnych i biznesowych.* Materiały III Kongresu. Katowice 2007.
5. Zarządzenie Nr 57/MON Ministra Obrony Narodowej z dnia 16 grudnia 2011 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych, sposobi i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego.

6. Decyzja nr 385/MON Ministra Obrony Narodowej z dnia 17 grudnia 2013 r. w sprawie wprowadzenia do użytku „Instrukcji o zasadach pracy biurowej w resorcie obrony narodowej".
7. Decyzja nr 61/MON Ministra Obrony Narodowej z dnia 5 marca 2013 r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz w komórkach organizacyjnych Ministerstwa Obrony Narodowej (Dz. Urz. MON Poz. 86)