AKADEMIA
OBRONY NARODOWEJ

Płk mgr Krzysztof BRODA

OCHRONA INFORMACJI NIEJAWNYCH W SIŁACH ZBROJNYCH RZECZYPOSPOLITEJ POLSKIEJ W ŚWIETLE WYMOGÓW BEZPIECZEŃSTWA ORGANIZACJI TRAKTATU PÓŁNOCNOATLANTYCKIEGO

Rozprawa doktorska

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid.
55871

WARSZAWA 2003

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ STRATEGICZNO – OBRONNY

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 55871
Akademii Obrony Narodowej

Płk mgr Krzysztof BRODA

OCHRONA INFORMACJI NIEJAWNYCH W SIŁACH ZBROJNYCH RZECZYPOSPOLITEJ POLSKIEJ W ŚWIETLE WYMOGÓW BEZPIECZEŃSTWA ORGANIZACJI TRAKTATU PÓŁNOCNOATLANTYCKIEGO

Rozprawa doktorska

Opracowana pod kierownictwem naukowym
prof. dr. hab. Stefana Koryckiego

WARSZAWA 2003

SPIS TREŚCI

WSTĘP 4

I. SYSTEM OCHRONY INFORMACJI NIEJAWNYCH W POLSCE 13

1. Czynniki determinujące konieczność ochrony informacji niejawnych w Polsce oraz zagrożenia dla ich bezpieczeństwa 13
2. Rys historyczny kształtowania się podstaw prawnych ochrony informacji niejawnych w Polsce 24
3. Podstawy prawne ochrony informacji niejawnych w sferze wojskowej i cywilnej 34
4. Istota informacji niejawnych, organizacja systemu ich ochrony 40

II. SYSTEM OCHRONY INFORMACJI NIEJAWNYCH W SIŁACH ZBROJNYCH RP 73

1. Kompetencje, zakres odpowiedzialności i zasady współdziałania instytucji odpowiedzialnych za bezpieczeństwo i ochronę informacji niejawnych w sferze wojskowej 73
2. Zasady ochrony fizycznej informacji niejawnych 87
3. Procedury sprawdzające przed wydaniem poświadczenia bezpieczeństwa osobowego 95
4. Regulacje dotyczące postępowań sprawdzających przed wydaniem świadectwa bezpieczeństwa przemysłowego 108
5. Bezpieczeństwo wytwarzania, przetwarzania, przechowywania i przesyłania informacji niejawnych 117
6. Działalność szkoleniowa i kontrolna w sferze ochrony informacji niejawnych 131

III. POLITYKA BEZPIECZEŃSTWA ORGANIZACJI TRAKTATU PÓŁNOCNOATLANTYCKIEGO 139

1. Główne dokumenty normatywne. Podstawowe zasady oraz minimalne standardy bezpieczeństwa 139
2. Charakterystyka organów bezpieczeństwa Sojuszu i zakresów ich odpowiedzialności 147
3. Analiza wybranych aspektów bezpieczeństwa osobowego, fizycznego, informacji, przemysłowego i teleinformatycznego 150

IV. OCENA ZGODNOSCI POLSKICH ROZWIĄZAŃ W DZIEDZINIE BEZPIECZEŃSTWA I OCHRONY INFORMACJI NIEJAWNYCH W SFERZE WOJSKOWEJ ZE STANDARDAMI NATO 175

1. Prowadzenie postępowań sprawdzających przed wydaniem poświadczenia bezpieczeństwa osobowego 175
2. Stosowanie fizycznych środków ochrony informacji niejawnych 182
3. Wytwarzanie, obieg i niszczenie dokumentów niejawnych 184
4. Prowadzenie postępowań sprawdzających przed wydaniem świadectwa bezpieczeństwa przemysłowego 187
5. Ochrona informacji niejawnych w systemach i sieciach teleinformatycznych 190

UWAGI KOŃCOWE 194

BIBLIOGRAFIA 206

ZAŁĄCZNIKI 214

WSTĘP

W 1999 roku Polska stała się członkiem organizacji Traktatu Północnoatlantyckiego. W czasie przygotowywania do wstąpienia do NATO, określanego jako proces akcesyjny kraj nasz musiał dokonać istotnych regulacji prawnych oraz zmian organizacyjnych w wielu sferach jak np. w administracji publicznej czy strukturze Sił Zbrojnych.

Procesowi dostosowywania do wymogów Sojuszu podlegał też system ochrony informacji niejawnych, wytwarzanych w kraju, wymienianych z innymi państwami tak należącymi do NATO, objętymi Planem Członkostwa[1], programem Partnerstwa dla Pokoju[2] jak również pozostającymi poza strukturami Paktu.

Należy podkreślić, że Polska dokonała dużego wysiłku legislacyjnego i organizacyjnego w tym procesie. W bardzo krótkim czasie sfinalizowano prace legislacyjne nad Ustawą o ochronie informacji niejawnych[3] i w momencie formalnego akcesu do Sojuszu kraj nasz posiadał nową ustawę, kompatybilną z tego typu aktami obowiązującymi w państwach sojuszniczych oraz dokumentami normującymi kwestie szeroko pojętego bezpieczeństwa w Organizacji Traktatu Północnoatlantyckiego. Jednocześnie w resorcie obrony narodowej rozpoczęto prace nad opracowaniem niezbędnych aktów wykonawczych, które uzupełniły system normujący sprawy bezpieczeństwa i ochrony informacji niejawnych w Siłach Zbrojnych. Dwuletnia praktyka wykazała jednak konieczność nowelizacji przyjętych aktów prawnych. Zmiany w Ustawie o ochronie informacji niejawnych, które pod koniec 2000 roku zostały zaproponowane przez ówczesne służby ochrony

---

[1] Plan Członkostwa *(ang. Membership Action Plan)* to funkcjonujący od 1999 roku system rozwiązań organizacyjnych i prawnych, którego celem jest przygotowanie państw kandydujących do członkostwa do funkcjonowania w strukturach Organizacji Traktatu Północnoatlantyckiego. Istotnym elementem procesu akcesyjnego jest stworzenie legislacyjnych i funkcjonalnych podstaw systemu ochrony informacji niejawnych, odpowiadającego wymogom bezpieczeństwa, które obowiązują wszystkie państwa członkowskie.

[2] Partnerstwo dla Pokoju *(ang. Partnership for Peace)* to wdrożony w 1994 roku natowski program współpracy i wymiany doświadczeń z państwami partnerskimi, nie objętymi Planem Członkostwa.

[3] Dz. U. z 1999 roku, Nr 11, poz. 95 z późniejszymi zmianami. Ilekroć w dalszej części pracy używany jest termin „ustawa" odnosi się on do Ustawy o ochronie informacji niejawnych.

państwa, Urząd Ochrony Państwa[4] i Wojskowe Służby Informacyjne, weszły w życie 08 kwietnia 2001r. Nowelizacja ta niejako zamknęła okres budowy podstaw prawnych w tej dziedzinie. Jednakże stworzony system prawny nie mógł być i nie jest doskonały. Jednym z podstawowych obowiązków służb ochrony państwa jest jego stałe dostosowywanie do zmieniających się warunków ochrony informacji niejawnych. Dlatego też zmiany w Ustawie o ochronie informacji niejawnych i w przepisach wykonawczych do niej są w przyszłości nieuniknione.

Podkreślić należy, że sfera bezpieczeństwa i ochrony informacji niejawnych jest dziedziną, która pozostaje w stałym zainteresowaniu władz politycznych i wojskowych Organizacji Traktatu Północnoatlantyckiego. Dokumenty normatywne NATO wydane po raz pierwszy w 1955 roku są okresowo uaktualniane. W 2002 roku sfinalizowany został kolejny etap ich modyfikacji i dostosowywania do aktualnej sytuacji, z uwzględnieniem zmieniających się warunków funkcjonowania Sojuszu i nowych pojawiających się zagrożeń w sferze bezpieczeństwa. W pracach Komitetu Bezpieczeństwa[5] i grup roboczych NATO, zajmujących się opracowaniem wspomnianych dokumentów brali udział przedstawiciele Wojskowych Służb Informacyjnych, w tym autor niniejszej rozprawy.

Przedstawione okoliczności upoważniają do podjęcia wysiłku w celu naukowego opracowania tematu kształtowania się całkowicie nowego modelu ochrony informacji niejawnych w Polsce, analizy problemów, które pojawiły się w ciągu czterech lat funkcjonowania systemu i oceny czy przyjęte standardy spełniają wymogi stawiane w tej dziedzinie przez politykę bezpieczeństwa Sojuszu. Bazą ocen i rozważań był stan prawny, jaki obowiązywał w Polsce i w Organizacji Traktatu Północnoatlantyckiego na dzień 22 stycznia 2003 roku.

Analiza dostępnych materiałów źródłowych i zgromadzonych faktów, istotnych dla procesu poznania pozwoliła na sprecyzowanie i osiągnięcie w niniejszej rozprawie następujących celów badań:

---

[4] Do czasu powołania Agencji Bezpieczeństwa Wewnętrznego, w lipcu 2002 roku, służbą ochrony państwa był Urząd Ochrony Państwa.

[5] Organ NATO odpowiadający za kształtowanie polityki NATO w sferze ochrony informacji niejawnych, składający się z reprezentantów Krajowych Władz Bezpieczeństwa państw członkowskich. Zwoływany dwa razy do roku.

- analiza systemu ochrony informacji niejawnych w Polsce a zwłaszcza w Siłach Zbrojnych RP oraz omówienie procesu jego budowy w procesie przystosowawczym do funkcjonowania naszego kraju w NATO;
- analiza podstawowych zasad i standardów ochrony informacji niejawnych w Organizacji Traktatu Północnoatlantyckiego;
- analiza rozwiązań wprowadzonych mocą Ustawy o ochronie informacji niejawnych oraz aktów wykonawczych w sferze bezpieczeństwa w dziedzinie obronności[6] i określenie stopnia ich zgodności z rozwiązaniami obowiązującymi wszystkie państwa członkowskie Sojuszu;
- ocena skuteczności systemu i mechanizmów ochrony informacji niejawnych w sferze wojskowej.

Cele te osiągnięto poprzez realizację poniższych celów szczegółowych:

- określenie obiektywnych przyczyn determinujących potrzebę ochrony informacji niejawnych w państwie i w Siłach Zbrojnych RP;
- ustalenie, w jaki sposób rozwijał się proces budowy podstaw prawnych ochrony informacji niejawnych, w tym w czasie procesu akcesyjnego do NATO;
- analiza procesu doskonalenia regulacji prawnych, dotyczących ochrony informacji niejawnych w latach 1999 – 2003;
- sprecyzowanie istoty informacji niejawnych, stanowiących niejako jądro, wokół którego zbudowany został system zapewniający skuteczną ich ochronę;
- charakterystyka zasad i procedur związanych z ochroną informacji niejawnych w Siłach Zbrojnych RP;
- analiza postanowień dokumentów normatywnych i regulacji w sferze ochrony informacji niejawnych, ustanowionych w Organizacji Traktatu Północnoatlantyckiego;

---

[6] Pojęcia dziedzina obronności czy używane alternatywnie sfera wojskowa odnoszą się do Sił Zbrojnych RP, ich jednostek organizacyjnych, przedsiębiorców, jednostek naukowych i badawczo – rozwojowych, pozostających w kompetencjach ministra obrony narodowej lub realizujących niejawne kontrakty bądź usługi związane z obronnością państwa i potrzebami sił zbrojnych.

- ustalenie zgodności mechanizmów, norm i zasad ustanowionych mocą polskiego prawa z zaleceniami zawartymi w dokumentach natowskich, dotyczących ochrony informacji niejawnych;
- dokonanie oceny polskich rozwiązań pod kątem zapewnienia skuteczności ochrony informacji niejawnych w Siłach Zbrojnych RP;
- sprecyzowanie zaleceń dotyczących zmian w systemie prawnym, które zwiększyłyby skuteczność funkcjonowania systemu ochrony informacji niejawnych w Siłach Zbrojnych RP.

Główny problem badawczy ujęty został w taki sposób, aby jego rozwiązanie dało odpowiedź na pytanie czy polskie regulacje prawne dotyczące bezpieczeństwa i ochrony informacji niejawnych odpowiadają rozwiązaniom w sferze bezpieczeństwa, określonym w dokumentach normatywnych Sojuszu i czy zapewniają skuteczną ochronę informacji niejawnych, w tym pochodzących z wymiany międzynarodowej, w Siłach Zbrojnych RP. Rozważania teoretyczne zostały wsparte oceną doświadczeń, nabytych w czasie współpracy przedstawicieli Wojskowych Służb Informacyjnych z Komitetem Bezpieczeństwa, Biurem Bezpieczeństwa NATO[7] i przedstawicielami Krajowych Władz Bezpieczeństwa państw członkowskich Sojuszu.

Biorąc za punkt wyjścia przedstawione cele pracy i treść głównego problemu naukowego sformułowane zostały następujące problemy szczegółowe:

- jak jest zorganizowany system ochrony informacji niejawnych w Siłach Zbrojnych RP;
- w jaki sposób Wojskowe Służby Informacyjne jako służba ochrony państwa w dziedzinie wojskowej wypełniają zadania określone przez naczelne władze państwowe w sferze bezpieczeństwa informacji niejawnych;
- w jakim stopniu polskie rozwiązania spełniają wymogi polityki bezpieczeństwa Organizacji Traktatu Północnoatlantyckiego zawarte w dokumentach normatywnych, obowiązujących w NATO;

[7] Etatowy organ NATO odpowiadający za ochronę informacji niejawnych w NATO i przestrzeganie przepisów w tym zakresie przez państwa członkowskie.

- czy polski system ochrony informacji niejawnych w sferze wojskowej jest akceptowany przez Komitet Bezpieczeństwa i Biuro Bezpieczeństwa NATO?
- jakie są perspektywy rozwoju systemu ochrony informacji niejawnych w sferze wojskowej?

W następstwie poszukiwania odpowiedzi na wymienione pytania uzyskano zbiory faktów oparte na analizie dostępnej literatury, aktów prawnych oraz danych, dotyczących ilości przeprowadzonych procedur sprawdzających w sferze bezpieczeństwa osobowego, przemysłowego, teleinformatycznego, certyfikacji i działalności kontrolnej.[8]

Rozważania podjęte w pracy ograniczone są zakresem podmiotowym, przedmiotowym i czasowym. Zakres podmiotowy stanowiły prawne podstawy funkcjonowania systemu ochrony informacji niejawnych w Polsce, w sferze wojskowej oraz praktyczne aspekty jego funkcjonowania. Równolegle istotnym polem rozważań była ocena zgodności systemu z rozwiązaniami modelowymi, zalecanymi przez NATO.

Zakres przedmiotowy stanowiły problemy skuteczności systemu, przede wszystkim uogólnienie osobistych doświadczeń autora, związanych z wykonywaniem przez Wojskowe Służby Informacyjne zadań służby ochrony państwa a przez szefa Wojskowych Służb Informacyjnych zadań Krajowej Władzy Bezpieczeństwa w relacjach międzynarodowych.

Zakres czasowy, objęty badaniami to głównie lata 1999 – 2003. Przedział ten determinowały początki funkcjonowania systemu ochrony informacji niejawnych w Polsce i w Siłach Zbrojnych RP oraz termin zakończenia prac organów bezpieczeństwa Sojuszu nad nowymi dokumentami, regulującymi całokształt polityki bezpieczeństwa NATO.

Istotnym ograniczeniem prowadzonych badań był fakt, iż literatura dotycząca tematu pracy jest wyjątkowo uboga. Pozycje, które dotychczas ukazały się na rynku to głównie przedruki aktów prawnych opatrzone krótkim komentarzem. Dlatego też głównymi źródłami pracy były polskie akty prawne o

[8] Wymienione sfery bezpieczeństwa zostały omówione w Rozdziale II.

randze ustawy, akty wykonawcze do tych ustaw, zwłaszcza przyjęte w resorcie obrony narodowej oraz jawne dokumenty normatywne Wojskowych Służb Informacyjnych. Oprócz źródeł krajowych istotną pozycję w bibliografii stanowiły jawne dokumenty normatywne NATO, regulujące sprawy bezpieczeństwa i ochrony informacji niejawnych w Organizacji Traktatu Północnoatlantyckiego.

Równie ważnym ograniczeniem w prowadzonych badaniach był brak możliwości wykorzystania informacji opatrzonych klauzulą tajności, takich jak dane ewidencyjne dotyczące służb ochrony państwa, statystyczne, dotyczące ilości przeprowadzonych postępowań czy analityczne, traktujące o efektywności funkcjonowania tych służb. Pomimo tego, iż sfera ochrony informacji niejawnych jest jawną dziedziną funkcjonowania Agencji Bezpieczeństwa Wewnętrznego i Wojskowych Służb Informacyjnych to pamiętać trzeba, że instytucje te jako służby specjalne zajmują się działalnością o charakterze niejawnym, w tym zwłaszcza wywiadowczą i kontrwywiadowczą. Dokonywanie ocen efektywności, analiz czy porównań tych dwu służb nie mogło być przeprowadzone w niniejszej pracy, bowiem intencją autora było opracowanie jawnej rozprawy naukowej, posiadającej praktyczny wymiar, dostępnej dla szerokiego kręgu odbiorców: żołnierzy i funkcjonariuszy służb ochrony państwa, kierowników jednostek organizacyjnych i pełnomocników ochrony informacji niejawnych.

Uwzględniając sprecyzowane ograniczenia, w osiągnięciu założonych celów rozprawy pomocnym było postawienie następujących hipotez roboczych:

1. System ochrony informacji niejawnych w Polsce, w tym w Siłach Zbrojnych Rzeczypospolitej Polskiej posiada niezbędną bazę normatywną, ujmującą wszystkie aspekty bezpieczeństwa (osobowego, fizycznego, przemysłowego, teleinformatycznego);
2. Polskie, narodowe rozwiązania w sferze wojskowej spełniają, a w niektórych dziedzinach nawet przewyższają, wymogi zawarte w instrukcjach, dyrektywach i wytycznych NATO w dziedzinie ochrony informacji niejawnych;
3. Sprawne funkcjonowanie systemu zapewniają właściwie zorganizowane i współpracujące ze sobą instytucje cywilne i wojskowe oraz właściwy

poziom wiedzy i tzw. „kultury bezpieczeństwa" zarówno osób wytwarzających dokumenty niejawne jak i osób funkcyjnych, odpowiedzialnych za sprawy ich bezpieczeństwa.

Hipotezy te zostały poddane weryfikacji w rozprawie, mającej charakter studium analityczno – empirycznego, którego rozważania koncentrowały się na dwóch płaszczyznach dociekań:

- teoretyczno – metodologicznej;
- praktyczno – empirycznej.

Dociekania podjęte na płaszczyźnie teoretyczno – metodologicznej dotyczyły określenia obszarów szeroko pojętego bezpieczeństwa w Polsce i Siłach Zbrojnych, identyfikacji przyjętych rozwiązań w jego wszystkich sferach oraz ich oceny przez pryzmat zapewnienia bezpieczeństwa informacji, stanowiących głównie tajemnicę państwową. Płaszczyznę praktyczno - empiryczną stanowiło studium analityczne zgodności systemu z natowskimi standardami i ocena jego sprawności funkcjonalnej.

Przyjętą metodologię badań determinowały cele pracy i podjęte problemy badawcze. Zasadniczą metodą była analiza dokumentów normatywnych w sferze bezpieczeństwa, obowiązujących wszystkie państwa członkowskie NATO i norm ustanowionych w naszym kraju. Główny nacisk położono na analizę dokumentów obowiązujących w sferze wojskowej.

Badania wstępne, w oparciu o które sformułowany został problem badawczy obejmowały:

- analizę literatury i dostępnych materiałów dotyczących problematyki rozprawy;
- analizę danych statystycznych dotyczących ilości przeprowadzonych procedur sprawdzających w sferze bezpieczeństwa osobowego, fizycznego, przemysłowego i teleinformatycznego;

Na etapie badań wstępnych zastosowano takie metody badawcze jak: analiza, synteza, analogia, ilościowe i jakościowe ujmowanie problemów, porównanie i uogólnienie. Na kolejnych etapach procesu badawczego, w czasie weryfikacji poszczególnych hipotez zastosowano takie metody jak analiza,

porównanie, definiowanie, interpretacja i wnioskowanie. W rozprawie zastosowano różne metody badawcze, ponieważ nie ma jednej, uniwersalnej metody badawczej, która miałaby zastosowanie do zbadania wszystkich niuansów problematyki podjętej w niniejszej pracy. Wydaje się, iż zastosowane metody, techniki i narzędzia badawcze były wystarczające do rozwiązania podjętych w rozprawie problemów naukowych.

Z naukowego punktu widzenia temat rozprawy jest jak najbardziej aktualny. Mam nadzieję, że praca pozwoli wielu osobom zwłaszcza zaangażowanym profesjonalnie w sprawy ochrony informacji niejawnych uporządkować i rozszerzyć posiadaną wiedzę a osobom nie mającym zawodowo styczności z jej tematem zainteresuje je.

Praca składa się ze wstępu, w którym omówiono problemy metodologiczne, cele badań, problemy naukowe, hipotezy robocze, metody i techniki badawcze, czterech rozdziałów, uwag końcowych i załączników.

W rozdziale pierwszym, zatytułowanym **„System ochrony informacji niejawnych w Polsce"** przedstawione zostały problemy dotyczące historycznych aspektów kształtowania się obecnego modelu bezpieczeństwa i ochrony informacji w Polsce. Zdefiniowane zostały obiektywne zjawiska (konieczność dostosowania systemu ochrony informacji niejawnych do standardów NATO i zagrożenia dla bezpieczeństwa informacji ze strony obcych służb specjalnych), które spowodowały potrzebę ukształtowania nowego modelu ochrony informacji niejawnych. Oprócz tego analizie zostały poddane akty prawne i kwestia odpowiedzialności organów państwa za ochronę informacji niejawnych.

Rozdział drugi, pod tytułem **„System ochrony informacji niejawnych w Siłach Zbrojnych RP"** poświęcony jest bezpieczeństwu i ochronie informacji w sferze wojskowej. Szczegółowo przedstawione zostały zarówno wymogi aktów normatywnych jak i dotychczasowe doświadczenia związane z funkcjonowaniem systemu w sferze bezpieczeństwa osobowego, fizycznego, przemysłowego, teleinformatycznego, działalności kontrolnej i szkoleniowej.

Trzeci rozdział, zatytułowany **„Polityka bezpieczeństwa Organizacji Traktatu Północnoatlantyckiego"** traktuje o wybranych aspektach bezpieczeństwa

i ochrony informacji niejawnych w NATO. Szczegółowo omówione zostały postanowienia jawnych dokumentów normatywnych, obowiązujące wszystkie państwa członkowskie.

W czwartym rozdziale pod tytułem **„Ocena zgodności polskich rozwiązań w dziedzinie bezpieczeństwa i ochrony informacji niejawnych w sferze wojskowej ze standardami NATO"** określone zostały elementy spójne rozwiązań natowskich i polskich norm bezpieczeństwa w sferze wojskowej. Dokonana została ocena zdolności Sił Zbrojnych RP do ochrony narodowych i sojuszniczych informacji niejawnych oraz informacji wymienianych w kontaktach dwustronnych z innymi państwami.

Na bazie dokonanej analizy zgodności narodowych rozwiązań i rozwiązań wynikających z polityki bezpieczeństwa NATO, w uwagach końcowych zostały zaproponowane zmiany w Ustawie o ochronie informacji niejawnych, które zbliżyłyby polskie standardy, w tym obowiązujące w Siłach Zbrojnych RP, do rozwiązań istniejących w Organizacji Traktatu Północnoatlantyckiego.

Pragnę serdecznie podziękować promotorowi – prof. dr hab. Stefanowi Koryckiemu za cenne uwagi i sugestie dotyczące zarówno merytorycznych jak i metodologicznych aspektów mojej rozprawy. Wierzę, że wysiłek włożony w przygotowanie niniejszej rozprawy przyczyni się do zrozumienia istoty, konieczności i mechanizmów ochrony informacji niejawnych w Polsce a zwłaszcza w Siłach Zbrojnych RP.

ROZDZIAŁ I

SYSTEM OCHRONY INFORMACJI NIEJAWNYCH W POLSCE

1. Czynniki determinujące konieczność ochrony informacji niejawnych w Polsce oraz zagrożenia dla ich bezpieczeństwa.

Z funkcjonowaniem każdego państwa i jego wewnętrznych organów a zwłaszcza sił zbrojnych wiąże się konieczność ochrony informacji o różnym stopniu poufności, ujawnienie których mogłoby się okazać szkodliwe dla interesów wszystkich obywateli czy dla sprawnego działania władz państwowych i samorządowych lub firm państwowych bądź komercyjnych. Dlatego w każdym kraju niezależnie od etapu jego historycznego rozwoju czy geograficznego położenia informacje niejawne są chronione z mocy prawa. Nigdy bowiem tak nie było i być nie mogło aby jakikolwiek organizm państwowy mógł żyć swoim niezależnym bytem w oderwaniu od sąsiadów, międzynarodowej konkurencji, sojuszy, wolny od konfliktów zbrojnych i wewnętrznych zagrożeń.

Polska była w ostatnich latach ważnym podmiotem przemian na arenie międzynarodowej, inicjatorem demokratycznej transformacji w Europie Środkowo – Wschodniej. W jej wyniku odzyskaliśmy suwerenność, staliśmy się niezależnym państwem, przed którym pojawiło się wiele wyzwań. Apogeum tych jakościowych zmian osiągnęliśmy w 1999 roku przystępując do Organizacji Traktatu Północnoatlantyckiego. Akces ten wymagał gruntownej przebudowy systemu ochrony informacji niejawnych, wprowadzenia nowych standardów bezpieczeństwa i zmiany mentalności osób, które mają do czynienia z informacjami stanowiącymi tajemnicę państwową bądź służbową. Nie możemy powiedzieć jednoznacznie czy poprzedni system ochrony tajemnicy państwowej i służbowej był gorszy czy lepszy. Był po prostu inny tak jak inne było państwo.

Oceniając, jakie czynniki wpływają obecnie na potrzebę budowy skutecznego systemu ochrony informacji niejawnych należy brać pod uwagę szereg uwarunkowań. W przypadku Polski należy uwzględniać, iż:

- przystępując do NATO, Polska zobowiązała się do zorganizowania efektywnego systemu ochrony sojuszniczych informacji co znalazło wyraz w ratyfikacji, w dniu 27 maja 1999 roku „Umowy między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzonej w Brukseli dnia 06 marca 1997 roku" *(ang. Security Agreement between the Parties to the North Atlantic Treaty for the Security of Information)*[9];
- Polska jest obok Czech i Węgier najmłodszym członkiem NATO, posiadającym jeszcze niezbyt dużo doświadczenia w budowie efektywnych mechanizmów bezpieczeństwa informacji niejawnych. Aby sprostać sojuszniczym standardom należy więc z determinacją budować i doskonalić system ochrony informacji niejawnych;
- Polska jest krajem granicznym Paktu, narażonym na bezpośrednie oddziaływanie innych państw, w tym Rosji, które przez lata były definiowane przez Radę Północnoatlantycką jako największe „niebezpieczeństwo" dla tej organizacji. Pomimo znacznej poprawy stosunków NATO-Rosja, zwłaszcza po atakach terrorystycznych na Stany Zjednoczone, we wrześniu 2001 roku, musimy się ciągle liczyć z realnymi zagrożeniami ze strony tego kraju;
- Polska jest zainteresowana rozwojem dobrosąsiedzkich kontaktów ze wszystkimi krajami Europy a zwłaszcza Europy Środkowo – Wschodniej. Rozwojowi kontaktów zawsze towarzyszy wymiana informacji. Musi więc istnieć balans pomiędzy wymogami bezpieczeństwa, które stawia przed Polską członkostwo w NATO a narodowymi interesami naszego kraju związanymi z budową kontaktów międzynarodowych, w tym w sferze wojskowej;

---

[9] Jednolita treść Umowy została ogłoszona w Dz. U. z 2000 roku Nr 64, poz. 740. Postanowienia Umowy są omówione w Rozdziale III.

- położenie geopolityczne Polski jest wyjątkowo niekorzystne. W przypadku jakiegokolwiek konfliktu zbrojnego tak globalnego jak i o wymiarze lokalnym, w Europie, obszar naszego kraju może być objęty działaniami zbrojnymi. Dlatego musimy liczyć się z faktem rozpoznawania naszego terytorium na wypadek przyszłych działań wojennych.

Uwzględniając powyższe, obiektywne przesłanki można zdefiniować następujące zewnętrzne zagrożenia dla narodowych i sojuszniczych informacji niejawnych:

a. działalność wywiadowcza obcych służb specjalnych;

O tym, że każde państwo niezależnie od swego potencjału ekonomicznego czy militarnego prowadzi działalność wywiadowczą, skierowaną przeciwko innym krajom nie trzeba nikogo przekonywać. Jest to aksjomat funkcjonowania każdej formy państwowości. Wywiad znany był już w starożytności, rozwinął się w epoce wojen napoleońskich a jego szczególny rozwój nastąpił w czasach współczesnych, podczas dwu światowych wojen a zwłaszcza potem, w okresie zimnej wojny. Jak zdefiniować wywiad? Oto jedna z dostępnych definicji:

Wywiad – instytucja państwowa mająca za zadanie zdobywanie i analizowanie **tajnych** informacji dotyczących polityki, wojskowości i gospodarki innych państw.[10]

Definicja ta podkreśla instytucjonalny charakter wywiadu jako organizmu państwowego o określonej strukturze. Wywiad oznacza również działalność prowadzoną przez wyspecjalizowane komórki w celu zdobywania informacji. Zdobywanie tych informacji odbywa się w różny sposób. Może być to tak zwany wywiad biały, polegający na zbieraniu informacji zawartych w prasie i wszelkiego rodzaju publikacjach. Jest to bardzo skuteczna metoda, bowiem często dzięki dziennikarzom wiele szczątkowych informacji jest dostępnych w środkach masowego przekazu. Ich połączenie i umiejętna analiza dostarczają wielu ciekawych wniosków. Jest też inny wywiad, ten polegający na tworzeniu siatek

[10]Popularna Encyklopedia Powszechna, Wyd. Pinnex, Kraków 1998, tom 21 str. 94.

agentów w innych krajach, zdobywaniu informacji z naruszeniem prawa państwa, w którym działalność wywiadowcza jest prowadzona. Ten wywiad określany jako agenturalny stanowi o istocie działalności wywiadowczej, jest kosztowny, niebezpieczny a przede wszystkim nielegalny. Agenci wywiadu, w swoich krajach określani jako szpiedzy dostarczają do 5% ogółu zdobywanych przez wywiad informacji, jednak jak się ocenia są to informacje najcenniejsze, strategiczne i pewne. Mówiąc o metodach pracy wywiadowczej należy podkreślić, że żadne państwo nie przyznaje się otwarcie do prowadzenia działalności wywiadowczej przeciwko jakiemukolwiek innemu podmiotowi prawa międzynarodowego. Natomiast faktem jest, iż ogromne środki finansowe są przeznaczane na działalność wywiadowczą a takie organizacje jak rosyjskie GRU[11] czy amerykańska CIA[12] to prawdziwe potęgi, które są w stanie skutecznie rozpoznawać wszelkie sfery życia publicznego wielu państw i wpływać na ich losy.

Służby wywiadowcze są organizacjami o wysokim stopniu specjalizacji. Dlatego możemy dzisiaj mówić o wywiadzie:

- politycznym – zbierającym informacje na temat polityków, organizacji politycznych, tendencji rozwojowych w kształtowaniu się doktryn polityczno - obronnych, działalności opozycyjnej, informacje o ruchach dysydenckich, pacyfistycznych czy antyrządowych;
- gospodarczym – zdobywającym dane na temat ekonomicznego potencjału państwa, wskaźników makroekonomicznych, międzynarodowej współpracy gospodarczej, tendencji rozwojowych i możliwości wytwórczych, zasobach bogactw naturalnych, stanie finansów kraju zainteresowania;
- naukowym bądź technologicznym – gromadzącym informacje o ośrodkach naukowo – badawczych i prowadzonych w nich pracach, o potencjale naukowym danego państwa i trendach w rozwoju nauki, w tym myśli wojskowej;

---

[11] Główny Zarząd Rozpoznania *(ros. Gławnoje Razwiedywatielnoje Uprawlienije)* jest centralnym organem rosyjskiego wywiadu wojskowego, skutecznie przez lata rywalizującym z wywiadem cywilnym.

[12] Centralna Agencja Wywiadowcza *(ang. Central Intelligence Agency)* jest potężną, dysponującą ogromnymi środkami finansowymi agencją wywiadu cywilnego Stanów Zjednoczonych.

- wojskowym – zajmującym się siłami zbrojnymi, strukturą i kadrami armii, jej zdolnością do obrony terytorium, możliwościami mobilizacyjnymi, sojuszami wojskowymi, stanem nastrojów wśród żołnierzy.

Oprócz wymienionych, tradycyjnych pól zainteresowania wywiadu pojawiają się coraz to nowe dziedziny, jak na przykład wywiad komputerowy. Gwałtowny rozwój informatyki i Internetu spowodował powstanie wyspecjalizowanych ośrodków wywiadowczych starających się poznać informacje wytwarzane w systemach i sieciach teleinformatycznych oraz wniknąć w tajne systemy komputerowe państwa czy jego sił zbrojnych.

Jest oczywistym, iż działalność wywiadowcza wiąże się nierozerwalnie ze zdobywaniem prawnie chronionych informacji niejawnych innego państwa. Rozważając sytuację Polski i zagrożenia ze strony obcego wywiadu można śmiało postawić tezę, iż kraj nasz jest obiektem intensywnych działań wywiadowczych, ukierunkowanych na zdobywanie narodowych informacji, stanowiących tajemnicę państwową a także informacji niejawnych NATO, które są powierzane Polsce w związku z wykonywaniem sojuszniczych zobowiązań. Najbardziej narażonymi na działalność prowadzoną przez kadrowych pracowników obcego wywiadu i ich agentów wobec naszego kraju są:

- przedstawiciele władz zwłaszcza szczebla centralnego, mający zarówno dużą wiedzę o największych tajemnicach Polski jak również decydujący o najważniejszych sprawach dotyczących rozwoju kraju we wszystkich dziedzinach (polityka zagraniczna, administracja, sfera obronności, etc.);
- pracownicy ośrodków naukowych i analitycznych, dysponujący nieocenioną wiedzą na temat nowoczesnych technologii, stosowanych w gospodarce i Siłach Zbrojnych RP;
- osoby mające z tytułu wykonywanego zawodu naturalny dostęp do informacji, w tym niejawnych, o najważniejszych wydarzeniach, jak na przykład dziennikarze, mający jednocześnie możliwość oddziaływania na opinię publiczną;

- pracownicy służb specjalnych, będący nośnikami informacji najbardziej chronionych w państwie, do których zaliczyć można dane dotyczące rozpoznania działalności obcego wywiadu i jego agentury na terenie Polski;
- wyżsi dowódcy Sił Zbrojnych RP i kadra posiadająca wiedzę o sprawach mobilizacyjnego rozwinięcia armii, kierunkach jej rozwoju, doktrynie obronnej.

Ocenia się, że polska armia jest obiektem szczególnego zainteresowania obcego wywiadu. Siły zbrojne są bowiem ze swej natury dysponentem wielu tajemnic, najważniejszym ogniwem decydującym o zdolności kraju do obrony jego suwerenności. Jeśli dodamy do tego fakt, iż armia polska od 1999 roku jest armią natowską, to naturalnym wydaje się wzrost zainteresowania obcych służb specjalnych takimi sprawami jak proces adaptacji do nowych warunków funkcjonowania w organizacji sojuszniczej, wyposażanie w nowe uzbrojenie, realizacja inwestycji finansowanych przez NATO na rzecz polskich Sił Zbrojnych na terenie kraju czy stosunek polskich żołnierzy do udziału we wspólnych, sojuszniczych akcjach zbrojnych, takich jak na przykład na Bałkanach czy w Afganistanie. Biorąc powyższe pod uwagę celowym wydaje się wyszczególnienie, jakie struktury armii i jakie osoby funkcyjne są szczególnie zagrożone przez obcy wywiad. Należą do nich:

- jednostki (komórki) organizacyjne resortu obrony narodowej a zwłaszcza Sztab Generalny WP, dowództwa i sztaby okręgów wojskowych i rodzajów sił zbrojnych;
- obiekty wojskowych służb specjalnych.

Osoby funkcyjne wymienionych struktur Wojska Polskiego, posiadające dostęp do najważniejszych dla obronności tajemnic będą zawsze obiektem zainteresowania obcego wywiadu. Jakkolwiek nie jest wykluczone, iż oficerowie czy nawet podoficerowie i chorążowie pracujący na niższych szczeblach są również inwigilowani. Praktyka działalności wywiadowczej pokazuje bowiem, że każdy może być przydatny obcemu wywiadowi, jeśli nie w danej chwili to być może w przyszłości.

Z działalnością obcych służb specjalnych wiążą się nierozerwalnie inne zagrożenia dla bezpieczeństwa informacji niejawnych takie jak dywersja czy sabotaż. Są to niezwykle groźne zjawiska, typowe dla prowadzonych pomiędzy państwami działań wojennych a często realizowane przez wyspecjalizowane oddziały wojskowe takie jak na przykład rosyjski SPECNAZ[13]. Ukierunkowane są na osłabienie nieprzyjaciela poprzez dezorganizację jego systemu dowodzenia, zaopatrzenia, łączności, komunikacji, zniszczenie bądź uszkodzenie ważnych obiektów, głównie realizujących produkcję zbrojeniową. Należy brać pod uwagę fakt, iż technika działania służb specjalnych w czasie działań wojennych będzie skuteczną wówczas, gdy obiekty ataków dywersyjnych i sabotażowych będą wszechstronnie rozpoznane w czasie pokoju oraz gdy przygotowani zostaną agenci zdolni do wykonania zadań sabotażowych w czasie bezpośrednich działań zbrojnych. Zagrożenie to należy uwzględniać przy ochronie obiektów specjalnych Sił Zbrojnych a także przy doborze i wszechstronnym sprawdzaniu osób pracujących w tych kluczowych dla państwa obiektach.

b. działalność terrorystyczna;

Terroryzm jest zjawiskiem niezwykle groźnym dla każdego organizmu państwowego. Istnieje mnóstwo określeń, starających się ująć najbardziej istotne aspekty tego zjawiska. Oto jedna z dostępnych definicji:

Taktyka ugrupowań ekstremistycznych wypływająca z przesłanek politycznych, religijnych, ideologicznych, narodowościowych polegająca na stosowaniu przemocy nie tylko wobec władzy lub przeciwników terrorysty, lecz wobec całego społeczeństwa w celu osiągnięcia korzyści politycznych lub zwrócenia na siebie uwagi opinii publicznej.[14]

Terroryzm jest znany od zarania dziejów, stosunkowo dużego znaczenia nabrał w XIX wieku a jego najbardziej znaną wówczas formą był anarchizm. W XX wieku stał się ulubioną metodą ruchów lewackich i lewicowych a także

---

[13] Oddziały formacji SPECNAZ *(ros. Specjalnowo Naznaczenija)* należą do najlepiej wyszkolonych jednostek, przeznaczonych do działalności dywersyjnej, sabotażowej i rozpoznawczej na tyłach przeciwnika.
[14] Popularna Encyklopedia Powszechna, Wyd. Pinnex, Kraków 1998, tom 19, str. 146.

wyzwoleńczych. Takie nazwy jak RAF[15], Czerwone Brygady[16], IRA[17], stały się sztandarowymi formacjami światowego terroryzmu, niezwykle groźnymi nie tylko dla państw, w których się narodziły. Kraje takie jak Hiszpania, Irlandia, Izrael na co dzień doświadczały i doświadczają nadal zagrożeń ze strony terrorystycznych organizacji.

11 września 2001 roku to kamień milowy w niechlubnych dziejach światowego terroryzmu. Niespotykany w całej dotychczasowej historii, bezprecedensowy i barbarzyński atak terrorystów islamskich na Stany Zjednoczone *(Centrum Handlu Światowego, Pentagon)* został zdecydowanie potępiony przez społeczność międzynarodową a przez państwa NATO potraktowany jako atak na cały Sojusz. NATO po raz pierwszy w historii odwołało się formalnie do zasady wzajemnej obrony, zawartej w art. 5 Traktatu Waszyngtońskiego, stanowiącym, iż:

... Strony zgadzają się, że zbrojna napaść na jedną lub kilka z nich w Europie lub Ameryce Północnej będzie uważana za napaść przeciwko nim wszystkim; wskutek tego zgadzają się one na to, że jeżeli taka zbrojna napaść nastąpi, każda z nich, w wykonaniu prawa do indywidualnej lub zbiorowej samoobrony, uznanego przez artykuł 51 Karty Narodów Zjednoczonych, udzieli pomocy Stronie lub Stronom tak napadniętym, podejmując natychmiast indywidualnie i w porozumieniu z innymi Stronami taką akcję, jaka uzna za konieczną, nie wyłączając użycia siły zbrojnej, w celu przywrócenia i utrzymania bezpieczeństwa obszaru północnoatlantyckiego...[18].

Na szczycie NATO w Pradze, w listopadzie 2002 roku, przywódcy państw członkowskich zaakceptowali opracowaną w Sojuszu Koncepcję walki z terroryzmem,[19] systematycznie dokonywana jest ocena zagrożeń ze strony terroryzmu dla całego Paktu i poszczególnych państw członkowskich.

---

[15] RAF *(niem. Rote Armee Fraktion)* – Frakcja Czerwonej Armii, zachodnioniemieckie ugrupowanie terrorystyczno – anarchistyczne.

[16] Czerwone Brygady *(wł. Brigate Rosso)* – organizacja terrorystyczna działająca we Włoszech reprezentująca radykalny i bezwzględny w swym działaniu nurt terroryzmu, powołująca się na skrajnie lewicową ideologię.

[17] IRA *(ang. Irish Republican Army)* – Irlandzka Armia republikańska walcząca o zjednoczenie Irlandii, zaliczana do narodowo – wyzwoleńczego nurtu terroryzmu.

[18] Za „NATO Vademecum", Wyd. Bellona, Warszawa 1995r., str. 262.

W taki sposób pojawiła się nowa jakość w historii walki z terroryzmem. Zjawisko to zostało określone jako największe zagrożenie dla pokoju światowego początku XXI wieku a działania USA wobec terrorystów są popierane nie tylko przez członków NATO *(w tym przez Polskę)*, ale przez większość cywilizowanych krajów świata. Poparcie naszego kraju ma nie tylko swój polityczny, ale również militarny wymiar. Żołnierze polscy od marca 2002, w ramach międzynarodowej koalicji wykonują zadania w strefie działań zbrojnych chociaż Afganistanie.

I chociaż globalna krucjata przeciwko terroryzmowi trwa, ruchy ekstremistyczne nadal są niebezpieczne i wiele państw, w tym Polska, musi się liczyć z realnymi zagrożeniami. Co prawda w całej historii Polski niewiele było aktów jawnego terroru kierowanego przeciwko naszemu krajowi ale jednak uwzględniając wydarzenia roku 2001 oraz konieczność dotrzymania sojuszniczych zobowiązań wynikających z członkostwa w NATO, musimy być przygotowani na przeciwdziałanie wszelkim przejawom terroru.

Ilość terrorystycznych organizacji na świecie jest bardzo duża, dzielą się one, tworzą się nowe ich odłamy. Departament Stanu USA aktualizuje co dwa lata listę międzynarodowych organizacji terrorystycznych. Według jej wersji z końca 2001 roku największe zagrożenie stwarzało 28 organizacji terrorystycznych[20]. Większość to ugrupowania islamskie – między innymi Al. – Ka'ida (kierowane przez Osamę bin Ladena)[21], szyickie Hezbollah[22], palestyńskie Hamas[23], egipskie Al. – Dżihad[24].

Biorąc pod uwagę fakt, iż z każdym praktycznie aktem terroru łączy się konieczność zdobycia przez przeprowadzających atak informacji niejawnych dotyczących lokalizacji atakowanych obiektów państwowych czy wojskowych,

---

[19] NATO po Pradze *(ang. NATO after Prague)*, Biuro Prasy i Informacji NATO, Bruksela, 2002, str. 5.
[20] Trybuna, nr 235 (3528) z 8 października 2001 roku.
[21] Al. Ka'ida – *(w tłumaczeniu baza)*, organizacja terrorystyczna skupiająca fundamentalistów islamskich z wielu krajów arabskich, których łączy jeden cel DŻIHAD – święta wojna przeciwko Stanom Zjednoczonym i światowi zachodniemu. Członkowie tej organizacji przeprowadzili atak na USA 11 września 2001 roku.
[22] Hezbollah *(w tłumaczeniu Hezb-e-Allah – partia Boga)*, partia wojujących fundamentalistów szyickich w Libanie, założona w 1985 roku, odpowiedzialna za szereg zamachów terrorystycznych na terenach tzw. Autonomii Palestyńskiej i w samym Izraelu.
[23] Hamas – Islamski ruch oporu, organizacja reprezentująca religijny nurt terroryzmu fundamentalistów islamskich, działająca w Izraelu, strefie Gazy.
[24] Al.-Dżihad – egipska, islamska organizacja terrorystyczna. Nazwa pochodzi od „świętej wojny", wywodzącej się z Koranu, która według interpretacji terrorystów daje im moralne prawo do walki z wszystkimi, którzy nie są wyznawcami islamu. Celem programowym jest zjednoczenie wszystkich Arabów na gruncie islamu i zbudowanie wspólnego państwa.

planów i systemów ich obrony, danych osób, które są nośnikami tajemnic państwowych, zagrożenia dla ochrony informacji niejawnych ze strony terroryzmu muszą być uwzględniane w organizacji systemów ochrony fizycznej czy systemów i sieci teleinformatycznych. Ostatnie doświadczenia społeczności międzynarodowej związane z walką przeciwko terroryzmowi oraz przewidywany długi czas otwartej z nim walki determinują jednoznacznie konieczność skutecznej ochrony informacji niejawnych przed tym niebezpiecznym zjawiskiem, chorobą czasów współczesnych.

c. międzynarodowa przestępczość zorganizowana;

Działalność grup przestępczych jest olbrzymim zagrożeniem dla porządku prawnego każdego kraju. W ostatnich latach przestępczość przekroczyła granice państw stając się problemem globalnym dla międzynarodowej społeczności. Grupy przestępcze, porozumiewając się ponad granicami, utworzyły międzynarodowe organizacje, doskonale zorganizowane, świetnie współpracujące ze sobą. Było to możliwe dzięki ogromnym środkom finansowym, jakie uzyskały z prowadzenia nielegalnej działalności. Pozwoliły one nabyć przestępcom wysokiej jakości sprzęt, broń, środki transportu i łączności. Dzisiaj nikogo już nie dziwi fakt, że przestępcy są lepiej wyposażeni niż ścigający ich policjanci. Jest to typowe dla krajów biedniejszych, takich jak Polska.

Ogromne środki finansowe, jakie są w dyspozycji organizacji przestępczych i mafijnych muszą być zalegalizowane. Dlatego świat kryminalny stara się lokować nielegalnie zdobyte środki w legalne przedsięwzięcia. Powstają nowe firmy tylko po to, aby na ich konto zostały przelane pieniądze, szerzy się łapówkarstwo i korupcja po to, aby zalegalizować wątpliwe interesy. Przestępcy idą coraz dalej, przenikają do świata polityki, wymuszają bądź przekupują decydentów z pierwszych stron gazet po to, aby zapewnić ujście nielegalnie zdobywanemu potokowi pieniędzy. Polska doświadcza na co dzień zagrożeń jakie stwarza przestępczość zorganizowana. Spektakularne zabójstwa gen. Marka PAPAŁY czy ministra Jacka DĘBSKIEGO potwierdzają, iż macki przestępców sięgają bardzo

wysoko i że przed państwem stoją bardzo trudne zadania, związane z likwidacją wyjątkowo dla niego szkodliwej działalności.

Przestępczość to zjawisko, którego doświadczamy codziennie, które dezorganizuje wiele dziedzin życia publicznego. Nie ulega wątpliwości, iż przestępcy są również zagrożeniem dla systemu ochrony informacji niejawnych w naszym kraju. Pomyślność każdego nielegalnego procederu wiąże się ze zdobywaniem informacji, często niejawnych, z pozyskiwaniem osób, które zapewnić mają pomyślną realizację kolejnego przestępczego przedsięwzięcia. Dlatego zagrożenie to trzeba definiować jako realne, oceniać je w kategoriach zagrożeń zewnętrznych a także istniejących wewnątrz naszego kraju.

Oprócz powyżej omówionych zagrożeń **zewnętrznych** można zdefiniować szereg zagrożeń **wewnętrznych**, które determinują konieczność sprawnego funkcjonowania systemu ochrony informacji niejawnych w Polsce. Do głównych należą działalność grup przestępczych czy wewnętrzna konkurencja powiązanych z biznesem grup wpływu. Równie ważnym zagrożeniem, o którym często zapominamy jest niski poziom świadomości dysponentów informacji niejawnych. Wiele osób, w tym zajmujących wysokie stanowiska służbowe lekceważy przepisy, zaniża klauzule tajności wytwarzanych dokumentów, niewłaściwie je zabezpiecza bądź po prostu otwarcie mówi o zawartych w nich tajemnicach. Tego, co można określić mianem kultury wykonawczej w sferze ochrony informacji niejawnych często jeszcze w naszym kraju, w tym w Siłach Zbrojnych brakuje.

W jaki sposób przeciwdziałać wymienionym, zewnętrznym i wewnętrznym zagrożeniom. Na to pytanie można sobie odpowiedzieć rozpatrując możliwość występowania każdego z zagrożeń w realnych warunkach funkcjonowania konkretnego organu władzy publicznej, jednostki wojskowej czy firmy realizującej kontrakt, z którym łączy się dostęp do informacji niejawnych. Należy też uwzględniać możliwość jednoczesnego występowania różnych zagrożeń wobec jednego podmiotu w tych samych warunkach. Nie ulega wątpliwości, że zagrożenia ze strony służb specjalnych mają charakter stały a w przypadku naszego kraju zainteresowanie obcego wywiadu nigdy nie zniknie. Inne zagrożenia, być może trudne do wyobrażenia sobie przez przeciętnego Polaka, zagrożenia ze strony

terroryzmu i przestępczości zorganizowanej będą się utrzymywać stale, choć ich skala i natężenie może się zmieniać. Zagrożenia o charakterze stałym związane z dyscypliną wewnętrzną i brakiem niezbędnej wiedzy osób, które mają do czynienia z informacjami niejawnymi są zależne od jakości organizacji systemu ochrony informacji w państwie, wymagalności kierowników jednostek organizacyjnych, poziomu szkolenia i kontroli. Odpowiedź na pytanie jak przeciwdziałać zagrożeniom może być tylko jedna – **zbudować sprawny, przemyślany system ochrony informacji niejawnych, bezpieczeństwa osobowego, fizycznego, przemysłowego, teleinformatycznego, szkolenia i kontroli. System bazujący na optymalnych rozwiązaniach ustawowych, posiadający jasno określone ramy odpowiedzialności osób funkcyjnych i kształtujący świadomą dyscyplinę wykonawczą osób wytwarzających, przechowujących i przesyłających informacje niejawne.**[25]

2. Rys historyczny kształtowania się podstaw prawnych ochrony informacji niejawnych w Polsce.

Do marca 1999 roku w Polsce obowiązywała Ustawa o ochronie tajemnicy państwowej i służbowej, przyjęta w 1982 roku,[26] która weszła w życie z dniem 1 lipca 1983 roku. Zgodnie z tą ustawą nadzór oraz ogólną koordynację nad ochroną tajemnicy państwowej i służbowej w kraju sprawowało Ministerstwo Spraw Wewnętrznych poprzez swe Biuro ds. Koordynacji Ochrony Tajemnicy. Ustawa definiowała istotę tajemnicy państwowej i służbowej w sposób ogólny ustanawiając klauzule TAJNE i TAJNE SPECJALNEGO ZNACZENIA dla wiadomości stanowiących tajemnicę państwową i POUFNE dla informacji stanowiących tajemnicę służbową. Jednocześnie, na mocy tej ustawy, minister obrony narodowej odpowiadał za określenie szczegółowych zasad i sposobów postępowania z informacjami stanowiącymi tajemnicę państwową o szczególnym znaczeniu dla obronności państwa i Sił Zbrojnych RP. Na mocy tej delegacji minister obrony

[25] System ten jest opisany w dalszej części Rozdziału I i w Rozdziale II.
[26] Ustawa z dnia 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej, Dz. U. nr 40, poz. 271 z późniejszymi zmianami.

narodowej wprowadził do użytku „Przepisy o ochronie tajemnicy w Siłach Zbrojnych", które stanowiły między innymi, iż:

... Upoważnieniem żołnierza zawodowego do dostępu do wiadomości stanowiących tajemnicę państwową jest rozkaz personalny o wyznaczeniu na stanowisko służbowe lub rozkaz o wyznaczeniu do prac związanych z dostępem do wiadomości stanowiących tajemnice państwową... .[27]

Oceniając ten akt prawny należy stwierdzić, iż regulował on kwestie ochrony informacji, stanowiących tajemnicę państwową i służbową, w sposób właściwy, wystarczający dla czasu, w którym został przyjęty. Jednakże z biegiem lat ustawa z 1982 roku stawała się nieco anachroniczną, bowiem nie uwzględniała realiów zmieniającej się rzeczywistości w sferze ochrony informacji. Przede wszystkim ustawodawca nie przewidział zagrożeń dla bezpieczeństwa informacji wytwarzanych, przechowywanych i przesyłanych w systemach komputerowych. Ustawa nie regulowała ponadto spraw dotyczących bezpieczeństwa przemysłowego oraz nie ustanawiała tak podstawowego standardu dla natowskich rozwiązań, jakim jest cykliczne prowadzenie postępowań sprawdzających wobec osób przed upoważnieniem ich do dostępu do informacji niejawnych. Przyczyny te sprawiły, iż w aspekcie coraz bardziej realnego wstąpienia Polski do Organizacji Traktatu Północnoatlantyckiego, przyjęcie całkowicie nowego aktu prawnego w sferze ochrony informacji niejawnych stawało się koniecznością.

Innym aspektem zmian w dziedzinie ochrony informacji niejawnych w ostatnich latach były skutki przemian ustrojowych w państwie, po transformacji, która zapoczątkowana została w 1989 roku oraz przejawy politycznej i społecznej dezaprobaty dla większości norm prawnych, które wiązały się z poprzednim ustrojem. Na fali demokratycznych przemian krytykowano również ustawę z 1982 roku, której przypisywano ... wojenny rodowód... .[28]

W latach 90-tych podejmowano próby opracowania nowej ustawy o ochronie tajemnicy państwowej i służbowej a jej uchwalenie wydawało się bardzo realne:

---

[27] Sygn. Sztab Gen. 1251/86, § 5...Rozdz. II, część I „Zasady ogólne".
[28] Jakubus B., Ryszkowski M, „Ochrona informacji niejawnych", Wyd. Projekt, Warszawa 2001, str. 7.

- 15 września 1994 roku Sejm Rzeczypospolitej Polskiej uchwalił nową ustawę, która jednak w lutym 1995 roku podczas ponownej debaty nad propozycjami poprawek wniesionymi przez Senat została w całości odrzucona;
- 27 sierpnia 1997 roku, w związku ze zbliżającą się akcesją do NATO Sejm przyjął nowelizację ustawy, która uwzględniała zastosowanie natowskich rozwiązań i wprowadzenie sojuszniczych standardów bezpieczeństwa w sferze ochrony informacji niejawnych[29].

Pomimo faktu przyjęcia nowej ustawy w 1997 roku nie ukazały się do niej żadne akty wykonawcze, ponieważ w ocenie Rady Ministrów RP, wyłonionej po wyborach parlamentarnych w 1997 roku, przyjęte rozwiązania nie zapewniały skutecznej ochrony informacji w warunkach przynależności naszego kraju do NATO i za lepsze rozwiązanie uznano opracowanie całkiem nowego aktu prawnego. W wyniku efektywnie prowadzonych prac legislacyjnych Sejm RP uchwalił 22 stycznia 1999 roku Ustawę o ochronie informacji niejawnych, obowiązującą po dzień dzisiejszy. Do ustawy wydano szereg aktów wykonawczych w formie:

- rozporządzeń Rady Ministrów;
- rozporządzeń prezesa Rady Ministrów;
- rozporządzeń ministra spraw wewnętrznych i administracji;
- rozporządzeń ministrów spraw wewnętrznych i administracji oraz obrony narodowej.

W uzupełnieniu tych aktów normatywnych minister obrony narodowej wydał jedno zarządzenie i szereg szczegółowych decyzji regulujących zasady ochrony informacji niejawnych w resorcie obrony narodowej.

Pomimo tego, że ustawa jest stosunkowo obszernym aktem prawnym i uwzględnia większość standardów natowskich, dotyczących ochrony informacji niejawnych, nie jest doskonałą. Świadczą o tym dokonane, od czasu jej wejścia w życie, nowelizacje. Do dnia 22 stycznia 2003 roku przeprowadzono następujące nowelizacje Ustawy o ochronie informacji niejawnych:

---

[29] Nowelizacja została opublikowana w Dz. U. Nr 110 z dnia 23 października 1997 roku, poz. 714.

- dotycząca możliwości przedłużenia czasu ochrony materiałów kartograficznych i geodezyjnych, oznaczonych klauzulą POUFNE powyżej 5 lat *(pięcioletni okres ochrony tego typu informacji został określony w pierwotnej wersji ustawy)*[30].
- związana z wyrokiem Trybunału Konstytucyjnego w sprawie niezgodności zapisów ustawy z innymi aktami prawnymi[31]. W art. 42 ust. 1 pierwotnej wersji ustawy istniał zapis stanowiący, iż do postępowania sprawdzającego nie mają zastosowania przepisy Kodeksu Postępowania Administracyjnego oraz przepisy o zaskarżaniu do Naczelnego Sądu Administracyjnego. Zapis ten, zaskarżony przez Rzecznika Praw Obywatelskich został uznany przez Trybunał Konstytucyjny jako niezgodny z art. 13 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności, sporządzonej w Rzymie 4 listopada 1950 r. [32] przez to, że pozbawiał osobę sprawdzaną jakiegokolwiek skutecznego środka odwoławczego w wypadku odmowy wydania poświadczenia bezpieczeństwa. Ponadto przepis ten był niezgodny z Konstytucją Rzeczypospolitej Polskiej, stanowiącą, iż

  ... Każdy ma prawo do sprawiedliwego i jawnego rozpatrzenia sprawy bez nieuzasadnionej zwłoki przez właściwy, niezależny, bezstronny i niezawisły sąd ...[33] . Ustawa zasadnicza stanowi również, iż ...Ustawa nie może nikomu zamykać drogi sądowej dochodzenia naruszonych wolności lub praw...[34]. Zapis art. 42 był więc niezgodny z Ustawą zasadniczą, ponieważ w zakresie realizacji prawa dostępu do służby publicznej, zamykał drogę do sądu, uniemożliwiając kontrolę zgodności z prawem procedur stosowanych w postępowaniu sprawdzającym. W związku z powyższym Trybunał Konstytucyjny zdecydował, iż z dniem 31 stycznia

---

[30] Nowelizacja została wprowadzona na mocy Ustawy z dnia 21 stycznia 2000 roku o zmianie niektórych ustaw związanych z funkcjonowaniem administracji publicznej i opublikowana w Dz. U. z 2000 roku, Nr 12, poz. 136.

[31] Nowelizacja została wprowadzona na mocy wyroku Trybunału Konstytucyjnego z dnia 10 maja 2000 roku, sygn. Akt K 21/99 i opublikowana w Dz. U. z 2000 roku, Nr 39, poz. 462.

[32] Dz. U. z 1993 r. Nr 61, poz. 284 z późniejszymi zmianami.

[33] Art. 45, ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku, Dz. U. z 2001 roku, Nr 28 poz. 319.

2001 roku przepis ten utraci moc obowiązującą. Wyrok Trybunału Konstytucyjnego z dnia 10 maja 2000 roku stał się asumptem do przyśpieszenia prac związanych z kompleksową nowelizacją ustawy, które praktycznie po kilku miesiącach jej obowiązywania i pierwszych doświadczeniach służb ochrony państwa stały się oczywiste;

- kompleksowa, która wprowadziła szereg nowych regulacji między innymi w sprawach postępowania odwoławczego i skargowego, bezpieczeństwa przemysłowego, odpłatności za czynności wykonywane przez służby ochrony państwa w toku postępowań sprawdzających[35].

Do najważniejszych zmian wprowadzonych tą nowelizacją należały:

/ dodanie do ustawy rozdziału „Postępowanie odwoławcze i skargowe", dzięki czemu zmaterializował się wyrok Trybunału Konstytucyjnego w sprawie niezgodności zapisów ustawy z innymi aktami prawnymi. Postanowienia zawarte w tej części ustawy precyzyjnie określiły zasady odwoływania się osób sprawdzanych zarówno przez służbę ochrony państwa jak i przez pełnomocnika ochrony od odmowy wydania im poświadczenia bezpieczeństwa;

/ wprowadzenie możliwości przedłużania, przez osobę upoważnioną do podpisania dokumentu niejawnego, czasu ochrony informacji niejawnych, stanowiących tajemnicę służbową łącznie na okres do 50 lat;

/ określenie trybu prowadzenia postępowań sprawdzających wobec osób sprawujących najważniejsze urzędy w państwie, w tym na przykład wyznaczonych na stanowiska ministrów, nie powoływanych w składzie całej Rady Ministrów, formowanej na przykład po wyborach parlamentarnych;

/ sprecyzowanie zasad doręczania osobie sprawdzanej odmowy wydania poświadczenia bezpieczeństwa. Zarówno pełnomocnik jak i służba ochrony państwa zostały zobowiązane do bezpośredniego

---

[34] Tamże, art. 77, ust. 2.

[35] Nowelizacja została wprowadzona na mocy Ustawy z dnia 3 lutego 2001 roku o zmianie ustawy o ochronie informacji niejawnych i opublikowana w Dz. U. z 2001 roku, Nr 22, poz. 247.

przekazania tego typu decyzji osobie, której odmowa dotyczy z jednoczesnym powiadomieniem o tym fakcie osoby upoważnionej do obsady stanowiska, zajmowanego przez osobę sprawdzaną;

- wprowadzenie zapisów umożliwiających służbie ochrony państwa prowadzenie zwykłych postępowań sprawdzających wobec pełnomocników ochrony przed upoważnieniem ich do dostępu do informacji stanowiących tajemnicę służbową o klauzuli POUFNE;
- określenie trybu udostępniania przez pełnomocnika ochrony bądź służbę ochrony państwa akt postępowania sprawdzającego na żądanie sądu, prokuratora, Naczelnego Sądu Administracyjnego lub innych uprawnionych organów w celu rozpatrzenia odwołania;
- wprowadzenie obowiązku certyfikacji urządzeń i narzędzi kryptograficznych wchodzących w skład systemów i sieci teleinformatycznych służących do wytwarzania, przechowywania, przetwarzania lub przekazywania informacji niejawnych stanowiących tajemnicę służbową o klauzuli POUFNE;
- wprowadzenie obowiązku pobierania przez służby ochrony państwa opłat za przeprowadzenie postępowania sprawdzającego przed wydaniem poświadczenia bezpieczeństwa osobowego oraz za wydanie tego poświadczenia, opłat za czynności realizowane przed wydaniem świadectwa bezpieczeństwa przemysłowego oraz za wydanie takiego świadectwa a także opłat za przeprowadzenie czynności warunkujących wydanie certyfikatu dla systemu lub sieci teleinformatycznej, urządzenia lub narzędzia kryptograficznego oraz za wydanie tych certyfikatów. Jednostki budżetowe zostały zwolnione z obowiązku uiszczania wymienionych powyżej opłat, z wyłączeniem opłaty za wydanie certyfikatu;
- określenie, iż do obowiązków zleceniodawcy należy zebranie i przesłanie do służby ochrony państwa dokumentów wymaganych do przeprowadzenia postępowania sprawdzającego przed wydaniem świadectwa bezpieczeństwa przemysłowego;

/ wprowadzenie możliwości przeprowadzenia przez służbę ochrony państwa postępowania sprawdzającego przed wydaniem świadectwa bezpieczeństwa przemysłowego z urzędu;

/ rozszerzenie zakresu informacji stanowiących tajemnicę państwową, wyszczególnionych w Załączniku Nr 1 do ustawy.

Oprócz wymienionych powyżej, głównych regulacji nowelizacja wprowadziła szereg innych zmian, ukierunkowanych na sprecyzowanie niezbyt jasnych sformułowań jej pierwotnej wersji.

- wprowadzająca zmiany w Załączniku Nr 1 *(w części II)* do Ustawy o ochronie informacji niejawnych „Informacje niejawne oznaczone klauzulą TAJNE ze względu na obronność i bezpieczeństwo państwa oraz porządek publiczny", na mocy których szczegółowa struktura organizacyjna i etatowa jednostek organizacyjnych Biura Ochrony Rządu oraz system ewidencji danych o jego funkcjonariuszach, żołnierzach i pracownikach a także szczegółowych formach i metodach działania BOR uznane zostały za informacje stanowiące tajemnicę państwową, które muszą być oznaczane klauzulą TAJNE.[36]
- wprowadzająca zmiany w Załączniku Nr 1 *(w części III)* do Ustawy o ochronie informacji niejawnych „Informacje niejawne oznaczone klauzulą TAJNE ze względu na ważny interes państwa", na mocy których informacje, dotyczące technologii wytwarzania bonów paliwowych oraz system ich zabezpieczenia w wytwórniach, drukujących je, uznane zostały za informacje stanowiące tajemnicę państwową, które muszą być oznaczane klauzulą TAJNE.[37]
- wprowadzająca zmiany w Załączniku Nr 1 *(w części II)* do Ustawy o ochronie informacji niejawnych „Informacje niejawne oznaczone klauzulą TAJNE ze względu na obronność i bezpieczeństwo państwa oraz porządek publiczny", na mocy których szczegółowa struktura

[36] Nowelizacja została wprowadzona na mocy Ustawy z dnia 16 marca 2001 roku o Biurze Ochrony Rządu i opublikowana w Dz. U. z 2001 roku, Nr 27, poz. 298.

[37] Nowelizacja została wprowadzona na mocy Ustawy z dnia 27 kwietnia 2001 roku o zmianie ustawy o podatku od towarów i usług oraz o podatku akcyzowym, ustawy o zamówieniach publicznych oraz ustawy o ochronie informacji niejawnych i opublikowana w Dz. U. z 2001 roku, Nr 56, poz. 580.

organizacyjna i etatowa jednostek organizacyjnych Krajowego Centrum Informacji Kryminalnych oraz system ewidencji danych o jego funkcjonariuszach, żołnierzach i pracownikach uznane zostały za informacje stanowiące tajemnicę państwową, które muszą być oznaczane klauzulą TAJNE.[38]

- uzupełniająca ustawę o szereg zapisów, które wynikały z uchwalenia przez Sejm RP, w dniu 24 sierpnia 2001 roku, Ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych[39]. Stosownie do art. 67 wymienionej ustawy zmiany obejmowały:
  / nowelizację rozdziału 5 Ustawy o ochronie informacji niejawnych, dotyczącego prowadzenia postępowań sprawdzających, na mocy której Żandarmeria Wojskowa jako wyodrębniona i wyspecjalizowana służba wchodząca w skład Sił Zbrojnych, uzyskała prawo do samodzielnego prowadzenia postępowań sprawdzających wobec osób ubiegających się o przyjęcie do służby lub pracy w jej organach *(analogicznie jak UOP, WSI, Policja, Straż Graniczna i Służba Więzienna)*. Jednocześnie Komendant Główny Żandarmerii Wojskowej uzyskał stosowne uprawnienia w postępowaniu odwoławczym i skargowym oraz w zakresie wglądu do akt postępowań sprawdzających *(analogicznie jak szef UOP, szef WSI, Komendant Główny Policji, Komendant Główny Straży Granicznej, Dyrektor Generalny Służby Więziennej)*;
  / nowelizację części II Załącznika Nr 1 do Ustawy o ochronie informacji niejawnych „Informacje niejawne oznaczone klauzulą TAJNE ze względu na obronność i bezpieczeństwo państwa oraz porządek publiczny", na mocy której szczegółowa struktura organizacyjna i etatowa Żandarmerii Wojskowej oraz system ewidencji danych o jej funkcjonariuszach, żołnierzach i pracownikach

[38] Nowelizacja została wprowadzona na mocy Ustawy z dnia 6 lipca 2001 roku o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych i opublikowana w Dz. U. z 2001 roku, Nr 110, poz.1189.
[39] Ustawa została opublikowana w Dz. U. z 2001 roku, Nr 123, poz. 1353.

uznane zostały za informacje stanowiące tajemnicę państwową, które muszą być oznaczane klauzulą TAJNE.

- wprowadzająca zmiany w Załączniku Nr 1 *(w części II)* do Ustawy o ochronie informacji niejawnych „Informacje niejawne oznaczone klauzulą TAJNE ze względu na obronność i bezpieczeństwo państwa oraz porządek publiczny", na mocy których szczegółowe formy i metody działania Żandarmerii Wojskowej uznane zostały za informacje stanowiące tajemnicę państwową, które muszą być oznaczane klauzulą TAJNE.[40]
- związana z utworzeniem Agencji Bezpieczeństwa Wewnętrznego. Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[41]wprowadziła niezwykle istotne zmiany w Ustawie o ochronie informacji niejawnych. Ustanowiła on nowy system funkcjonowania służb specjalnych w Rzeczypospolitej Polskiej poprzez likwidację Urzędu Ochrony Państwa i powołanie w jego miejsce dwóch agencji – Agencji Bezpieczeństwa Wewnętrznego (ABW) i Agencji Wywiadu (AW). Zadania w sferze ochrony informacji niejawnych, które dotychczas realizował Urząd Ochrony Państwa zostały przypisane ABW. Zadania te zostały sprecyzowane następująco:

  ... realizowanie, w granicach swojej właściwości, zadań służby ochrony państwa oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych...[42]

  W konsekwencji wymieniona ustawa wprowadziła szereg zarówno jakościowych jak i redakcyjnych zmian w Ustawie o ochronie informacji niejawnych. Należały do nich w szczególności:

---

[40] Nowelizacja została wprowadzona na mocy Ustawy z dnia 21 grudnia 2001 roku o zmianie Ustawy o organizacji i trybie pracy Rady Ministrów oraz o zakresie działania ministrów, ustawy o działach administracji rządowej oraz o zmianie niektórych ustaw i opublikowana w Dz. U. z 2001 roku, Nr 154, poz. 1800.

[41] Ustawa z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz. U. z 2002 roku, Nr 74, poz. 676.

[42] Tamże, art. 5, ust. 1, pkt 3.

/ likwidacja Komitetu Ochrony Informacji Niejawnych i przejęcie zadań, dotychczas realizowanych przez ten organ przez Kolegium do spraw Służb Specjalnych działające przy Radzie Ministrów;

/ przypisanie uprawnień określonych dla Urzędu Ochrony Państwa, szefa UOP oraz funkcjonariusza UOP odpowiednio Agencji Bezpieczeństwa Wewnętrznego, szefowi ABW i funkcjonariuszowi ABW;

/ upoważnienie Agencji Wywiadu do prowadzenia postępowań sprawdzających wobec osób ubiegających się o przyjęcie do służby lub pracy oraz pełniących służbę lub zatrudnionych w tej agencji.

- likwidująca uprawnienie służb ochrony państwa do korzystania, w zakresie koniecznym do wykonywania swoich zadań w celu ochrony informacji niejawnych, z informacji uzyskanych przez organy inspekcji celnej. Organy te, od 2002 roku, nie mają już obowiązku okazywania pomocy służbom ochrony państwa przy wykonywaniu ich czynności w ramach prowadzonych postępowań sprawdzających.[43]

Poza zmianami w ustawie, które już obowiązują, w przyszłości wprowadzone zostaną zmiany, wynikające z utworzenia, z dniem 1 stycznia 2004 roku, wojewódzkich sądów administracyjnych, które powstaną w miejsce ośrodków zamiejscowych Naczelnego Sądu Administracyjnego oraz z zastąpienia instytucji rewizji nadzwyczajnej - skargą kasacyjną.[44] Obecnie obowiązujące przepisy o Naczelnym Sądzie Administracyjnym[45], mające zastosowanie w postępowaniu odwoławczym w związku z odmową wydania poświadczenia bezpieczeństwa osobowego będą obowiązywać do końca 2003 roku.

Pomimo niedoskonałości pierwszej wersji Ustawy o ochronie informacji niejawnych i częstej krytyki przyjętych w niej rozwiązań, zwłaszcza ze strony służb ochrony państwa i przedsiębiorców realizujących kontrakty niejawne, generalnie

---

[43] Nowelizacja została wprowadzona na mocy Ustawy z dnia 7 czerwca 2002 roku o zniesieniu Generalnego Inspektora Celnego, o zmianie ustawy o kontroli skarbowej oraz o zmianie niektórych, innych ustaw i opublikowana w Dz. U. z 2002 roku, Nr 89, poz. 804.

[44] Ustawa z dnia 30 sierpnia 2002 roku – Prawo o postępowaniu przed sądami administracyjnymi, Dz. U. z 2002 roku, Nr 153, poz. 1270.

[45] Ustawa z dnia 11 maja 1995 roku o Naczelnym Sądzie Administracyjnym, Dz. U. z 1995 roku, Nr 74, poz. 368 z późniejszymi zmianami.

ten akt prawny należy ocenić pozytywnie. Przyjęte w niej rozwiązania pozwoliły bowiem wprowadzić do polskiego prawa i praktyki wszystkie standardy bezpieczeństwa, obowiązujące w Organizacji Traktatu Północnoatlantyckiego. Natomiast mechanizmy działania służb ochrony państwa, obowiązki kierowników jednostek organizacyjnych i pionów ochrony zostały sprecyzowane stosunkowo wyczerpująco, w sposób który pozwala z mocy prawa przestrzegać i zmuszać do przestrzegania przepisów o ochronie informacji niejawnych w naszym kraju, w tym w Siłach Zbrojnych RP.

W niedalekiej przyszłości należy liczyć się z koniecznością zmian w Ustawie o ochronie informacji niejawnych. Są one nieuchronne, dlatego że nie jest możliwym uregulowanie wszystkich aspektów ochrony informacji niejawnych w jednym, nawet najlepszym akcie prawnym. Jak dowodzi praktyka działalności służb ochrony państwa, kierowników jednostek organizacyjnych i pełnomocników ochrony życie stawia przed nimi szereg nowych pytań, na które nie ma jasnej odpowiedzi w ustawie i które wymagają prawnych ocen i interpretacji.[46]

Ponadto praktyka funkcjonowania organów bezpieczeństwa NATO i opracowywanych przez nie dokumentów normatywnych w sferze bezpieczeństwa świadczy o tym, że cyklicznie są one oceniane i jeśli jest taka potrzeba w sposób kolektywny nowelizowane. Na przykład w 2002 roku zakończył się kilkuletni okres przeglądu dokumentów bezpieczeństwa, w rezultacie czego dostosowano obowiązujące przepisy do nowej rzeczywistości w jakiej działa NATO i do nowych wyzwań zwłaszcza w dziedzinie bezpieczeństwa teleinformatycznego i przemysłowego[47].

3. Podstawy prawne ochrony informacji niejawnych w sferze wojskowej i cywilnej.

Zasadniczym aktem prawnym regulującym w Polsce zasady ochrony informacji niejawnych jest, kilkakrotnie nowelizowana, Ustawa z dnia 22 stycznia

[46] Przewidywane zmiany w Ustawie o ochronie informacji niejawnych, wraz z uzasadnieniem potrzeby ich wprowadzenia omówione zostały w Uwagach Końcowych.
[47] Dokumenty normatywne NATO w sferze ochrony informacji niejawnych omówione są w Rozdziale III.

1999 roku o ochronie informacji niejawnych. Ustawa weszła w życie 10 marca 1999 roku, otwierając tym samym nowy rozdział w historii ochrony informacji niejawnych w Polsce, w tym w Siłach Zbrojnych RP.

Ustawa stanowi, iż informacje niejawne, które są wytwarzane, przechowywane, przesyłane w Polsce oraz wymieniane z innymi państwami i organizacjami międzynarodowymi podlegają ochronie prawnej i muszą być w odpowiedni sposób chronione a osoby, które mają z nimi do czynienia muszą dawać rękojmię, iż będą się z nimi w odpowiedni sposób obchodzić. Wychodząc z tych generalnych założeń ustawa określa zasady:

- organizowania ochrony informacji niejawnych;
- klasyfikowania informacji niejawnych;
- udostępniania informacji niejawnych;
- prowadzenia postępowania sprawdzającego przed wydaniem poświadczenia bezpieczeństwa osobowego;
- prowadzenia postępowania sprawdzającego przed wydaniem świadectwa bezpieczeństwa przemysłowego;
- szkolenia w zakresie ochrony informacji niejawnych;
- ewidencjonowania, przechowywania, przetwarzania i udostępniania danych uzyskiwanych w związku z prowadzonymi postępowaniami sprawdzającymi przed wydaniem poświadczenia bezpieczeństwa osobowego i świadectwa bezpieczeństwa przemysłowego;
- organizacji kontroli przestrzegania zasad ochrony informacji niejawnych;
- ochrony informacji niejawnych w systemach i sieciach teleinformatycznych;
- stosowania środków fizycznej ochrony informacji niejawnych.

Zasady te mają zastosowanie do wszystkich jednostek organizacyjnych w państwie, którymi w rozumieniu ustawy są:

- organy władzy publicznej, w tym Sejm, Senat, Prezydent, organy administracji rządowej, organy samorządu terytorialnego, sądy i trybunały, organy kontroli państwowej i ochrony prawa;
- Siły Zbrojne RP i ich jednostki organizacyjne;

- Narodowy Bank Polski i banki państwowe;
- państwowe osoby prawne i inne państwowe jednostki organizacyjne;
- przedsiębiorcy, jednostki naukowe lub badawczo – rozwojowe, ubiegające się o zawarcie lub wykonujące umowy związane z dostępem do informacji niejawnych albo wykonujące na podstawie przepisów prawa zadania na rzecz obronności i bezpieczeństwa państwa, związane z dostępem do informacji niejawnych.

Wraz z ustawą o ochronie informacji niejawnych ukazały się akty wykonawcze, które stanowiąc uzupełnienie podstawowego aktu prawnego uregulowały najbardziej szczegółowe kwestie dotyczące ochrony informacji niejawnych. Należą do nich:

- Rozporządzenia Rady Ministrów z dnia 9 lutego 1999 r. w sprawie stanowisk i rodzajów prac zleconych w organach administracji rządowej, których wykonywanie może łączyć się z dostępem do informacji niejawnych stanowiących tajemnicę państwową[48];
- Rozporządzenie Rady Ministrów z dnia 9 lutego 1999 r. w sprawie organizacji kancelarii tajnych[49];
- Rozporządzenie Rady Ministrów z dnia 9 lutego 1999 r. w sprawie wzorów: kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, odmowy wydania świadectwa bezpieczeństwa przemysłowego[50];
- Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie szczegółowego zakresu, warunków i trybu współdziałania organów, służb i innych państwowych jednostek organizacyjnych ze służbami ochrony państwa w toku prowadzonych postępowań sprawdzających[51];
- Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie szczegółowego trybu prowadzenia przez służby ochrony państwa

[48] Dz. U. z 1999 roku, Nr 18, poz. 155.
[49] Tamże, poz. 156 z późniejszymi zmianami.
[50] Tamże, poz. 157.
[51] Tamże, poz. 159.

kontroli w zakresie ochrony informacji niejawnych stanowiących tajemnicę państwową[52];

- Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie sposobu i trybu udostępniania danych z ewidencji[53];
- Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych[54];
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 23 lutego 1999 r. w sprawie wzoru poświadczenia bezpieczeństwa oraz wzoru odmowy wydania poświadczenia bezpieczeństwa[55];
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 23 lutego 1999 r. w sprawie wzoru zaświadczenia stwierdzającego odbycie przeszkolenia w zakresie ochrony informacji niejawnych[56];
- Rozporządzenie Ministrów Spraw Wewnętrznych i Administracji oraz Obrony Narodowej z dnia 26 lutego 1999 r. w sprawie sposobu oznaczania materiałów, w tym klauzulami tajności oraz sposobu umieszczania klauzul na tych materiałach[57];
- Rozporządzenie Ministrów Spraw Wewnętrznych i Administracji oraz Obrony Narodowej z dnia 26 lutego 1999 r. w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów[58];
- Rozporządzenie Prezesa Rady Ministrów z dnia 13 lipca 2001 r. w sprawie wysokości opłat za przeprowadzenie postępowania sprawdzającego przez służbę ochrony państwa oraz za wydanie świadectwa bezpieczeństwa przemysłowego[59];
- Rozporządzenie Prezesa Rady Ministrów z dnia 16 lipca 2001 r. w sprawie wysokości opłat za przeprowadzenie przez służbę ochrony

---

[52] Tamże, poz. 160.
[53] Tamże, poz. 161 z późniejszymi zmianami.
[54] Tamże, poz. 162.
[55] Tamże, poz. 165 z późniejszymi zmianami.
[56] Tamże, poz. 166.
[57] Tamże, poz. 167 z późniejszymi zmianami.
[58] Tamże, poz. 168.
[59] Dz. U. z 2001 roku, Nr 74, poz. 788.

państwa czynności warunkujących wydanie certyfikatu dla systemu lub sieci teleinformatycznej, urządzenia lub narzędzia kryptograficznego oraz za wydanie tych certyfikatów[60].

Wymienione rozporządzenia obowiązują wszystkie podmioty, wobec których mają zastosowanie przepisy Ustawy o ochronie informacji niejawnych. Jednakże biorąc pod uwagę fakt, iż Siły Zbrojne są instytucją szczególną, dysponującą ogromną ilością dokumentów niejawnych, wytwarzanych w czasie pokoju i przygotowywanych na czas wojny, w resorcie obrony narodowej opracowano szereg aktów normatywnych, regulujących szczegółowo kwestie dotyczące ochrony informacji niejawnych.

Do dokumentów tych należą:

- Zarządzenie Nr 49/MON ministra obrony narodowej z dnia 7 sierpnia 2002 roku w sprawie szczególnych zasad organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych[61];
- Decyzja Nr 29/MON ministra obrony narodowej z dnia 8 marca 2000 r. w sprawie szczególnych zasad i trybu przeprowadzania postępowań sprawdzających, dokumentowania i archiwizacji materiałów dotyczących postępowań[62];
- Decyzja Nr 30/MON ministra obrony narodowej z dnia 8 marca 2000 r. w sprawie powołania pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów i sieci teleinformatycznych oraz utworzenia pionów ochrony w jednostkach organizacyjnych resortu obrony narodowej[63];

---

[60] Dz. U. z 2001 roku, Nr 77, poz. 820.

[61] Dziennik Urzędowy ministra obrony narodowej z 30 sierpnia 2002 roku, Nr 15; poz. 149. Zarządzenie Nr 49 zastąpiło, obowiązujące uprzednio Zarządzenie Nr 10/MON ministra obrony narodowej z dnia 5 czerwca 2000 r. w sprawie szczególnych zasad organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych, opublikowane w Dzienniku Rozkazów MON z 2001 roku, pod pozycją 51.

[62] Dziennik Rozkazów MON z 2001 roku, poz. 74.

[63] Tamże, poz. 75 z późniejszymi zmianami.

- Decyzja Nr 31/MON ministra obrony narodowej z dnia 8 marca 2000 r. w sprawie zasad opracowywania planów ochrony jednostek organizacyjnych resortu obrony narodowej[64];
- Decyzja Nr 181/MON ministra obrony narodowej z dnia 6 października 2000 r. w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej[65];
- Decyzja Nr 182/MON ministra obrony narodowej z dnia 8 marca 2000 r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej[66];
- Decyzja Nr 100/MON ministra obrony narodowej z dnia 6 czerwca 2000 r. w sprawie Jednostki Certyfikującej, właściwej w Ministerstwie Obrony Narodowej do certyfikacji wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych[67];
- Decyzja Nr 16/MON ministra obrony narodowej z dnia 25 stycznia 2001 r. w sprawie szkolenia w zakresie ochrony informacji niejawnych[68];
- Decyzja Nr 29/MON ministra obrony narodowej z dnia 22 lutego 2001 r. w sprawie trybu certyfikacji i kontroli kancelarii zagranicznych, kancelarii środków i materiałów kryptograficznych, punktów obsługi dokumentów zagranicznych, stacji łączności kryptograficznej oraz pomieszczeń wydzielonych (terminali) teleinformatycznych w jednostkach organizacyjnych resortu obrony narodowej[69].

Powyższe zarządzenie i decyzje ministra obrony narodowej regulują większość kwestii związanych z ochroną informacji niejawnych. Nie są to jednak przepisy doskonałe i ostateczne. Zmieniające się warunki funkcjonowania armii i wynikające z nich potrzeby w zakresie modyfikacji systemu ochrony informacji

---

[64] Tamże, poz. 76.
[65] Tamże, poz. 111.
[66] Tamże, poz. 112.
[67] Tamże, poz. 55.
[68] Dziennik Urzędowy ministra obrony narodowej Nr 1 z 15 lutego 2001 roku, poz. 9 *(od 2001 roku akty normatywne wydane przez ministra obrony narodowej publikowane są w Dzienniku Urzędowym – podstawa: Decyzja Nr 251/MON z 22 grudnia 2000 roku w sprawie wydawania i dystrybucji Dziennika Urzędowego Ministerstwa Obrony Narodowej).*
[69] Dziennik Urzędowy ministra obrony narodowej Nr 3 z 20 marca 2001 roku, poz. 32.

niejawnych niewątpliwie spowodują konieczność nowelizacji wyszczególnionych powyżej, obowiązujących w Siłach Zbrojnych RP, dokumentów normatywnych.

4. Istota informacji niejawnych, organizacja systemu ich ochrony.

Istota informacji niejawnych sprowadza się do konieczności ich ochrony. Ustawa o ochronie informacji niejawnych określa dwie kategorie informacji, podlegających prawnej ochronie. Są to informacje stanowiące tajemnicę państwową *(o klauzuli ŚCIŚLE TAJNE i TAJNE)* oraz tajemnicę służbową *(o klauzuli POUFNE i ZASTRZEŻONE)*.

Przez **tajemnicę państwową** rozumieć należy informację niejawną określoną w wykazie rodzajów informacji niejawnych, stanowiącym Załącznik nr 1 do ustawy, której nieuprawnione ujawnienie może spowodować istotne zagrożenie dla podstawowych interesów Rzeczypospolitej Polskiej a w szczególności dla niepodległości lub nienaruszalności terytorium, interesów obronności, bezpieczeństwa państwa i obywateli albo narazić te interesy na co najmniej znaczną szkodę.

Informacje o klauzuli ŚCIŚLE TAJNE to takie informacje, których nieuprawnione ujawnienie mogłoby spowodować istotne zagrożenie dla niepodległości, nienaruszalności terytorium, polityki zagranicznej, stosunków międzynarodowych Rzeczypospolitej Polskiej, mogłoby zagrażać nieodwracalnymi lub wielkimi stratami dla interesów obronności, bezpieczeństwa państwa i obywateli a także innych istotnych interesów państwa albo narazić je na szkodę w wielkich rozmiarach. Załącznik nr 1 do ustawy zalicza tu 30 rodzajów informacji, wśród których są między innymi:

- informacje dotyczące zagrożeń zewnętrznych bezpieczeństwa państwa o charakterze militarnym, plany i prognozowanie obronne oraz wynikające z nich decyzje i zadania;
- struktura, organizacja i funkcjonowanie systemu kierowania państwem oraz dowodzenia Siłami Zbrojnymi w czasie zagrożenia państwa i wojny;

- lokalizacja, wyposażenie, właściwości ochronne i organizacja obrony stanowisk kierowania państwem i stanowisk dowodzenia Siłami Zbrojnymi w czasie zagrożenia państwa i wojny;
- informacje i przedmioty uzyskane w wyniku zastosowania środków technicznych umożliwiających uzyskiwanie w sposób tajny informacji oraz utrwalanie dowodów, a także w wyniku zastosowania kontroli korespondencji;
- gospodarowanie środkami budżetowymi i mieniem państwowym na cele specjalne;
- informacje niejawne wymieniane przez Polskę z NATO, Unią Europejską i innymi organizacjami międzynarodowymi i państwami, oznaczone klauzulą "TOP SECRET"[70] lub równorzędną.

Informacje TAJNE - to takie informacje, których nieuprawnione ujawnienie mogłoby spowodować zagrożenie dla międzynarodowej pozycji państwa, interesów obronności, bezpieczeństwa państwa i obywateli, innych istotnych interesów państwa albo narazić je na znaczną szkodę. W Załączniku nr 1 do ustawy informacje o klauzuli TAJNE dzielą się na dwie podgrupy:

- TAJNE ze względu na obronność i bezpieczeństwo państwa oraz porządek publiczny. Lista tego typu informacji zawiera 40 pozycji, do których między innymi zaliczamy;
  / planowanie, rozmieszczenie i stan rezerw państwowych,
  / plany i prognozy rozwoju organizacyjnego i technicznego Sił Zbrojnych oraz poszczególnych rodzajów wojsk,
  / plany obrony cywilnej państwa oraz plany obrony cywilnej województw,
  / szczegółowe informacje dotyczące funkcjonowania systemu ochrony informacji niejawnych stanowiących tajemnicę państwową,

[70] Ustawa określa jako odpowiednik polskiej klauzuli ŚCIŚLE TAJNE natowską klauzulę TOP SECRET. Jednakże dokumenty natowskie definiują klauzulę COSMIC TOP SECRET jako najwyższą z obowiązujących w NATO. W dalszej części pracy klauzule tajności, pojęcia i nazwy pochodzące z dokumentów normatywnych Sojuszu, po przytoczeniu ich tłumaczenia będą używane w oryginalnej wersji językowej.

/ informacje dotyczące planowania, rozmieszczenia, przeznaczenia i wyposażenia obiektów i nieruchomości specjalnych oraz plany ich obrony i ochrony,

/ informacje niejawne wymieniane przez Rzeczpospolitą Polską z Organizacją Traktatu Północnoatlantyckiego, Unią Europejską i innymi organizacjami międzynarodowymi i państwami, oznaczone klauzulą "SECRET" lub równorzędną,

- TAJNE ze względu na ważny interes państwa, do których zalicza się 26 rodzajów informacji, wśród których znajdują się na przykład;

/ materiały dla Rady Ministrów dotyczące potencjału strategicznego państwa oraz strategicznych zamówień rządowych i ich realizacji,

/ limit rezerwy specjalnej krajowych znaków pieniężnych w Narodowym Banku Polskim,

/ informacje o organizacji i zabezpieczeniu transportów wartości pieniężnych przekraczających równowartość kwoty 500 tys. EURO organizowanych przez banki państwowe oraz przedsiębiorstwa produkujące znaki pieniężne,

/ decyzje o skokowych zmianach kursu złotego w stosunku do walut obcych (dewaluacja, rewaluacja) dokonywane przez Narodowy Bank Polski do czasu podania ich do publicznej wiadomości,

/ informacje dotyczące rozwiązań technicznych, technologicznych i organizacyjnych, których ujawnienie naraziłoby na szkodę ważny interes gospodarczy państwa,

/ informacje niejawne wymieniane przez Rzeczpospolitą Polską z Organizacją Traktatu Północnoatlantyckiego, Unią Europejską i Unią Zachodnioeuropejską oraz z innymi organizacjami międzynarodowymi i państwami, oznaczone klauzulą "SECRET" lub równorzędną.

Należy podkreślić, iż wyżej wymieniony załącznik do ustawy nie stanowi - pomimo enumeratywnego charakteru wyliczenia - zamkniętego katalogu tajemnic państwowych, bowiem uregulowania dotyczące informacji o takim charakterze spotyka się także w innych ustawach. Przykładowo można tu wymienić:

- ustawę z dnia 25 czerwca 1997 r. o świadku koronnym[71], która w art. 23 stanowi, iż tajemnicę państwową stanowią przebieg i treść zeznań świadka koronnego zawierające informacje, które mogą przyczynić się do ujawnienia okoliczności przestępstwa, wykrycia pozostałych sprawców, ujawnienia dalszych przestępstw lub zapobieżenia im a także dotyczące osób uczestniczących w przestępstwie, do chwili wydania przez sąd postanowienia o dopuszczeniu dowodu z zeznań świadka koronnego. Tajemnicę państwową stanowią też okoliczności dotyczące ochrony lub pomocy, którą objęty został świadek koronny lub osoba dla niego najbliższa.
- ustawę z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej - Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu[72], której art. 39 stanowi, że tajemnicą państwową jest zastrzeżenie dostępu, na czas określony, do określonych dokumentów, jeżeli jest to konieczne dla bezpieczeństwa państwa. Dokumenty te stanowią wyodrębniony, tajny zbiór w archiwum Instytutu Pamięci i podlegają szczególnej ochronie. Zastrzeżenie wydaje szef Agencji Bezpieczeństwa Wewnętrznego, szef Agencji Wywiadu lub minister obrony narodowej.
- ustawę z dnia 30 czerwca 2000 roku Prawo własności przemysłowej[73], która w art. 57 określa, iż tajemnicę państwową stanowi wynalazek tajny. W rozumieniu ustawy tajnym jest wynalazek dokonany przez obywatela polskiego, jeśli dotyczy obronności lub bezpieczeństwa państwa *(rodzaje broni, sprzętu wojskowego, sposoby walki, środki techniczne stosowane przez służby państwowe, uprawnione do wykonywania czynności operacyjno – rozpoznawczych, nowe rodzaje wyposażenia i sprzętu oraz sposoby ich wykorzystania przez te służby)*. O tajności wynalazku lub zniesieniu tej tajności decydują minister Obrony Narodowej, minister Spraw Wewnętrznych i Administracji lub szef Agencji Bezpieczeństwa Wewnętrznego.

---

[71] Ustawa z dnia 25 czerwca 1997 r. o świadku koronnym, Dz. U. Nr 114 z 1997 r., poz. 738 z późniejszymi zmianami.
[72] Ustawa z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, Dz. U. Nr 155 z 1998 r., poz. 1016 z późniejszymi zmianami.
[73] Ustawa z dnia 30 czerwca 2000 roku Prawo własności przemysłowej, Dz. U. z 2001 roku, Nr 49, poz. 508.

Informacje stanowiące tajemnicę państwową podlegają ochronie w sposób określony w art. 25 ustawy, zgodnie z którym są chronione przez okres 50 lat od daty ich wytworzenia. Wyjątkiem od tej zasady są informacje chronione bez względu na upływ czasu. Należą do nich:

- dane identyfikujące funkcjonariuszy i żołnierzy służb ochrony państwa, wykonujących czynności operacyjno-rozpoznawcze;
- dane identyfikujące osoby, które udzieliły pomocy w zakresie czynności operacyjno-rozpoznawczych organom, służbom i instytucjom państwowym uprawnionym do ich wykonywania na podstawie ustawy;
- informacje niejawne uzyskane od innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia.

Po to, aby nie przechowywać niepotrzebnie informacji stanowiących tajemnicę państwową ustawa stanowi, iż Rada Ministrów może określić, w drodze rozporządzenia, które spośród informacji niejawnych oznaczonych klauzulą TAJNE przestały stanowić tajemnicę państwową, jeżeli od ich powstania upłynęło co najmniej 20 lat. Nie dotyczy to jednak informacji chronionych bez względu na upływ czasu.

Pomimo faktu, iż Załącznik nr 1 do ustawy stosunkowo precyzyjnie rozgranicza rodzaje informacji oznaczone klauzulami ŚCIŚLE TAJNE i TAJNE to jednak często osoby odpowiedzialne za nadanie określonemu dokumentowi klauzuli tajności mają trudności z precyzyjnym rozgraniczeniem pomiędzy informacją, która jest TAJNĄ a tą, która powinna zostać określona jako ŚCIŚLE TAJNA. Należy pamiętać o tym, że ustawodawca nie odpowiedział szczegółowo na wszystkie wątpliwości, jakie mogą pojawiać się w czasie oznaczania dokumentów niejawnych. Nie sposób bowiem przewidzieć wszystkiego i uregulować każdego szczegółu. Ustawa zdefiniowała różnicę pomiędzy informacjami oznaczonymi jako TAJNE i ŚCIŚLE TAJNE przez rozmiar szkód, jakie mogłoby spowodować ich nieuprawnione ujawnienie. W przypadku informacji ŚCIŚLE TAJNEJ jest to „istotne zagrożenie", są to „nieodwracalne lub wielkie straty" oraz „szkoda o wielkich rozmiarach", natomiast w przypadku informacji TAJNEJ jest to „zagrożenie", „istotna szkoda".

Wskazaniem, jaką klauzulą należy oznaczyć daną informację, jest także stopień jej ogólności. Na przykład, centralny plan mobilizacji gospodarki musi być oznaczony klauzulą ŚCIŚLE TAJNE, podczas gdy resortowe i wojewódzkie plany mobilizacji gospodarki należy oznaczyć klauzulą TAJNE. W przypadku informacji szczególnie wrażliwych, klauzula powinna być tym wyższa, im bardziej są one szczegółowe. Na przykład, szczegółowa struktura organizacyjna i etatowa jednostek organizacyjnych Wojskowych Służb Informacyjnych powinna być oznaczona klauzulą TAJNE, podczas gdy szczegółowa struktura organizacyjna oraz etatowa jednostek i komórek organizacyjnych Wojskowych Służb Informacyjnych wykonujących czynności operacyjno-rozpoznawcze musi być objęta klauzulą ŚCIŚLE TAJNE.

Tajemnicą służbową jest informacja niejawna nie będąca tajemnicą państwową, uzyskana w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, której nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej. Kategoria ta obejmuje dwie klauzule: POUFNE i ZASTRZEŻONE.

Informacje niejawne oznacza się klauzulą POUFNE w przypadku, gdy ich nieuprawnione ujawnienie spowodowałoby szkodę dla interesów państwa, interesu publicznego lub prawnie chronionego interesu obywateli. Natomiast klauzulę ZASTRZEŻONE stosuje się do informacji niejawnych, których nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej.

Informacją niejawną w rozumieniu ustawy nie będzie informacja podlegająca ochronie na podstawie innych przepisów na przykład Kodeksu Karnego[74] lub Ustawy o ochronie danych osobowych[75], jeżeli nie spełnia jednocześnie wymogów określonych w definicjach ustawowych. Informacja, która stanowi tajemnicę zawodową, np. tajemnica lekarska, tajemnica dziennikarska,

---

[74] Ustawa z dnia 6 czerwca 1997 roku Kodeks Karny, Dz. U. z 1997 roku, Nr 88, poz. 553 z późniejszymi. zmianami.

[75] Ustawa z dnia 29 stycznia 1997 roku o ochronie danych osobowych, Dz. U. Nr 133, poz. 883 z późniejszymi zmianami.

tajemnica adwokacka, nie jest z mocy tego faktu informacją niejawną i nie podlega ochronie przewidzianej w ustawie o ochronie informacji niejawnych.

Informacje POUFNE chronione są przez okres pięciu lat, z wyjątkiem materiałów geodezyjnych i kartograficznych oznaczonych tą klauzulą, które mogą podlegać ochronie przez okres dłuższy. Informacje ZASTRZEŻONE natomiast chronione są przez dwa lata. Osoba nadająca klauzulę tajności może określić krótszy okres ochrony tajemnicy służbowej. Może także, po dokonaniu przeglądu materiałów zawierających taką tajemnicę, przedłużać okres jej ochrony na kolejne okresy nie dłuższe niż 5 lat - dla oznaczonych klauzulą POUFNE i 2 lata - dla oznaczonych klauzulą ZASTRZEŻONE, nie dłużej jednak niż na okres do 50 lat od daty wytworzenia tych informacji.

W przeciwieństwie do tajemnicy państwowej, definicja tajemnicy służbowej nie odsyła do żadnych załączników ani wyliczeń. Szczegółowe uregulowania zawarte są w przepisach ustaw regulujących zakres obowiązków osób związanych stosunkiem służbowym. Przykładem może tu być Ustawa o Prokuraturze[76], stanowiąca w art. 48, iż „... Prokurator jest obowiązany zachować w tajemnicy okoliczności sprawy, o których w postępowaniu przygotowawczym, a także poza jawną rozprawą sądową, powziął wiadomość ze względu na swoje stanowisko prokuratora ...". Obowiązek zachowania tajemnicy trwa także po ustaniu stosunku służbowego. Obowiązek zachowania tajemnicy ustaje, gdy prokurator składa zeznania jako świadek w postępowaniu przygotowawczym lub przed sądem, chyba że ujawnienie tajemnicy zagraża dobru Państwa albo takiemu ważnemu interesowi prywatnemu, który nie jest sprzeczny z celami wymiaru sprawiedliwości. W takich wypadkach od obowiązku zachowania tajemnicy może zwolnić prokuratora Prokurator Generalny.

Organizacja systemu ochrony informacji niejawnych

Zgodnie z duchem ustawy, dostęp do informacji, posiadających klauzulę tajności oparty jest na generalnej zasadzie potrzeby wiedzy *(ang. need to know)*,

[76] Ustawa z dnia 20 czerwca 1985 r. o Prokuraturze, Dz. U. z 2002 roku., Nr 21, poz. 206

sprecyzowanej w art. 3. Zgodnie z nią informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy, pełnienia służby na zajmowanym stanowisku lub wykonywania pracy zleconej. Przez rękojmię zachowania tajemnicy należy rozumieć spełnienie ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem.

System ochrony informacji niejawnych, stworzony na podstawie postanowień ustawy i około ustawowych aktów normatywnych można rozpatrywać w następujących wymiarach:

- instytucjonalno – organizacyjnym;
- funkcjonalnym.

W wymiarze instytucjonalno – organizacyjnym postrzegany jest poprzez instytucje odpowiedzialne zarówno za przygotowanie norm prawnych, określających jego ramy jak i zasady funkcjonowania i składa się z następujących elementów:

- Kolegium do spraw Służb Specjalnych przy Radzie Ministrów RP,
- służby ochrony państwa;
  / Agencja Bezpieczeństwa Wewnętrznego,
  / Wojskowe Służby Informacyjne,
- kierownik jednostki organizacyjnej;
- pełnomocnik ochrony;
- pion ochrony.[77]

Kolegium do spraw Służb Specjalnych przy Radzie Ministrów RP jest powołanym na mocy ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu organem opiniodawczo-doradczym w sprawach programowania, nadzorowania i koordynowania działalności Agencji Bezpieczeństwa Wewnętrznego (ABW), Agencji Wywiadu (AW) i Wojskowych Służb Informacyjnych (WSI). Poza służbami specjalnymi w sferze zainteresowania Kolegium pozostają podejmowane dla ochrony bezpieczeństwa państwa działania

[77] Schemat, ukazujący zależności pomiędzy składowymi systemu znajduje się w Załączniku Nr 1.

Policji, Straży Granicznej, Żandarmerii Wojskowej, Służby Więziennej, Biura Ochrony Rządu, Inspekcji Celnej, organów celnych, urzędów skarbowych, izb skarbowych, organów kontroli skarbowej, organów informacji finansowej oraz służb rozpoznania Sił Zbrojnych Rzeczypospolitej Polskiej. Do zadań Kolegium należy między innymi formułowanie ocen lub wyrażanie opinii w sprawach:

- powoływania i odwoływania szefa ABW, szefa AW oraz szefa Wojskowych Służb Informacyjnych,
- kierunków i planów działania służb specjalnych,
- szczegółowych projektów budżetów służb specjalnych, przed rozpatrzeniem ich przez Radę Ministrów,
- projektów aktów normatywnych i innych dokumentów rządowych dotyczących działalności służb specjalnych,
- wykonywania przez służby specjalne powierzonych im zadań zgodnie z kierunkami i planami działania tych służb,
- rocznych sprawozdań przedstawianych przez szefów z działalności podległych im służb specjalnych,
- koordynowania działalności ABW, AW i WSI a także działalności służb specjalnych z Policją, Strażą Graniczną, Żandarmerią Wojskową, Biurem Ochrony Rządu, Inspekcją Celną, organami celnymi, urzędami skarbowymi, izbami skarbowymi, organami kontroli skarbowej, organami informacji finansowej i służbami rozpoznania Sił Zbrojnych Rzeczypospolitej Polskiej oraz ich współdziałania w dziedzinie ochrony bezpieczeństwa państwa,
- współdziałania służb specjalnych z właściwymi organami i służbami innych państw,
- organizacji wymiany informacji istotnych dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej pomiędzy organami administracji rządowej.

Poza wyszczególnionymi obszarami odpowiedzialności Kolegium bardzo istotną dziedziną jest opiniowanie w sprawach ochrony informacji niejawnych dotyczących w szczególności:

- zagrożeń o zasięgu ogólnokrajowym w zakresie ochrony informacji niejawnych, stanowiących tajemnicę państwową,
- sposobów postępowania w sytuacji zagrożenia o zasięgu ogólnokrajowym, powstałej wskutek ujawnienia informacji niejawnych stanowiących tajemnicę państwową oraz dokonywanie oceny skutków ujawnienia takich informacji,
- projektów aktów normatywnych i innych dokumentów rządowych dotyczących ochrony informacji niejawnych,
- innych spraw zlecanych przez Radę Ministrów lub prezesa Rady Ministrów oraz wnoszonych przez ministrów w zakresie realizacji zadań związanych z ochroną informacji niejawnych.[78]

W skład Kolegium wchodzą: prezes Rady Ministrów jako przewodniczący, sekretarz oraz członkowie:

- minister właściwy do spraw wewnętrznych,
- minister właściwy do spraw zagranicznych,
- minister obrony narodowej,
- minister właściwy do spraw finansów publicznych,
- szef Biura Bezpieczeństwa Narodowego.

W posiedzeniach Kolegium uczestniczą także szef ABW, szef AW, szef WSI oraz przewodniczący Sejmowej Komisji do Spraw Służb Specjalnych. W zależności od poruszanej tematyki na posiedzenia mogą być także delegowani bądź zapraszani przedstawiciele prezydenta RP, przewodniczący komisji sejmowych bądź organów państwowych.

Kolegium do spraw Służb Specjalnych, w lipcu 2002 roku, przejęło zadania realizowane od początku obowiązywania Ustawy o ochronie informacji niejawnych przez już nieistniejący Komitet Ochrony Informacji Niejawnych. W związku z tym, iż był to organ powołany w 1999 roku i funkcjonował przez pierwsze, jakże ważne lata kształtowania się systemu ochrony informacji niejawnych w Polsce celowym jest omówienie jego miejsca w systemie prawnym RP.

Komitet Ochrony Informacji Niejawnych *(w skrócie KOIN)* był, powołanym na mocy pierwotnej wersji Ustawy o ochronie informacji niejawnych organem, usytuowanym przy Radzie Ministrów, mającym kompetencje opiniodawczo-doradcze w sprawach kształtowania polityki w zakresie ochrony informacji niejawnych. W trakcie prac nad

---

[78] Art. 12 Ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

ustawą jego powołanie uzasadniano potrzebą koordynacji spraw związanych z ochroną informacji niejawnych w różnych działach administracji rządowej. Do zadań KOIN należało:

- ustalanie projektów generalnych założeń ochrony informacji niejawnych, w tym organizacyjnych i technicznych wymagań służących ochronie tych informacji w odniesieniu do głównych zagrożeń w tym zakresie;
- opiniowanie kierunków oraz planów postępowania w sytuacji szczególnego zagrożenia o zasięgu ogólnokrajowym, powstałej wskutek ujawnienia informacji niejawnych stanowiących tajemnicę państwową, w której wystarczające jest zastosowanie zwykłych środków konstytucyjnych;
- analiza i ocena oddziaływania na stan ochrony informacji niejawnych, sytuacji szczególnego zagrożenia lub innych zagrożeń oraz formułowanie opinii w tym zakresie;
- opracowywanie projektów dokumentów rządowych mających na celu zapewnienie spójności prawa polskiego w zakresie ochrony informacji niejawnych z zobowiązaniami wynikającymi z wiążących Rzeczpospolitą Polską umów międzynarodowych;
- opiniowanie projektów aktów normatywnych, projektów programów, analiz, sprawozdań i innych dokumentów rządowych dotyczących ochrony informacji niejawnych, a zwłaszcza;

  / systemu ochrony informacji niejawnych oraz podstaw jego funkcjonowania w odniesieniu do: przemysłu zbrojeniowego, obrotu uzbrojeniem i sprzętem specjalnym, badań naukowych i prac badawczo-rozwojowych prowadzonych na potrzeby obronności i bezpieczeństwa państwa, przygotowań mobilizacyjnych w gospodarce narodowej, tworzenia i gospodarowania rezerwami państwowymi oraz utrzymywania zdolności produkcyjnych i remontowych w gospodarce narodowej na potrzeby obronności państwa,

  / wymogów ochrony informacji niejawnych w planowaniu przestrzennym i rozbudowie infrastruktury gospodarczej, w tym łączności,
- rozpatrywanie innych spraw zlecanych przez Radę Ministrów i Prezesa Rady Ministrów oraz wnoszonych przez ministrów w dziedzinie realizacji zadań związanych z ochroną informacji niejawnych.

Komitetowi przewodniczył prezes Rady Ministrów, jego pierwszym zastępcą był minister spraw wewnętrznych i administracji, drugim - minister obrony narodowej.

Członkami KOIN byli ministrowie właściwi do spraw: zagranicznych, gospodarki, budżetu, finansów publicznych, sprawiedliwości, administracji publicznej oraz szefowie UOP i WSI a także nie więcej niż trzy osoby powołane przez prezesa Rady Ministrów ze względu na swoją wiedzę i doświadczenie. Oprócz tych osób udział w posiedzeniach mogli brać: inni ministrowie, zaproszeni do udziału w posiedzeniu w związku z rozpatrywaniem spraw należących do zakresu ich działań, przedstawiciel prezydenta RP, prezesi NIK i NBP oraz upoważnieni zastępcy członków KOIN (legitymujący się poświadczeniem bezpieczeństwa upoważniającym do ujawniania im określonych informacji niejawnych).

Szczegółowy zakres działania KOIN określało Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie szczegółowego trybu funkcjonowania Komitetu Ochrony Informacji Niejawnych, zasad udziału w jego posiedzeniach oraz zakresu czynności sekretarza Komitetu.[79] Wynikało z niego, że jawne *(przewodniczący mógł zarządzić tajność posiedzenia lub jego części)* posiedzenia odbywały się w obecności co najmniej połowy członków, z posiedzeń sporządzano protokół oraz pełny zapis, z zachowaniem przepisów o ochronie informacji niejawnych. W protokole odnotowywano stanowisko KOIN, o którego treści decydowała większość głosów; w razie równej ich liczby rozstrzygało stanowisko przewodniczącego. Osoba przegłosowana mogła zgłosić do protokołu stanowisko odrębne (*votum separatum).* Co roku KOIN sporządzał sprawozdanie ze swej działalności w celu przedstawienia Radzie Ministrów oraz przekazania prezydentowi RP i przewodniczącemu sejmowej Komisji do Spraw Służb Specjalnych.

Praktyka funkcjonowania KOIN wykazała, iż jako organ państwowy był bardzo potrzebny i właściwie spełnił swoją rolę. Działalność i efektywność KOIN można oceniać poprzez analizę rocznych sprawozdań z jego działalności przedstawianych Radzie Ministrów.

Jak wynika z rocznego sprawozdania za 1999 rok[80] organ ten formułował wnioski, ustalenia i rekomendacje do podejmowania działań przez służby ochrony państwa, organy administracji rządowej, instytucje państwowe oraz inne podmioty w związku z wymogami wynikającymi z Ustawy o ochronie informacji niejawnych a kluczowym problemem

---

[79] Rozporządzenie było opublikowane w Dz. U. z 1999 roku, Nr 18, poz. 158. Zostało uchylone mocą Ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

[80] Sprawozdanie z działalności KOIN w 1999 roku, Kancelaria Prezesa Rady Ministrów, Warszawa, styczeń 2000r.

omawianym w czasie każdego posiedzenia była ocena procesu wdrażania jej postanowień. Do przyjętych rekomendacji należały:

- konieczność dotrzymywania terminów ustawowych przy wprowadzaniu rozwiązań w sferze ochrony informacji niejawnych a zwłaszcza powoływania pełnomocników ochrony oraz tworzenia pionów ochrony;
- konieczność dotrzymywania terminów ustawowych w prowadzeniu postępowań sprawdzających;
- potrzeba aktywizacji szkolenia kadr odpowiedzialnych za wdrażanie przepisów ustawy oraz sprawdzania osób pełniących kierownicze funkcje, które odpowiadają za wdrażanie ustawy;
- potrzeba przyśpieszenia prac mających na celu uregulowanie problemów związanych z certyfikacją systemów i sieci teleinformatycznych oraz środków ochrony fizycznej;
- konieczność przyśpieszenia procesu przygotowywania dwustronnych porozumień o wymianie informacji niejawnych z innymi państwami, w tym z krajami członkowskimi NATO.

Ponadto w rezultacie zaleceń KOIN Ministerstwo Spraw Wewnętrznych i Administracji przesłało do urzędów stanu cywilnego zalecenie w sprawie udostępniania służbom ochrony państwa danych z akt stanu cywilnego w celu prowadzenia postępowań sprawdzających.

Jak wynika z przekazanego Radzie Ministrów rocznego sprawozdania z działalności Komitetu za 2000 rok[81] organ ten nadal formułował wnioski, ustalenia i rekomendacje do podejmowania działań przez służby ochrony państwa, organy administracji rządowej, instytucje państwowe oraz inne podmioty w związku z wymogami wynikającymi z ustawy o ochronie informacji niejawnych oraz kontynuował ocenę procesu wdrażania ustawy. Podstawą tych ocen były okresowe sprawozdania przedstawiane przez służby ochrony państwa;

Do decyzji i rekomendacji, jakie przyjął KOIN w 2000 roku należały między innymi:

- podjęcie przez pełnomocników ds. ochrony informacji niejawnych bardziej intensywnych działań w celu uniknięcia sytuacji, w których

[81] Informacja o działalności KOIN w 2000 roku, Kancelaria Prezesa Rady Ministrów, Warszawa, luty 2001.

osoby nie posiadające poświadczeń bezpieczeństwa wykonują prace związane z dostępem do informacji niejawnych;

- podjęcie przez Urząd Ochrony Państwa w konsultacji z Ministerstwem Spraw Zagranicznych i przedstawienie Radzie Ministrów projektu rozporządzenia określającego zasady wymiany informacji niejawnych pomiędzy NATO i Unią Zachodnioeuropejską;
- powołanie rządowej komisji, która koordynowałaby prace związane z oceną stanu bezpieczeństwa placówek i przedstawicielstw dyplomatycznych RP.

Analiza zagadnień rozpatrywanych przez KOIN w dwóch pierwszych latach obowiązywania ustawy pozwala na dokonanie uogólnienia, iż jego działalność ewoluowała i zmieniała się tak jak powstawał i rozwijał się system ochrony informacji niejawnych wprowadzony przez ustawę. Początkowo Komitet zajmował się głównie tworzeniem niezbędnej bazy normatywnej i organizacyjnej w państwie, która pozwoliłaby na sprawne funkcjonowanie wszystkich ogniw odpowiedzialnych za ochronę informacji a potem dokonywał ocen sprawności systemu. Głównymi podmiotami, których praca była poddawana ocenom Komitetu pozostawały służby ochrony państwa jako instytucje pełniące wiodącą funkcję w organizacji systemu ochrony i ciągłym nadzorze nad nim.

Należy się spodziewać, iż Kolegium do spraw Służb Specjalnych, bazując na doświadczeniach KOIN będzie się skupiało na rozpatrywaniu coraz bardziej szczegółowych czy jednostkowych problemów związanych z ochroną informacji niejawnych w kraju. W zasadzie system jest zbudowany, posiada niezbędne instrumenty prawne oraz przygotowane i sprawdzone kadry, w mentalności wykonawców, którzy mają dostęp do informacji niejawnych tworzą się zręby tak zwanej „kultury wykonawczej" i przeświadczenia o bezwzględnej konieczności ochrony informacji niejawnych, które są im powierzane.

Służby ochrony państwa to zgodnie z art. 2 Ustawy o ochronie informacji niejawnych Agencja Bezpieczeństwa Wewnętrznego i Wojskowe Służby Informacyjne. Pierwsza z nich jest centralnym organem administracji rządowej,

podlegającym prezesowi Rady Ministrów, druga pozostaje w strukturze Ministerstwa Obrony Narodowej i jest bezpośrednio podporządkowana ministrowi obrony narodowej. Niezależnie od różnego usytuowania na mapie organów państwa obie instytucje mają te same, wynikające z ustawy, prawa i obowiązki. Wojskowe Służby Informacyjne są właściwe do wykonywania obowiązków służby ochrony państwa wobec Sił Zbrojnych Rzeczypospolitej Polskiej, przedsiębiorców i jednostek naukowych lub badawczo – rozwojowych realizujących, łączące się z dostępem do informacji niejawnych, kontrakty lub wykonujących prace na rzecz obronności. Natomiast Agencja Bezpieczeństwa Wewnętrznego jest właściwa do realizacji zadań służby ochrony państwa wobec pozostałych podmiotów w państwie, które podlegają regulacjom zawartym w ustawie. W potocznym rozumieniu ABW jest służbą ochrony państwa w sferze cywilnej a WSI w sferze wojskowej. Stosownie do art. 14 Ustawy o ochronie informacji niejawnych służby ochrony państwa są właściwe do:

- kontroli ochrony informacji niejawnych oraz kontroli przestrzegania przepisów wydanych w tym zakresie;
- realizacji zadań w zakresie bezpieczeństwa systemów i sieci teleinformatycznych;
- prowadzenia postępowania sprawdzającego według zasad określonych w ustawie;
- ochrony informacji niejawnych wymienianych przez Rzeczpospolitą Polską z innymi państwami i organizacjami międzynarodowymi;
- szkolenia i doradztwa w zakresie ochrony informacji niejawnych;
- wykonywania innych zadań, w zakresie ochrony informacji niejawnych, określonych odrębnymi przepisami.

ABW i WSI w celu realizacji zadań związanych z ochroną informacji niejawnych mogą korzystać zarówno z informacji własnych jak i uzyskanych przez Policję, Straż Graniczną, Żandarmerię Wojskową oraz organy kontroli skarbowej. Mogą także zwracać się do tych służb i organów o udzielenie niezbędnej pomocy. Kwestie te reguluje Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie szczegółowego zakresu, warunków i trybu współdziałania organów,

służb i innych państwowych jednostek organizacyjnych ze służbami ochrony państwa w toku prowadzonych postępowań sprawdzających. Zgodnie z tym rozporządzeniem służby współdziałające mają 21 dni na przeprowadzenie czynności, o które wnosi właściwa służba ochrony państwa.

Ustawa daje służbom ochrony państwa szerokie uprawnienia kontrolne. Na mocy art. 16 ustawy, w zakresie niezbędnym do kontroli stanu bezpieczeństwa tajemnic państwowych, upoważnieni pisemnie funkcjonariusze ABW i żołnierze WSI mają prawo do:

- swobodnego wstępu do obiektów i pomieszczeń kontrolowanej jednostki, gdzie są wytwarzane, przechowywane lub przekazywane informacje niejawne;
- wglądu do dokumentów związanych z organizacją ochrony tych informacji w kontrolowanej jednostce organizacyjnej;
- żądania udostępnienia do kontroli sieci lub systemów teleinformatycznych służących do wytwarzania, przechowywania, przetwarzania lub przekazywania tych informacji;
- przeprowadzania oględzin obiektów, składników majątkowych i sprawdzania przebiegu określonych czynności związanych z ochroną tych informacji;
- żądania od kierowników i pracowników kontrolowanych jednostek organizacyjnych udzielania ustnych i pisemnych wyjaśnień oraz przekazania posiadanych przez nich informacji dotyczących działalności wywiadowczej albo terrorystycznej skierowanej przeciwko Rzeczypospolitej Polskiej, jej Siłom Zbrojnym, przedsiębiorcom, jednostkom naukowym lub badawczo – rozwojowym, w odniesieniu do prowadzonej produkcji albo usług stanowiących tajemnicę państwową ze względu na bezpieczeństwo lub obronność państwa a także na potrzeby Sił Zbrojnych;
- zasięgania, w związku z przeprowadzaną kontrolą, informacji w jednostkach nie kontrolowanych, jeżeli ich działalność pozostaje w związku z wytwarzaniem, przechowywaniem, przetwarzaniem,

przekazywaniem lub ochroną informacji niejawnych stanowiących tajemnicę państwową, oraz żądania wyjaśnień od kierowników i pracowników tych jednostek;

- korzystania z pomocy biegłych i specjalistów, jeżeli stwierdzenie okoliczności ujawnionych w czasie przeprowadzania kontroli wymaga wiadomości specjalnych;
- uczestniczenia w posiedzeniach kierownictwa, organów zarządzających lub nadzorczych, a także organów opiniodawczo – doradczych w sprawach dotyczących problematyki ochrony tych informacji w kontrolowanej jednostce organizacyjnej.

Do wykonywania przez funkcjonariuszy i żołnierzy służb ochrony państwa czynności kontrolnych mają zastosowanie przepisy ustawy o Najwyższej Izbie Kontroli[82]. Przewidziane w tej ustawie uprawnienia i obowiązki:

- Najwyższej Izby Kontroli przysługują służbom ochrony państwa;
- prezesa, wiceprezesa i pracownika Najwyższej Izby Kontroli przysługują odpowiednio szefowi, zastępcy szefa i upoważnionemu funkcjonariuszowi Agencji Bezpieczeństwa Wewnętrznego bądź upoważnionemu żołnierzowi Wojskowych Służb Informacyjnych.

Tryb prowadzenia kontroli określa Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie szczegółowego trybu prowadzenia przez służby ochrony państwa kontroli w zakresie ochrony informacji niejawnych stanowiących tajemnicę państwową. Ponadto wymienione Rozporządzenie określa zadania funkcjonariuszy i żołnierzy służb ochrony państwa nadzorujących oraz wykonujących czynności kontrolne w postępowaniu kontrolnym, szczegółowy tryb przygotowywania kontroli, dokumentowania czynności kontrolnych, sporządzania protokołu kontroli, wystąpienia pokontrolnego i informacji o wynikach przeprowadzanych kontroli.

Zgodnie z rozporządzeniem kontrola obejmuje badanie stanu zabezpieczenia informacji niejawnych, przestrzegania zasad ochrony informacji oraz stanu

---

[82] Ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli, Dz.U. z 1995 r., Nr 13, poz. 59 z późniejszymi zmianami.

zabezpieczenia sieci i systemów teleinformatycznych służących do wytwarzania, przechowywania, przetwarzania lub przekazywania informacji niejawnych. Kontrole prowadzone są zgodnie z rocznym planem zatwierdzonym przez szefa właściwej służby. Kontrolę nie ujętą w planie może zarządzić szef służby, jeżeli uzyska informację wskazującą na występowanie istotnych zagrożeń dla systemu ochrony tajemnicy państwowej. Służby ochrony państwa są zobowiązane do przechowywania akt kontroli.

Drugą poza działalnością kontrolną sferą działania i odpowiedzialności służb ochrony państwa jest bezpieczeństwo systemów i sieci teleinformatycznych. W art. 60 ustawa o ochronie informacji niejawnych stanowi, iż systemy i sieci teleinformatyczne, służące do wytwarzania, przechowywania, przetwarzania lub przekazywania informacji niejawnych stanowiących tajemnicę państwową podlegają szczególnej ochronie. Dlatego zarówno urządzenia jak i całe systemy bądź sieci muszą być certyfikowane. Co więcej, urządzenia i narzędzia kryptograficzne podlegają certyfikacji jeśli wytwarzają, przechowują, przetwarzają lub przekazują informacje niejawne stanowiące tajemnicę służbową i oznaczone są klauzulą POUFNE. Certyfikacją zajmują się służby ochrony państwa, które mają prawo wydania certyfikatu dopuszczającego urządzenie, system lub sieć do użytku po:

- przeprowadzeniu badań i oceny zdolności urządzenia, systemu lub sieci do ochrony informacji niejawnych przed nieuprawnionym ujawnieniem oraz przed możliwością narażenia ich bezpieczeństwa;
- przeprowadzeniu zgodnych z ustawą postępowań sprawdzających;
- zatwierdzeniu szczególnych wymagań bezpieczeństwa systemu lub sieci teleinformatycznej.

Szczegółowe regulacje dotyczące bezpieczeństwa teleinformatycznego, w tym określenie dla służb ochrony państwa wybranych obowiązków w tej dziedzinie zawarte są w Rozporządzeniu Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych.

W związku z tym, że certyfikacja jest bardzo ważną dziedziną odpowiedzialności, wymagającą specjalistycznej wiedzy od funkcjonariuszy i żołnierzy służb ochrony państwa, w ABW i w WSI stworzono nowe struktury skupiające specjalistów, informatyków a także utworzono jednostki certyfikujące zajmujące się bezpośrednio certyfikacją wyrobów oraz systemów i sieci teleinformatycznych. Za czynności związane z certyfikacją oraz za wydanie certyfikatu służby ochrony państwa pobierają opłaty, z części których zwolnione są jedynie jednostki budżetowe *(płacą jedynie za wydanie certyfikatu)*. Wysokość opłat określona jest w Rozporządzeniu Prezesa Rady Ministrów z dnia 16 lipca 2001 r. w sprawie wysokości opłat za przeprowadzenie przez służbę ochrony państwa czynności warunkujących wydanie certyfikatu dla systemu lub sieci teleinformatycznej, urządzenia lub narzędzia kryptograficznego oraz za wydanie tych certyfikatów.

Trzecią sferą odpowiedzialności jest prowadzenie postępowań sprawdzających. ABW i WSI są zobowiązane do prowadzenia poszerzonych i specjalnych postępowań sprawdzających wobec osób przed wydaniem poświadczenia bezpieczeństwa osobowego, uprawniającego do dostępu do informacji stanowiących tajemnicę państwową o klauzuli TAJNE i ŚCIŚLE TAJNE. Dotyczy to osób ubiegających się o stanowisko, zatrudnienie lub zlecenie prac, z którymi może łączyć się dostęp do informacji niejawnych, stanowiących tajemnicę państwową. Właściwość służb w tym zakresie została określona w art. 29 Ustawy o ochronie informacji niejawnych. Zgodnie z nim postępowania sprawdzające prowadzą:

- Wojskowe Służby Informacyjne - w przypadku ubiegania się osoby o zatrudnienie lub zlecenie prac związanych z obronnością państwa:
  / wobec żołnierzy pozostających w służbie czynnej w Siłach Zbrojnych i pracowników cywilnych wojska, z wyjątkiem jednostek wojskowych podporządkowanych ministrowi właściwemu do spraw wewnętrznych;
  / u przedsiębiorców, w jednostkach naukowych lub badawczo-rozwojowych, których organem założycielskim jest Minister Obrony Narodowej, a także w innych jednostkach organizacyjnych, w zakresie, w

jakim realizują one produkcję lub usługi, stanowiące tajemnicę państwową ze względu na obronność państwa i na potrzeby Sił Zbrojnych;

- u przedsiębiorców zajmujących się obrotem wyrobami, technologiami i licencjami objętymi tajemnicą państwową ze względu na obronność państwa, jeśli uczestnikami tego obrotu są Siły Zbrojne lub jednostki organizacyjne podległe Ministrowi Obrony Narodowej;
- w wojskowych organach ochrony państwa i wojskowych organach porządkowych;

- Agencja Bezpieczeństwa Wewnętrznego - w razie ubiegania się osoby o stanowisko, zatrudnienie lub zlecenie prac, z którymi może się łączyć dostęp do informacji stanowiących tajemnicę państwową w innych przypadkach niż wymienione powyżej.

Służby ochrony państwa prowadzą postępowania sprawdzające wobec przedsiębiorców, jednostek naukowych lub badawczo – rozwojowych, ubiegających się o zawarcie lub wykonujących umowę związaną z dostępem do informacji niejawnych stanowiących tajemnicę państwową przed wydaniem świadectwa bezpieczeństwa przemysłowego. Linia rozgraniczenia kompetencji w tej dziedzinie przebiega podobnie jak sformułowana powyżej w dziedzinie bezpieczeństwa osobowego.

W związku z trudnościami w interpretacji treści art. 29 Ustawy o ochronie informacji niejawnych, w konsekwencji z problemami z jednoznacznym określeniem granicy kompetencji pomiędzy służbami ochrony państwa w sferze realizacji postępowań sprawdzających przed wydaniem świadectwa bezpieczeństwa przemysłowego sprawą tą na jednym ze swych posiedzeń w 2001 roku zajął się KOIN. Było to niezbędne, bowiem obie służby ochrony państwa zetknęły się w owym czasie z koniecznością realizacji postępowań przed wydaniem świadectw bezpieczeństwa przemysłowego do kontraktów natowskich, realizowanych z funduszu Sojuszu, zarówno w kraju jak i za granicą oraz do innych kontraktów realizowanych na rzecz podmiotów zagranicznych w kraju i za granicą

Zgodnie z wykładnią KOIN przekazaną obu służbom ochrony państwa, Wojskowe Służby Informacyjne prowadzą postępowania sprawdzające wobec:

- przedsiębiorców, jednostek naukowych i badawczo – rozwojowych, podległych, podporządkowanych oraz tych dla których organem założycielskim jest minister obrony narodowej w przypadku ubiegania się bądź realizacji kontraktów niejawnych NATO w kraju i za granicą;
- przedsiębiorców, jednostek naukowych i badawczo – rozwojowych w przypadku ubiegania się bądź realizacji kontraktów niejawnych NATO, których zleceniodawcą jest minister obrony narodowej oraz innych kontraktów jeśli ich wykonanie ma bezpośredni związek z obronnością lub potrzebami Sił Zbrojnych RP.

W każdym innym przypadku niż wyszczególnione powyżej służbą ochrony państwa, właściwą do prowadzenia postępowań sprawdzających przed wydaniem świadectwa bezpieczeństwa przemysłowego jest Agencja Bezpieczeństwa Wewnętrznego.

Oba wymienione wyżej postępowania sprawdzające prowadzone są na zasadach odpłatności a wysokość opłat określona jest w Rozporządzeniu Prezesa Rady Ministrów z dnia 13 lipca 2001 r. w sprawie wysokości opłat za przeprowadzenie postępowania sprawdzającego przez służbę ochrony państwa oraz za wydanie świadectwa bezpieczeństwa przemysłowego.

Czwartą dziedziną działalności służb ochrony państwa jest ochrona informacji niejawnych wymienianych z innymi państwami i organizacjami. W art. 15 Ustawa o ochronie informacji niejawnych stanowi, iż w stosunkach międzynarodowych szef Agencji Bezpieczeństwa Wewnętrznego i szef Wojskowych Służb Informacyjnych pełnią funkcje krajowych władz bezpieczeństwa. Zapis ten jest praktyczną realizacją przepisów wynikających z regulacji natowskich w sferze bezpieczeństwa i ochrony informacji niejawnych, które definiują obowiązek wyznaczenia przez każde państwo członkowskie służby odpowiedzialnej za ochronę informacji niejawnych w relacjach międzynarodowych. Regulacja ta między innymi, upoważnia służby ochrony państwa do wydawania natowskich poświadczeń bezpieczeństwa osobowego *(ang NATO Personnel*

Security Clearance Certificate), natowskich świadectw bezpieczeństwa przemysłowego *(ang. Facility Security Clearance Certificate),* zawierania porozumień z innymi krajowymi władzami bezpieczeństwa, opiniowania międzynarodowych, rządowych i resortowych porozumień o współpracy w części dotyczącej ochrony informacji niejawnych a także do uznawania poświadczeń bezpieczeństwa osobowego i świadectw bezpieczeństwa przemysłowego wydanych przez inne władze bezpieczeństwa państw członkowskich NATO.

Piątą sferą odpowiedzialności służb ochrony państwa jest szkolenie i doradztwo w zakresie ochrony informacji niejawnych. ABW i WSI prowadzą szkolenie w stosunku do osób sprawujących najważniejsze stanowiska w państwie oraz do pełnomocników ochrony informacji. Szkolenia kończą się wydaniem zaświadczenia, którego wzór został określony w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 23 lutego 1999 r. w sprawie wzoru zaświadczenia stwierdzającego odbycie przeszkolenia w zakresie ochrony informacji niejawnych. Zgodnie z art. 54 ustawy szkolenie ma na celu zapoznanie z:

- zagrożeniami ze strony obcych służb specjalnych działających przeciwko Rzeczypospolitej Polskiej i państwom sojuszniczym a także z zagrożeniami ze strony organizacji terrorystycznych;
- przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności za ich ujawnienie;
- zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby;
- sposobami ochrony informacji niejawnych stanowiących tajemnicę państwową oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia;
- odpowiedzialnością karną, dyscyplinarną i służbową za naruszenie przepisów o ochronie informacji niejawnych.

Oprócz powyżej omówionych dziedzin odpowiedzialności służb ochrony państwa jest wiele innych szczegółowych zadań, które one realizują. Każdy bowiem dzień przynosi nowe, nie przewidziane w ustawie i innych aktach normatywnych sytuacje, które wymagają uregulowania bądź natychmiastowego działania. Poziom

ochrony informacji niejawnych bezpośrednio wpływa na bezpieczeństwo państwa, dlatego też wszystkie, nawet najbardziej szczegółowe kwestie muszą znaleźć swoje rozwiązania czy interpretacje. Jest to podstawową powinnością służb ochrony państwa, jako zasadniczego elementu polskiego systemu ochrony informacji niejawnych.

Kierownik jednostki organizacyjnej jest kluczowym elementem systemu ochrony informacji niejawnych na poziomie jednostki organizacyjnej, w której są one wytwarzane, przetwarzane, przekazywane lub przechowywane. Jest on zobowiązany między innymi do:

- stworzenia skutecznego systemu ochrony informacji w kierowanej jednostce organizacyjnej poprzez powołanie pełnomocnika ochrony i budowę podlegającego pełnomocnikowi pionu ochrony;
- określenia stanowisk lub rodzajów prac zleconych, z którymi może łączyć się dostęp do informacji niejawnych, odrębnie dla każdej klauzuli tajności.

Kierownik jednostki organizacyjnej wyraża zgodę na udostępnienie informacji niejawnych stanowiących tajemnicę służbową, które zostały wytworzone w kierowanej przez niego jednostce organizacyjnej oraz występuje do właściwej służby ochrony państwa z wnioskiem o przeprowadzenie postępowania sprawdzającego wobec podległych mu pracowników przed upoważnieniem ich do dostępu do informacji stanowiących tajemnicę państwową.

Pełnomocnik ochrony jest głównym elementem systemu ochrony informacji niejawnych w jednostce organizacyjnej. Podlega bezpośrednio kierownikowi jednostki i odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych. W art. 18 ustawa określa, iż pełnomocnikiem ochrony może być osoba, która:

- posiada obywatelstwo polskie;
- posiada co najmniej średnie wykształcenie;

- posiada odpowiednie poświadczenie bezpieczeństwa wydane przez służbę ochrony państwa;
- odbyła przeszkolenie w zakresie ochrony informacji niejawnych.

Pełnomocnik ochrony kieruje wyspecjalizowaną komórką organizacyjną do spraw ochrony informacji niejawnych, zwaną pionem ochrony. Do jej zadań należy:

- zapewnienie ochrony informacji niejawnych;
- ochrona systemów i sieci teleinformatycznych;
- zapewnienie ochrony fizycznej jednostki organizacyjnej;
- kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji;
- okresowa kontrola ewidencji, materiałów i obiegu dokumentów, opracowywanie planu ochrony jednostki organizacyjnej i nadzorowanie jego realizacji;
- szkolenie pracowników w zakresie ochrony informacji niejawnych.

Pracownikiem pionu ochrony może być osoba, która:

- posiada obywatelstwo polskie;
- posiada odpowiednie poświadczenie bezpieczeństwa wydane przez służbę ochrony państwa lub pełnomocnika ochrony;
- odbyła przeszkolenie w zakresie ochrony informacji niejawnych.

W skład pionu ochrony, w zależności od potrzeb jednostki organizacyjnej mogą wchodzić;

- kierownik i personel kancelarii tajnej;
- administrator systemów i sieci teleinformatycznych;
- inspektor bezpieczeństwa teleinformatycznego.

Pełnomocnik ochrony jest zobowiązany do współpracy ze służbami ochrony państwa w zakresie realizacji swoich zadań oraz informowania na bieżąco kierownika jednostki organizacyjnej o przebiegu tej współpracy. W przypadku ujawnienia informacji oznaczonej klauzulą POUFNE lub wyższą pełnomocnik ochrony zawiadamia obligatoryjnie właściwą służbę ochrony państwa. Również w przypadku odmowy wydania poświadczenia bezpieczeństwa, po zakończeniu

zwykłego postępowania sprawdzającego, pełnomocnik ochrony jest zobowiązany do powiadomienia o tym fakcie właściwej służby ochrony państwa.

W wymiarze funkcjonalnym system ochrony informacji niejawnych należy postrzegać jako konieczność zapewnienia bezpieczeństwa informacji i wypełnienia przez jednostki organizacyjne, w których dyspozycji znajdują się informacje niejawne, określonych obowiązków. Należą do nich:

- ***Obowiązek uzyskania poświadczenia bezpieczeństwa osobowego.***

Ustawa stanowi, że informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo innej zleconej pracy.

Warunkiem uzyskania takiego uprawnienia - poświadczenia bezpieczeństwa osobowego jest pozytywny wynik postępowania sprawdzającego. Wszczęcie postępowania jest uzależnione od pisemnej zgody osoby sprawdzanej a jego zakres zależy od charakteru informacji, do których dopuszczona ma być sprawdzana osoba. Najmniejszy jest przy postępowaniu zwykłym dla uzyskania dostępu do tajemnicy służbowej, szerszy przy informacjach TAJNYCH, zaś specjalny - przy ŚCIŚLE TAJNYCH. W trakcie postępowania ustala się m.in., czy występują związane z tą osobą okoliczności powodujące ryzyko jej podatności na szantaż lub wywieranie presji albo czy istnieją wątpliwości dotyczące zagrożenia osoby sprawdzanej ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania z nią kontaktu, a zwłaszcza obawy o wywieranie w tym celu presji. Służby ochrony państwa muszą także ustalić, czy nie istnieją wątpliwości związane z wyraźną różnicą między poziomem życia osoby sprawdzanej a uzyskiwanymi przez nią dochodami albo ewentualnymi informacjami o chorobie psychicznej, uzależnieniu od alkoholu, narkotyków. W celu ustalenia tych ostatnich okoliczności służby ochrony państwa mogą zobowiązać osobę sprawdzaną do poddania się specjalistycznym badaniom. Elementem procedury sprawdzającej jest wielostronicowa ankieta, najbardziej szczegółowa dla osób, które stykają się z informacjami TAJNYMI i ŚCIŚLE TAJNYMI. Pytania tej ankiety dotyczą, oprócz

osoby sprawdzanej, także jej rodziny, współmieszkańców, ewentualnych wspólników, pracodawcy *(zarówno aktualnego jak i poprzednich)*, a nawet właściciela zajmowanego mieszkania. Szczegółowo należy odpowiedzieć na pytania dotyczące m. in. stanu konta bankowego, stanu zdrowia, nałogów, karalności, współpracy z dawnymi służbami specjalnymi, wyjazdów zagranicznych. Dane zawarte w ankiecie podlegają kontroli poprzez m. in.: sprawdzenie ich w rejestrach państwowych, aktach stanu cywilnego, przeprowadzenie rozmowy z osobą sprawdzaną, wywiadu w miejscu zamieszkania, rozmowę z przełożonymi oraz innymi osobami, *(jeśli jest to konieczne na podstawie uzyskanych informacji)* a w przypadku informacji ŚCIŚLE TAJNYCH - także rozmowy z trzema osobami wskazanymi przez osobę sprawdzaną w celu potwierdzenia jej tożsamości.

Sprawdzenia osób ubiegających się o stanowiska lub prace, z którymi łączy się dostęp do tajemnic służbowych dokonuje pełnomocnik ochrony na pisemne polecenie kierownika jednostki organizacyjnej. Pełnomocnik wydaje bądź odmawia wydania poświadczenia bezpieczeństwa z tym, że odmowa taka nie jest wiążąca dla osoby upoważnionej do obsady stanowiska, z którym łączy się dostęp do tajemnic służbowych. Konieczne jest jednak poinformowanie o takim fakcie właściwej służby ochrony państwa.

W przypadku informacji niejawnych opatrzonych klauzulą TAJNE i ŚCIŚLE TAJNE czynności takich dokonują, na pisemny wniosek osoby upoważnionej do obsady stanowiska, Wojskowe Służby Informacyjne w sferze wojskowej oraz Agencja Bezpieczeństwa Wewnętrznego w sferze cywilnej. Postępowania sprawdzającego nie przeprowadza się, jeśli kandydat nie posiada obywatelstwa polskiego lub został skazany prawomocnym wyrokiem za przestępstwo umyślne ścigane z oskarżenia publicznego, gdyż osoba taka, z mocy art. 28 ustawy nie może być dopuszczona do pracy lub pełnienia służby na stanowisku albo do wykonywania prac zleconych, z którymi łączy się dostęp do tajemnicy państwowej. Służby mundurowe *(ABW, AW, WSI, Policja, Żandarmeria Wojskowa, Służba Więzienna)* przeprowadzają we własnym zakresie postępowanie sprawdzające wobec osób zatrudnionych i ubiegających się o przyjęcie do pracy w tych służbach. W trakcie postępowania sprawdzającego służby ochrony państwa mogą, w celu

uzyskania informacji o osobie sprawdzanej, zwracać się z pisemnym wnioskiem do kierowników jednostek organizacyjnych oraz służb współdziałających o przekazanie informacji oraz udostępnienie niezbędnych dokumentów. W niektórych sytuacjach chodzi nie tyle o odpowiedź, ile o udostępnienie upoważnionemu funkcjonariuszowi lub żołnierzowi służby ochrony państwa niezbędnych dokumentów. Uzyskaną korespondencję i dokumentację włącza się do akt postępowania sprawdzającego. Akta te mogą być udostępniane jedynie osobie sprawdzanej, osobie upoważnionej do obsadzenia stanowiska oraz na pisemne żądanie sądu lub prokuratora w celu ścigania karnego.

Z obowiązku przeprowadzenia postępowania sprawdzającego wyłączone są osoby sprawujące najwyższe urzędy w państwie: prezydent RP, marszałkowie Sejmu i Senatu, prezes Rady Ministrów, pierwszy prezes Sądu Najwyższego, prezes Naczelnego Sądu Administracyjnego, prezes Trybunału Konstytucyjnego, prezes Najwyższej Izby Kontroli, prezes Narodowego Banku Polskiego i rzecznik praw obywatelskich. Wyłączeni są także posłowie i senatorowie, chyba, że zachodzi konieczność przeprowadzenia tego postępowania w związku z dopuszczeniem do tajemnic opatrzonych klauzulą ŚCIŚLE TAJNE.

Po pozytywnym zakończeniu postępowania osobie sprawdzanej wydaje się poświadczenie bezpieczeństwa a po przeprowadzeniu szkolenia w zakresie ochrony informacji niejawnych stosowne zaświadczenie.

Kolejne postępowania sprawdzające wobec osób mających dostęp do informacji POUFNYCH prowadzone są, co 10 lat; TAJNYCH - co 5 lat, ŚCIŚLE TAJNYCH - co 3 lata. W razie wątpliwości, czy dana osoba daje rękojmię zachowania tajemnicy, kolejne sprawdzenie może być dokonane wcześniej.

- ***Obowiązek zorganizowania kancelarii tajnych.***

Kancelaria tajna to wyodrębniona komórka organizacyjna, podlegająca bezpośrednio pełnomocnikowi ochrony, odpowiedzialna za rejestrowanie, przechowywanie, obieg i wydawanie niejawnych dokumentów. Kancelarią kieruje kierownik wyznaczony przez kierownika jednostki organizacyjnej na wniosek pełnomocnika ochrony. Winna być ona zorganizowana w oddzielnym pomieszczeniu, zabezpieczonym zgodnie z przepisami o środkach ochrony

fizycznej informacji niejawnych i być obsługiwana przez pracowników pionu ochrony. Kancelarie tajne prowadzą rejestry dokumentów, w tym m. in.: karty zapoznania się z dokumentami niejawnymi, dziennik korespondencji dokumentów, rejestr teczek dokumentów niejawnych. Kancelarie muszą być organizowane odrębnie dla dokumentów o określonej klauzuli tajności, z tym, że dopuszczalne jest zorganizowanie jednej kancelarii, pod warunkiem, że dokumenty o różnych klauzulach są fizycznie od siebie oddzielone i obsługiwane przez osobę posiadającą poświadczenie bezpieczeństwa, odpowiednie do najwyższej klauzuli wytwarzanych, przetwarzanych, przekazywanych lub przechowywanych w kancelarii dokumentów. W celu właściwej ochrony informacji niejawnych sposób ich przyjmowania, przewożenia, wydawania i ochrony przed nieuprawnionym ujawnieniem, utratą, uszkodzeniem lub zniszczeniem przez podmioty wykonujące czynności lub świadczące usługi są szczegółowo określonych w przepisach o ochronie informacji niejawnych.

- ***Obowiązek szkolenia w zakresie informacji niejawnych.***

Odbycie przeszkolenia w zakresie ochrony informacji niejawnych, prowadzone przez pełnomocnika ochrony lub służbę ochrony państwa jest drugim, obok posiadania poświadczenia bezpieczeństwa, warunkiem uzyskania dostępu do informacji niejawnych. Ma ono na celu zapoznanie z: zagrożeniami ze strony obcych służb specjalnych i organizacji terrorystycznych; przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności za ich ujawnienie; sposobami ochrony oraz postępowania w sytuacjach zagrożenia lub w przypadku ich ujawnienia; odpowiedzialnością karną, dyscyplinarną i służbową za naruszenie przepisów o ochronie informacji niejawnych. Dla osób spoza resortu obrony narodowej szkolenie odbywa się na zasadach odpłatności a jego koszty pokrywa zainteresowana jednostka organizacyjna.

- ***Obowiązek stosowania środków ochrony fizycznej.***

W jednostkach organizacyjnych, w których znajdują się informacje niejawne muszą być stosowane środki ochrony fizycznej w celu uniemożliwienia osobom postronnym dotarcia do nich. Muszą one być wystarczające, aby chronić informacje niejawne przed: działaniem obcych służb specjalnych; zamachem terrorystycznym

lub sabotażem; kradzieżą lub zniszczeniem; próbą wejścia osób nieuprawnionych; nieuprawnionym dostępem pracowników do informacji opatrzonych wyższą klauzulą tajności. Zakres tych środków jest uzależniony od rodzaju klauzuli, jaką opatrzone są materiały niejawne. Polegać one mają m.in. na: szczególnej kontroli wejść i wyjść; wydzieleniu strefy kontroli osób i pojazdów; wprowadzeniu systemu specjalnych przepustek; stosowaniu certyfikowanych sejfów, zamków, krat, systemów antywłamaniowych i alarmowych oraz urządzeń chroniących przed podsłuchem i podglądem.

- ***Obowiązek stosowania zabezpieczeń systemów i sieci teleinformatycznych.***

Ustawodawca, ze względu na wagę bezpieczeństwa tych systemów i sieci, poddał je szczególnej ochronie służb ochrony państwa. Służby te dopuszczają do użytkowania właściwe urządzenia jako bezpieczne, potwierdzają przydatność algorytmów i środków ich ochrony a także certyfikują systemy służące wytwarzaniu, przechowywaniu, przetwarzaniu lub przekazywaniu informacji niejawnych.

Dla każdego systemu lub sieci, w których mogą być przetwarzane informacje niejawne, opracowuje się na etapie projektowania szczególne wymagania bezpieczeństwa i procedury bezpieczeństwa. Powinny one określać wielkość i lokalizację stref bezpieczeństwa oraz środki ich ochrony odpowiednie dla danej jednostki. Należy w nich określić m.in. zadania administratora, kategorię uprawnień użytkowników w zależności od klauzuli tajności, sposób realizowania połączeń zewnętrznych oraz wewnętrznych. Już na tym etapie ustala się także szczególne wymagania w zakresie szkoleń dla administratorów, pracowników pionu i wszystkich użytkowników sieci. Podłączenie systemu z zawartością tajemnic państwowych do sieci lub systemu powszechnie dostępnego jest dopuszczalne pod warunkiem ścisłego przestrzegania zasad kryptograficznych, natomiast w przypadku tajemnicy służbowej wystarczająca jest kontrola dostępu ustalona poprzez administratora systemów i sieci *(m. in. poprzez przydzielanie użytkownikom kont i haseł)*.

- ***Obowiązek uzyskania świadectwa bezpieczeństwa przemysłowego.***

Przedsiębiorcy, jednostki naukowe lub badawczo-rozwojowe, starające się o zawarcie umowy lub wykonujące umowę, z którą łączy się dostęp do tajemnicy państwowej muszą obowiązkowo spełnić określone warunki. Część tych obowiązków określa umowa, pozostałe o charakterze podstawowym, reguluje ustawa. Zdolność wymienionych podmiotów do zapewnienia ochrony informacji niejawnych jest oceniana w postępowaniu sprawdzającym. W jego trakcie służby ochrony państwa analizują m.in. strukturę i pochodzenie kapitału przedsiębiorcy; jego sytuację finansową i źródła pochodzenia środków pozostających w jego dyspozycji a także konkretne osoby oraz funkcjonujący u przedsiębiorcy system ochrony. Efektem postępowania jest wydanie bądź odmowa wydania świadectwa bezpieczeństwa przemysłowego. Odmowa wydania nie wymaga uzasadnienia, jednakże przedsiębiorca, jednostka naukowa lub badawczo-rozwojowa powinna zostać poinformowana, że jej przedstawiciel może zapoznać się z zebranymi danymi, chyba, że zagraża to bezpieczeństwu państwa. W taki sposób sprawdzane są zarówno przedsiębiorstwa krajowe jak i zagraniczne.

- ***Obowiązek przestrzegania zasad udostępniania informacji niejawnych***

Ustawodawca przewidział możliwość udostępniania informacji niejawnych tylko w szczególnie uzasadnionych przypadkach. W przypadku tajemnicy państwowej pisemną zgodę na to mogą wydać: szefowie Kancelarii Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu lub Prezesa Rady Ministrów albo minister właściwy dla określonego działu administracji rządowej lub kierownik urzędu centralnego, a w przypadku ich braku - właściwa służba ochrony państwa.

Natomiast na udostępnienie informacji niejawnych stanowiących tajemnicę służbową zgodę może wyrazić na piśmie kierownik jednostki organizacyjnej *(ale tylko i wyłącznie w odniesieniu do informacji wytworzonych w tej jednostce).* W każdym przypadku pisemna zgoda musi określać zakres podmiotowy i przedmiotowy udostępnienia.

W przypadku innych aktów prawnych zasady udostępniania informacji niejawnych i zwalniania z obowiązku zachowania tajemnicy są następujące:

- na podstawie Ustawy o Instytucie Pamięci Narodowej - Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu zgodę taką może także wydać prezes Instytutu - „Prezes ... może, w szczególnie uzasadnionych wypadkach, zezwolić na ujawnienie wiadomości stanowiącej tajemnicę państwową lub służbową oraz na udostępnienie dokumentów lub materiałów objętych tajemnicą państwową określonej osobie lub instytucji, jeżeli zachowanie tajemnicy uniemożliwiałoby wykonanie wskazanych w ustawie zadań Instytutu Pamięci"[83];
- zasady zwalniania od obowiązku zachowania tajemnicy państwowej i służbowej w postępowaniu przed sądami i innymi organami określają przepisy Kodeksu Postępowania Karnego. Kodeks stanowi, iż „ Osoby obowiązane do zachowania tajemnicy państwowej mogą być przesłuchane co do okoliczności, na które rozciąga się ten obowiązek, tylko po zwolnieniu tych osób od obowiązku zachowania tajemnicy przez uprawniony organ przełożony. Zwolnienia wolno odmówić tylko wtedy, gdyby złożenie zeznania wyrządzić mogło poważną szkodę państwu. Sąd lub prokurator może zwrócić się do właściwego naczelnego organu administracji rządowej o zwolnienie świadka od obowiązku zachowania tajemnicy."[84]
- w przypadku osób zobowiązanych do zachowania tajemnicy służbowej (adwokackiej, lekarskiej, dziennikarskiej), powołanych na świadka, o zwolnieniu od obowiązku decyduje sąd lub prokurator.[85] Osoby obowiązane do zachowania tajemnicy państwowej bądź służbowej przesłuchuje się zawsze na rozprawie z wyłączeniem jawności. Natomiast sposób przechowywania protokołów zeznań obejmujących okoliczności, na które rozciąga się obowiązek zachowania tajemnicy państwowej lub służbowej został określony przez ministra sprawiedliwości w Rozporządzeniu Ministra Sprawiedliwości z dnia 1 grudnia 1998 r. w

---

[83] Art. 22 Ustawy z dnia 18 grudnia 1998 r. O Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu.
[84] Art. 179 Ustawy z dnia 6 czerwca 1997r. Kodeks Postępowania Karnego, Dz. U. Nr 89, poz. 555 z późniejszymi zmianami.
[85] Tamże, art.180.

sprawie sposobu przechowywania protokołów zeznań obejmujących okoliczności, na które rozciąga się obowiązek zachowania tajemnicy państwowej, służbowej albo związanej z wykonywaniem zawodu lub funkcji.[86]

- ***Odpowiedzialność karna.***

Ustawa o ochronie informacji niejawnych nie zawiera przepisów dotyczących odpowiedzialności z tytułu nieuprawnionego przekazania komuś informacji niejawnych. Kwestię tę pozostawiono Kodeksowi Karnemu, który penalizuje takie zachowania.[87] Osoba popełniająca przestępstwo ujawnienia informacji, stanowiącej tajemnicę państwową podlega karze pozbawienia wolności od 3 miesięcy do lat 5 natomiast, jeśli informacja ujawniana jest osobie działającej w imieniu lub na rzecz podmiotu zagranicznego od 6 miesięcy do lat 8. Nieumyślne ujawnienie informacji stanowiącej tajemnicę państwową podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.[88]

Kodeks w tej części zawiera typ kwalifikowany ze względu na współpracę z podmiotem zagranicznym nie definiując jego istoty. Możemy mieć tu na uwadze na przykład: zagraniczne organizacje, instytucje, banki, koncerny, firmy konsultingowe, czyli, ogólnie rzecz biorąc, instytucje nie mające charakteru wywiadowczego. Natomiast nie można do podmiotu zagranicznego zaliczyć obcego wywiadu, gdyż przestępstwo brania udziału w działalności obcego wywiadu (szpiegostwo) jest stypizowane w rozdziale XVII: "Przestępstwa przeciwko Rzeczypospolitej Polskiej".[89]

Jak wynika z lektury Kodeksu Karnego zakres podmiotowy odpowiedzialności karnej za umyślne, bezprawne ujawnienie lub wykorzystanie tajemnicy państwowej jest bardzo szeroki - dotyczy wszystkich obywateli, do których wiadomości ona dotarła, bez względu na sposób w jaki się to stało. Osobom

---

[86] Dz. U. Nr 148, poz. 975.
[87] Rozdział XXXIII „Przestępstwa przeciwko ochronie informacji" Ustawy z dnia 6 czerwca 1997r. Kodeks Karny.
[88] Tamże, art. 265.
[89] Tamże, art. 130.

takim bezwzględnie nie wolno ujawnić lub wykorzystać wiadomości objętych tajemnicą państwową, nawet gdyby zapoznały się z nimi zupełnie przypadkowo.

Przestępstwem jest również ujawnienie tajemnicy służbowej. Osoba ujawniająca informację tego typu podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Natomiast funkcjonariusz publiczny ujawniający tajemnicę służbową, którą uzyskał w związku z wykonywaniem czynności służbowych podlega karze pozbawienia wolności do lat 3.[90]

[90] Tamże, art. 266.

ROZDZIAŁ II

SYSTEM OCHRONY INFORMACJI NIEJAWNYCH W SIŁACH ZBROJNYCH RP

1. Kompetencje, zakres odpowiedzialności i zasady współdziałania instytucji odpowiedzialnych za bezpieczeństwo i ochronę informacji niejawnych w sferze wojskowej.

Minister obrony narodowej posiada szereg uprawnień i obowiązków w sferze ochrony informacji niejawnych w Siłach Zbrojnych RP, które wynikają z podstawowego aktu prawnego – Ustawy o ochronie informacji niejawnych. Do niektórych z nich należą:

- pełnienie obowiązków członka Kolegium do spraw Służb Specjalnych przy Radzie Ministrów RP;
- wyrażanie zgody na udostępnianie informacji niejawnych, stanowiących tajemnicę państwową, które zostały wytworzone w resorcie obrony narodowej;
- wspólnie z ministrem, właściwym do spraw wewnętrznych, określanie w drodze rozporządzenia sposobu nadawania klauzul dokumentom niejawnym oraz zasad przyjmowania, przewożenia, wydawania i ochrony materiałów celem ich zabezpieczenia przed nieuprawnionym ujawnieniem;
- określanie w drodze wewnętrznych rozporządzeń i decyzji szczegółowych zasad ochrony informacji niejawnych w resorcie obrony narodowej.

Stosownie do innego aktu prawnego - Ustawy o urzędzie Ministra Obrony Narodowej z 14 grudnia 1995 roku odpowiada on za ogólną koordynację działań w

zakresie ochrony informacji niejawnych w dziale obrony narodowej.[91] Obowiązki, jakie nakładają na ministra obrony narodowej wymienione akty prawne sprowadzają się do nadzoru, opracowywania dokumentów normatywnych oraz koordynacji wszelkich działań, jakie są podejmowane w resorcie obrony narodowej celem ochrony informacji niejawnych..

Podstawowym „narzędziem" ministra obrony narodowej w tej dziedzinie są, bezpośrednio jemu podporządkowane[92], Wojskowe Służby Informacyjne.[93] Instytucja ta, zgodnie z postanowieniami Ustawy o ochronie informacji niejawnych pełni zasadniczą rolę w sferze bezpieczeństwa i ochrony informacji niejawnych w dziedzinie obronności, w tym w Siłach Zbrojnych RP.

Poza zadaniami, które wynikają z Ustawy o ochronie informacji niejawnych Wojskowe Służby Informacyjne wykonują ... zadania związane z rozpoznawaniem i przeciwdziałaniem zagrożeniom, godzącym w obronność Państwa oraz naruszeniom tajemnicy państwowej w zakresie obronności, jak również przygotowują dla organów państwowych informacje i analizy istotne dla obronności państwa...[94]. Obowiązki i uprawnienia funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu mają zastosowanie do żołnierzy Wojskowych Służb Informacyjnych a sfery odpowiedzialności i uprawnienia ABW i AW dotyczą WSI.[95] Do zadań tych należą w szczególności:

- rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny a w szczególności w suwerenność i międzynarodową pozycję kraju, niepodległość, nienaruszalność jego terytorium i obronność państwa;
- rozpoznawanie, zapobieganie i wykrywanie przestępstw szpiegostwa, terroryzmu, naruszenia tajemnicy państwowej, w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym, nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i

---

[91] Art. 2, pkt 6a Ustawy z dnia 14 grudnia 1995 roku o urzędzie Ministra Obrony Narodowej, Dz. U. z 1996 roku, Nr 10, poz. 56 z późniejszymi zmianami.
[92] Tamże, Art. 5, pkt 1, ust. 1.
[93] Patrz również Rozdział I/4
[94] Art. 15 Ustawy z dnia 21 listopada 1967 roku o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, Dz. U. z 1967 roku, Nr 44, poz. 220 z późniejszymi zmianami.
[95] Tamże, art. 15, ust. 2

materiałami wybuchowymi, korupcji i innych przestępstw godzących w bezpieczeństwo państwa;

- uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji, mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej oraz jej potencjału ekonomicznego i obronnego;
- rozpoznawanie i przeciwdziałanie zagrożeniom zewnętrznym godzącym w bezpieczeństwo, obronność, niepodległość i nienaruszalność terytorium Rzeczypospolitej Polskiej, rozpoznawanie międzynarodowego terroryzmu, ekstremizmu oraz przestępczości zorganizowanej;
- rozpoznawanie i analizowanie zagrożeń występujących w rejonach napięć, konfliktów i kryzysów międzynarodowych, mających wpływ na bezpieczeństwo państwa oraz podejmowanie działań mających na celu eliminowanie tych zagrożeń;
- ochrona i osłona ochrona Sił Zbrojnych, sektora obronnego gospodarki narodowej, polskich przedstawicielstw i misji wojskowych za granicą, w tym polskich kontyngentów i jednostek wojskowych;
- organizowanie działalności wojskowych przedstawicielstw dyplomatycznych w innych państwach, utrzymywanie kontaktów z członkami wojskowego korpusu dyplomatycznego, akredytowanymi w Polsce.

Od dnia 11 marca 1999 roku, z chwilą wejścia w życie Ustawy o ochronie informacji niejawnych, Wojskowe Służby Informacyjne zostały zobowiązane do wykonywania dodatkowych zadań, określonych ustawowo dla służby ochrony państwa. Do głównych z nich należą:

- prowadzenie, określonych w ustawie, postępowań sprawdzających przed wydaniem poświadczenia *(odmową wydania poświadczenia)* bezpieczeństwa osobowego;

- prowadzenie, określonego w ustawie postępowania sprawdzającego przed wydaniem *(odmową wydania)* świadectwa bezpieczeństwa przemysłowego;
- realizacja zadań w zakresie bezpieczeństwa systemów i sieci teleinformatycznych;
- certyfikacja kancelarii zagranicznych, kryptograficznych, punktów obsługi dokumentów zagranicznych i wydzielonych terminali teleinformatycznych w jednostkach organizacyjnych Ministerstwa Obrony Narodowej;
- certyfikacja systemów i sieci teleinformatycznych, przetwarzających informacje niejawne w jednostkach organizacyjnych resortu obrony narodowej i u przedsiębiorców wykonujących usługi na rzecz obronności, związane z udostępnianiem informacji niejawnych;
- certyfikacja wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych;
- ochrona informacji niejawnych wymienianych przez Rzeczpospolitą Polską i Siły Zbrojne z innymi państwami, armiami i organizacjami międzynarodowymi;
- szkolenie kandydatów na pełnomocników ochrony, administratorów systemów i sieci teleinformatycznych, inspektorów bezpieczeństwa teleinformatycznego;
- kontrola ochrony informacji niejawnych w resorcie obrony narodowej oraz kontrola przestrzegania przepisów w tym zakresie;
- prowadzenie doradztwa w sferze ochrony informacji niejawnych.[96]

Zadania te znajdują odzwierciedlenie i specyfikację w obowiązkach, jakie ustawa o ochronie informacji niejawnych i przepisy wykonawcze do niej nałożyły na szefa Wojskowych Służb Informacyjnych. Abstrahując od faktu, iż szef WSI stoi na czele służby ochrony państwa a w relacjach międzynarodowych pełni funkcję Krajowej Władzy Bezpieczeństwa, z czego wynika szereg specyficznych, właściwych tylko dla niego zadań to równocześnie pozostaje kierownikiem

[96] Źródło – opracowanie własne, na podstawie obowiązujących aktów normatywnych.

jednostki organizacyjnej i jest zobligowany do realizacji zadań typowych dla każdego dowódcy, szefa, komendanta, stojącego na czele jednostki organizacyjnej resortu obrony narodowej. Dlatego do jego najważniejszych zadań należą:

- pełnienie funkcji Krajowej Władzy Bezpieczeństwa w stosunkach międzynarodowych, w tym współpraca z Biurem Bezpieczeństwa NATO i krajowymi władzami bezpieczeństwa państw – Stron Traktatu Północnoatlantyckiego oraz zawieranie międzynarodowych umów o współpracy w sferze wzajemnej ochrony informacji niejawnych;
- organizacja, funkcjonującego na zasadach odpłatności, systemu prowadzenia postępowań sprawdzających przed wydaniem świadectwa bezpieczeństwa przemysłowego wobec przedsiębiorców, jednostek naukowych lub badawczo – rozwojowych, ubiegających się o zawarcie lub wykonujących umowy związane z dostępem do informacji niejawnych albo wykonujących na podstawie przepisów prawa zadania na rzecz obronności, związane z dostępem do informacji niejawnych stanowiących tajemnicę państwową;
- organizacja systemu prowadzenia postępowań sprawdzających, wydawania i ewidencjonowania certyfikatów bezpieczeństwa przemysłowego NATO *(ang. NATO Facility Security Clearance Certificate)* o poziomie POUFNE *(ang. CONFIDENTIAL)* i wyższym;
- organizacja systemu prowadzenia postępowań sprawdzających przed wydaniem poświadczenia bezpieczeństwa osobowego;
- organizacja systemu wydawania i ewidencjonowania certyfikatów bezpieczeństwa osobowego NATO *(ang. NATO Personnel Security Clearance Certificate)*;
- realizacja określonych w ustawie czynności związanych z postępowaniem odwoławczym i skargowym, w tym rozpatrywanie odwołań od wydanych przez pełnomocników odmów wydania poświadczenia bezpieczeństwa osobowego;
- nadzór nad prowadzonym na zasadach odpłatności szkoleniem pełnomocników u przedsiębiorców, w jednostkach naukowych lub

badawczo – rozwojowych, ubiegających się o zawarcie lub wykonujących umowy związane z dostępem do informacji niejawnych albo wykonujących na podstawie przepisów prawa zadania na rzecz obronności, związane z dostępem do informacji niejawnych stanowiących tajemnicę państwową;

- organizacja szkolenia dla pełnomocników w resorcie obrony narodowej, w tym opracowywanie programów szkolenia specjalistycznego w zakresie ochrony informacji niejawnych;
- wyrażanie zgody na udostępnianie informacji niejawnych stanowiących tajemnicę służbową, wytworzonych w jednostkach *(komórkach)* organizacyjnych WSI;
- zapewnienie bezpieczeństwa systemów i sieci teleinformatycznych w WSI, w tym opracowywanie szczególnych wymagań bezpieczeństwa, określanie organu bezpieczeństwa systemów łączności i informatyki WSI, wyznaczanie administratora systemu i inspektora bezpieczeństwa teleinformatycznego;
- nadzór nad certyfikacją i prowadzeniem kontroli kancelarii zagranicznych, punktów obsługi dokumentów zagranicznych, kancelarii i stacji łączności kryptograficznych oraz pomieszczeń wydzielonych terminali teleinformatycznych;
- organizacja systemu zatwierdzania bądź opiniowania szczególnych wymagań bezpieczeństwa systemów i sieci teleinformatycznych opracowanych przez jednostki organizacyjne resortu obrony narodowej;
- zarządzanie kontroli na zasadach określonych w Rozporządzeniu Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie szczegółowego trybu prowadzenia przez służby ochrony państwa kontroli w zakresie ochrony informacji niejawnych stanowiących tajemnicę państwową;
- organizacja systemu kontroli problemowych stanu ochrony informacji niejawnych w resorcie obrony narodowej na podstawie decyzji Nr 182/MON ministra obrony narodowej z dnia 6 października 2000 roku w

sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej;

- przedstawianie ministrowi Obrony Narodowej rocznej, zbiorczej oceny stanu ochrony informacji niejawnych w resorcie obrony narodowej;
- zarządzanie rocznych kontroli stanu ochrony informacji niejawnych w WSI;
- organizacja w WSI systemu funkcjonowania stałych i powoływanych na czas ćwiczeń kancelarii tajnych i kancelarii zagranicznej oraz systemu ochrony informacji niejawnych, w tym wyznaczanie i określanie zakresu obowiązków kierowników kancelarii oraz zatwierdzanie planów ochrony;
- udostępnianie danych z ewidencji na podstawie Rozporządzenia Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie sposobu i trybu udostępniania danych z ewidencji;
- podejmowanie decyzji związanych z ochroną informacji przewożonych, w tym za granicę, na podstawie Rozporządzenia Ministrów Spraw Wewnętrznych i Administracji i Obrony Narodowej z dnia 26 lutego 1999 roku w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów;
- organizacja współpracy uprawnionych jednostek *(komórek)* organizacyjnych WSI z Policją, Strażą Graniczną, Żandarmerią Wojskową, organami kontroli skarbowej w zakresie prowadzonych postępowań sprawdzających;
- upoważnianie żołnierzy WSI do kontroli stanu zabezpieczenia informacji niejawnych stanowiących tajemnicę państwową na zasadach i zgodnie z uprawnieniami określonymi w ustawie z dnia 23 grudnia 1994 roku o Najwyższej Izbie Kontroli;
- zatwierdzanie szczegółowych wymagań w zakresie ochrony informacji niejawnych oznaczonych klauzula ZASTRZEŻONE w podległych komórkach organizacyjnych;

- zapewnienie przeszkolenia podległej kadry i pracowników wojska w zakresie klasyfikowania informacji niejawnych.[97]

Na mocy zarządzenia szefa Wojskowych Służb Informacyjnych z 1999 roku, zasadniczy ciężar odpowiedzialności za realizację zadań służby ochrony państwa oraz wynikających z pełnienia przez szefa WSI funkcji Krajowej Władzy Bezpieczeństwa spoczywa na jednostkach terenowych Wojskowych Służb Informacyjnych[98]. Podkreślenia wymaga fakt, iż jednocześnie nie zostały ograniczone w jakikolwiek sposób dotychczas wykonywane przez jednostki terenowe Wojskowych Służb Informacyjnych zadania, ukierunkowane na ochronę obiektów wojskowych i osłonę stanów osobowych Wojska Polskiego. Postawienie nowych zadań jednostkom terenowym zbiegło się w czasie ze zmianami organizacyjnymi w Siłach Zbrojnych i koniecznością dostosowywania stanów osobowych Wojskowych Służb Informacyjnych do poziomu redukcji, jakimi objęte były całe Siły Zbrojne od 1999 roku. Przyznać jednak należy, iż realizacja zadań służby ochrony państwa i wynikających z pełnienia przez szefa WSI funkcji Krajowej Władzy Bezpieczeństwa spowodowały, że skala redukcji była w porównaniu z innymi jednostkami organizacyjnymi resortu obrony narodowej niezbyt duża. Decyzje kierownictwa resortu pozwoliły na zachowanie większości posiadanych etatów a nawet tworzenie nowych, niezbędnych dla realizacji zadań struktur.

Stosownie do rozwiązań wprowadzonych mocą Ustawy o ochronie informacji niejawnych Wojskowe Służby Informacyjne są najważniejszym komponentem systemu ochrony informacji niejawnych w sferze wojskowej, ze ściśle określonymi zadaniami i szerokimi kompetencjami. Jednakże, analogicznie jak w sferze cywilnej, do elementów składowych systemu należą również:

- kierownicy jednostek organizacyjnych;

---

[97] Źródło – opracowanie własne, na podstawie obowiązujących aktów normatywnych. Do czasu likwidacji Komitetu Ochrony Informacji Niejawnych do obowiązków szefa WSI należało również pełnienie obowiązków członka Komitetu Ochrony Informacji Niejawnych, przedstawianie Przewodniczącemu Komitetu okresowych sprawozdań z działalności WSI w sferze ochrony informacji niejawnych, występujących problemów oraz propozycji systemowych rozwiązań w dziedzinie ochrony informacji niejawnych w sferze wojskowej.

[98] Zarządzenie szefa Wojskowych Służb Informacyjnych nr 12 z dnia 9 czerwca 1999 roku. Dokument wewnętrzny, dostępny w WSI.

- pełnomocnicy ochrony;
- piony ochrony[99].

W przypadku Sił Zbrojnych ***kierownikami jednostek organizacyjnych*** są dowódcy jednostek wojskowych bowiem regulacje ustawowe dotyczą „... Sił Zbrojnych Rzeczypospolitej Polskiej i ich jednostek organizacyjnych ..."[100] Z delegacji tej wynika, iż dowódcy jednostek wojskowych mają szereg obowiązków i uprawnień oraz odpowiadają jednoosobowo za stan ochrony informacji niejawnych w podległych jednostkach wojskowych.

Do głównych zadań dowódców jednostek jako kierowników jednostek organizacyjnych w rozumieniu Ustawy o ochronie informacji niejawnych należą:

- powołanie pełnomocnika ochrony, organizacja pionu ochrony a zwłaszcza kancelarii tajnej w przypadku wytwarzania w jednostce organizacyjnej dokumentów o klauzuli od POUFNE wzwyż;
- określenie stanowisk lub rodzajów prac zleconych, z którymi może łączyć się dostęp do informacji niejawnych, odrębnie dla każdej klauzuli tajności;
- dostosowanie pomieszczeń służbowych do wymogów ustawy i normatywnych aktów wykonawczych do niej;
- pisemne zlecanie pełnomocnikowi ochrony prowadzenia zwykłych postępowań sprawdzających;
- wyrażanie zgody na udostępnianie informacji niejawnych stanowiących tajemnicę służbową, które zostały wytworzone w jednostce organizacyjnej;
- opracowanie i przekazanie Wojskowym Służbom Informacyjnym szczególnych wymagań bezpieczeństwa i procedur bezpieczeństwa dla systemów i sieci teleinformatycznych, służących do wytwarzania, przechowywania, przetwarzania lub przekazywania informacji niejawnych;

---

[99] Schemat systemu ochrony informacji niejawnych w Siłach Zbrojnych znajduje się w Załączniku nr 2.
[100] Art. 1 Ustawy o ochronie informacji niejawnych.

- każdorazowe wyrażanie zgody na przechowywanie dokumentów zawierających informacje niejawne poza kancelarią, pod warunkiem spełnienia wymogów bezpieczeństwa odpowiednich do ich klauzuli tajności, na czas niezbędny do realizacji zadań związanych z dostępem do tych informacji;
- zatwierdzanie opracowanych przez pełnomocnika ochrony szczegółowych wymagań w zakresie ochrony informacji niejawnych oznaczonych klauzulą ZASTRZEŻONE w podległej komórce organizacyjnej.[101]

Dowódcom jednostek podlegają bezpośrednio etatowi ***pełnomocnicy ochrony***, którzy realizując ustawowe delegacje i zakres zadań wynikających z wewnętrznych aktów normatywnych resortu obrony narodowej, bezpośrednio organizują system ochrony informacji niejawnych w jednostkach wojskowych. W jednostce organizacyjnej poniżej szczebla samodzielnego pułku (równorzędnego) dopuszczalne jest połączenie tego stanowiska z innym już istniejącym w etacie jednostki. Jednakże obowiązków pełnomocnika nie może wykonywać kierownik kancelarii tajnej i osoba będąca jej pracownikiem. Do zadań, jakie realizują pełnomocnicy ochrony należą:

- kierowanie wyspecjalizowaną komórką organizacyjną do spraw ochrony informacji niejawnych – pionem ochrony;
- prowadzenie, na pisemne polecenie kierownika jednostki organizacyjnej, zwykłego postępowania sprawdzającego przed wydaniem, odmową wydania, poświadczenia bezpieczeństwa upoważniającego osobę sprawdzaną do dostępu do informacji niejawnych stanowiących tajemnicę służbową;
- prowadzenie wykazu stanowisk i prac zleconych oraz osób dopuszczonych do pracy i służby na stanowiskach, z którymi wiąże się dostęp do informacji niejawnych;
- przekazywanie właściwym jednostkom i komórkom organizacyjnym Wojskowych Służb Informacyjnych danych, wymaganych do ewidencji

[101] Źródło – opracowanie własne na podstawie Ustawy o ochronie informacji niejawnych.

osób dopuszczonych do pracy lub służby na stanowiskach, z którymi wiąże się dostęp do informacji niejawnych stanowiących tajemnicę służbową, oznaczonych klauzulą POUFNE, a także do ewidencji osób, którym odmówiono wydania poświadczenia bezpieczeństwa;

- prowadzenie podstawowego i uzupełniającego szkolenia w zakresie ochrony informacji niejawnych dla osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej;
- opracowanie i aktualizacja planu ochrony jednostki organizacyjnej;
- bieżący nadzór nad stosowaniem środków ochrony fizycznej w jednostce organizacyjnej;
- żądanie od komórek organizacyjnych w swojej jednostce organizacyjnej udzielenia natychmiastowej pomocy w wypadku wprowadzenia stanu nadzwyczajnego;
- współpraca z właściwymi terytorialnie jednostkami i komórkami organizacyjnymi Wojskowych Służb Informacyjnych i bieżące informowanie kierownika jednostki organizacyjnej o przebiegu tej współpracy;
- opracowanie planu postępowania z materiałami zawierającymi informacje niejawne stanowiące tajemnicę państwową w razie wprowadzenia stanu nadzwyczajnego;
- wykonywanie czynności sprawdzających w ramach prowadzonych w jednostce organizacyjnej kontroli stanu ochrony informacji niejawnych;
- wyjaśnianie okoliczności naruszania przepisów o ochronie informacji niejawnych, zawiadamianie o tym kierownika jednostki organizacyjnej, a w przypadku naruszenia przepisów o ochronie informacji niejawnych, oznaczonych klauzulą POUFNE lub wyższą, również Wojskowych Służb Informacyjnych.[102]

Trzecim elementem systemu są kierowane przez pełnomocników ***piony ochrony*** w jednostkach wojskowych. Z uwagi na ilość i różnorodność zadań realizowanych przez pełnomocników i piony ochrony w różnych strukturach

[102] Źródło – opracowanie własne na podstawie Ustawy o ochronie informacji niejawnych.

organizacyjnych Wojska Polskiego – w rozumieniu ustawy jednostką organizacyjną może bowiem być jednostka wojskowa licząca kilkudziesięciu żołnierzy jak i dowództwo rodzaju Sił Zbrojnych liczące kilkaset osób – ich liczebność i struktura są zróżnicowane. Organizacyjnie system wygląda następująco:

- na szczeblu ministerstwa obrony narodowej funkcjonuje Biuro Pełnomocnika Ochrony Informacji Niejawnych[103];
- na szczeblu rodzaju Sił Zbrojnych, okręgu wojskowego, dywizji, brygady, samodzielnego pułku, akademii, szkoły oficerskiej, bazy materiałowo – technicznej, centrum szkolenia funkcjonują pełnomocnicy ochrony oraz podległe im piony. W zależności od potrzeb pełnomocnicy kierują oddziałami *(na przykład Dowództwo rodzaju Sił Zbrojnych)*[104], wydziałami *(na przykład dywizja)* bądź pionami ochrony, budowanymi według potrzeb danej jednostki organizacyjnej *(brygada, pułk, inne równorzędne struktury)*. Takie wydziały i piony ochrony mogą liczyć do 10 osób.

Głównym, określonym w ustawie zadaniem pionów ochrony jest zapewnienie właściwej ochrony informacji niejawnych w jednostce organizacyjnej. Zadania pionów ochrony są tożsame z określonymi powyżej sferami odpowiedzialności pełnomocnika ds. ochrony informacji niejawnych bowiem są one narzędziem w ręku kierownika jednostki organizacyjnej, kierowanym przez pełnomocnika. Jednocześnie należy pamiętać, iż skala tych zadań jest różna w różnych jednostkach organizacyjnych resortu obrony narodowej.

Proces powoływania pełnomocników ochrony i budowy pionów ochrony w jednostkach organizacyjnych resortu obrony narodowej nie przebiegał bez komplikacji i opóźnień wobec ustawowo określonych terminów. Ustawodawca bowiem określił, iż „...Kierownicy jednostek organizacyjnych, w terminie 3 miesięcy od dnia wejścia w życie ustawy, powołają pełnomocników ochrony i

---

[103] Struktura Biura Pełnomocnika ministra obrony narodowej, ustanowiona na mocy Decyzji Nr 30/MON znajduje się w Załączniku nr 3. W zależności od realizowanych zadań struktura ta może i powinna być modyfikowana.

[104] Struktura oddziału ochrony informacji niejawnych Dowództwa Okręgu Wojskowego, ustanowiona na mocy Decyzji Nr 30/MON znajduje się w Załączniku nr 4. Może być modyfikowana i dostosowywana do zadań w sferze ochrony informacji niejawnych.

zorganizują piony ochrony w podległych jednostkach ..."[105]. Ustawa weszła w życie 11 marca 1999 roku a więc ustawodawca oczekiwał, iż w połowie roku w każdej jednostce organizacyjnej zacznie funkcjonować pełnomocnik ochrony. W warunkach Sił Zbrojnych było to zadanie praktycznie niewykonalne, ponieważ wiązało się z koniecznością utworzenia nowych etatów a jak powszechnie wiadomo proces taki do łatwych nie należy. Zbiegło się to również w czasie ze zmianami organizacyjnymi w Siłach Zbrojnych, etatyzacją[106] i wprowadzaniem kolejnych redukcji w stanie ilościowym polskiej armii. Uwzględniając te obiektywne przesłanki łatwo zrozumieć, dlaczego w większości jednostek wojskowych etaty pełnomocników utworzono w 2001 roku, uwzględniając je w powstałych po etatyzacji strukturach Wojska Polskiego. W okresie przejściowym, do czasu powołania etatowych pełnomocników dowódcy jednostek wojskowych zlecali realizację zadań pełnomocników innym żołnierzom zawodowym na zasadzie dodatkowych, powierzonych zadań służbowych.

Cechą charakterystyczną systemu jest fakt, iż WSI jako służba ochrony państwa pozostaje jednostką organizacyjną Sił Zbrojnych, zobowiązaną do powołania pełnomocników ochrony i organizacji pionów ochrony. Dlatego w samych Wojskowych Służbach Informacyjnych jak i w każdej jej wewnętrznej strukturze, stanowiącej w rozumieniu ustawy jednostkę organizacyjną, funkcjonują pełnomocnicy i piony ochrony realizujące przypisane im zadania. Podlegają one takim samym rygorom kontroli ze strony wyspecjalizowanych komórek WSI jako służby ochrony państwa jak każdy pion ochrony w Siłach Zbrojnych Rzeczypospolitej Polskiej.

Wyszczególnione powyżej elementy systemu ochrony informacji niejawnych *(WSI, kierownicy jednostek organizacyjnych i pełnomocnicy ochrony),* pomimo ustawowo określonej niezależności organizacyjnej i funkcjonalnej są ze sobą powiązane. Wynika to z następujących uwarunkowań:

- działają w ściśle określonym i specyficznym środowisku jakim są Siły Zbrojne Rzeczypospolitej Polskiej;

---

[105] Art. 85 Ustawy o ochronie informacji niejawnych.
[106] Etatyzacja to proces tworzenia przejrzystych struktur Sił Zbrojnych polegająca na dostosowywaniu stopni wojskowych do stanowisk etatowych.

- realizują szereg tych samych zadań w sferze ochrony informacji niejawnych;
- są zobowiązane do ścisłej współpracy i wymiany informacji.

Tak zbudowany system i zależności występujące pomiędzy jego komponentami są gwarantem skutecznej ochrony informacji niejawnych i zapewnienia jednolitych standardów bezpieczeństwa w różnych komórkach organizacyjnych Sił Zbrojnych. Czy jest to system działający skutecznie i czy spełnia postawione przez ustawodawcę wymagania?. Cztery lata doświadczeń pozwalają postawić tezę, iż system działa sprawnie i skutecznie. Prawdą jest, iż jego organizacja zajęła więcej czasu niż było to pierwotnie określone w Ustawie o ochronie informacji niejawnych, prawdą jest, że jego obecny kształt nie jest jeszcze ostateczny i podlega ciągłym modyfikacjom. Wynika to z faktu, iż w chwili stanowienia ustawy bardzo trudno było określić, jaka będzie skala zadań w dziedzinie ochrony informacji niejawnych. Nikt nie przewidział, iż ilość niezbędnych do przeprowadzenia postępowań sprawdzających będzie tak duża. Teraz jest to oczywiste i za aksjomat przyjmujemy, iż Siły Zbrojne RP są strukturą państwa, gdzie zgromadzonych jest najwięcej informacji niejawnych o najwyższych klauzulach tajności. Nie przewidziano również, że polscy żołnierze będą w krótkim czasie służyć w tak wielu strukturach Paktu Północnoatlantyckiego, co będzie wymagało prowadzenia wobec nich postępowań sprawdzających, szkoleń, wydawania certyfikatów bezpieczeństwa NATO. Jednocześnie w 1999 roku temu trudno było ocenić, jaka będzie skala zmian organizacyjnych w polskiej armii i ile wysiłku kosztować będzie dostosowywanie struktur WSI i pionów ochrony do likwidowanych czy nowo formowanych jednostek wojskowych. Uwzględniając doświadczenia przeszłości, z całą pewnością możemy dziś powiedzieć, iż system ochrony informacji niejawnych w Siłach Zbrojnych jest efektywny i dobrze zorganizowany. Jednakże oczywistym jest, że będzie podlegał dalszym zmianom i modyfikacjom tak w sferze normatywnej jak i organizacyjnej.

2. Zasady ochrony fizycznej informacji niejawnych.

Jednostki organizacyjne resortu obrony narodowej, w których są wytwarzane, przetwarzane, przekazywane lub przechowywane informacje niejawne mają ustawowy obowiązek ich fizycznej ochrony. Celem stosowania środków ochrony fizycznej jest uniemożliwienie osobom nieupoważnionym dostępu do takich informacji oraz ich ochrona przed:

- działaniem obcych służb specjalnych;
- zamachem terrorystycznym lub sabotażem;
- kradzieżą lub zniszczeniem materiału;
- próbą wejścia osób nieuprawnionych;
- nieuprawnionym dostępem pracowników do materiałów oznaczonych wyższą klauzulą tajności.[107]

Zrozumiałym jest, że środki ochrony fizycznej muszą być dostosowane do klauzuli tajności i ilości informacji niejawnych znajdujących się w konkretnej jednostce organizacyjnej czy liczby osób posiadających dostęp do informacji niejawnych. Zastosowane środki ochrony muszą też uwzględniać realne zagrożenia występujące na danym terenie. Według ocen Wojskowych Służb Informacyjnych najbardziej narażone na penetrację obcych służb specjalnych są obiekty wojskowe rozlokowane w pobliżu wschodnich granic Polski. Równie duże zagrożenie notowane jest w pobliżu jednostek wielonarodowych takich jak Korpus Wielonarodowy Północ – Wschód w Szczecinie *(ang. Multinational Corps North – East)*. Dane tego typu przekazywane kierownikom jednostek organizacyjnych przez właściwe terytorialnie jednostki organizacyjne Wojskowych Służb Informacyjnych muszą być uwzględniane w organizacji systemu ochrony fizycznej.

System fizycznej ochrony informacji niejawnych, według ustawowych zaleceń obejmuje:

- wydzielenie stref bezpieczeństwa – części obiektów, które poddane być muszą szczególnej kontroli wejść i wyjść oraz kontroli przebywania w nich osób uprawnionych;[108]

---

[107] Art. 56 Ustawy o ochronie informacji niejawnych.

- wydzielenie stref administracyjnych wokół stref bezpieczeństwa, służących do kontroli osób i pojazdów;
- wprowadzenie systemu przepustek lub wariantowo innego systemu, który określa uprawnienia do wejścia, przebywania i wyjścia ze strefy bezpieczeństwa ;
- wprowadzenie systemu przechowywania kluczy do pomieszczeń chronionych, szaf pancernych i innych pojemników służących do przechowywania informacji niejawnych stanowiących tajemnicę państwową;
- zapewnienie kontroli stref bezpieczeństwa i stref administracyjnych przez przygotowanych i przeszkolonych pracowników pionu ochrony;
- stosowanie certyfikowanych lub posiadających świadectwa kwalifikacyjne urządzeń służących do ochrony informacji niejawnych.

Inną formą zapewnienia ochrony fizycznej informacjom niejawnych jest wydzielenie specjalnych stref bezpieczeństwa, które służą najczęściej do prowadzenia rozmów i odbywania spotkań, w czasie których omawiane są sprawy stanowiące tajemnicę państwową. Pomieszczenia te muszą być sprawdzone przed podsłuchem i podglądem.[109]

Za ochronę fizyczną informacji niejawnych odpowiada pełnomocnik ochrony, na bieżąco nadzorujący środki ochrony fizycznej w jednostce organizacyjnej. Jest on zobowiązany do opracowania planu ochrony i

---

[108] Rozróżniamy I i II strefę bezpieczeństwa. Do pierwszej zaliczany jest obszar chroniony w taki sposób, że wejście do niego oznacza bezpośredni dostęp do informacji niejawnych, osoby upoważnione do dostępu do informacji niejawnych, co najmniej o klauzuli informacji przechowywanych w strefie, nie będące żołnierzami albo pracownikami jednostki lub komórki organizacyjnej *(interesanci)* mogą w niej przebywać jedynie po uzyskaniu zgody kierownika jednostki *(komórki)* organizacyjnej i pod nadzorem żołnierza lub pracownika pionu ochrony. Druga strefa bezpieczeństwa to obszar, obiekt, fragment budynku, jedno lub kilka pomieszczeń, chroniony w taki sposób, że wejście do tej strefy nie oznacza bezpośredniego dostępu do informacji niejawnych, osoby upoważnione do dostępu do informacji niejawnych, co najmniej o klauzuli informacji przechowywanych w strefie, nie będące żołnierzami albo pracownikami jednostki lub komórki organizacyjnej *(interesanci)* mogą w niej przebywać bez nadzoru, za zgodą kierownika jednostki organizacyjnej.

[109] Pomiary, mające na celu sprawdzenie, czy w pomieszczeniach nie ma urządzeń podsłuchowych lub służących do podglądu dokonywane są przy użyciu specjalistycznego sprzętu przez wyspecjalizowane jednostki techniczne Wojskowych Służb Informacyjnych.

przedstawienia tego dokumentu kierownikowi jednostki organizacyjnej do zatwierdzenia.[110]

Plan ochrony składa się z dwóch części – graficznej i opisowej. W części graficznej ujmuje się rozmieszczenie:

- budynków mieszkalnych, magazynów, garaży i innych urządzeń znajdujących się w ochranianym obiekcie;
- technicznych środków wspomagających ochronę obiektów – bram, wież wartowniczych, umocnień inżynieryjnych, urządzeń alarmowych, środków łączności;
- posterunków wartowniczych, patroli i tras ich patrolowania;
- służb dyżurnych ochraniających jednostkę organizacyjną;
- stref bezpieczeństwa oraz rejonów szczególnej ochrony;
- sił i środków wydzielanych do ochrony jednostki organizacyjnej.

W części opisowej zawartych jest szereg szczegółowych, wynikających ze specyfiki, struktury i wielkości jednostki organizacyjnej danych. Do najważniejszych z nich należą:

- analiza zewnętrznych zagrożeń dla jednostki organizacyjnej, w tym wywiadowczych, terrorystycznych, dywersyjnych, sabotażowych i kryminalnych;
- analiza wewnętrznych zagrożeń związanych z przechowywaniem informacji i zabezpieczeniem broni, amunicji, materiałów wybuchowych;
- ocena aktualnego stanu ochrony komórki organizacyjnej i organizacja systemu ochrony w godzinach służbowych, w nocy oraz w dniach wolnych od zajęć służbowych;
- skład służb dyżurnych i sił ochronnych oraz zasady i organizacja ochrony obiektu;

[110] Metodyka opracowywania planu ochrony zawarta jest w Decyzji Nr 31/MON Ministra Obrony Narodowej z dnia 8 marca 2000 roku w sprawie zasad opracowywania planów ochrony jednostek organizacyjnych resortu obrony narodowej.

- rodzaj i ilość uzbrojenia sił ochronnych, posterunków, sposób zabezpieczenia broni i amunicji;
- dane o zabezpieczeniach technicznych wykorzystywanych w systemie ochrony;
- określenie stref bezpieczeństwa i stref administracyjnych oraz systemu kontroli dostępu do tych stref i poszczególnych obiektów, sposobu przechowywania kluczy do pomieszczeń podlegających szczególnej ochronie, takich jak np. magazyny broni;
- zasady postępowania i wzmocnienie służb dyżurnych i sił ochronnych w sytuacjach kryzysowych, takich jak napad bądź penetracja obiektu;
- zakres współdziałania służb dyżurnych i sił ochronnych z Policją, Żandarmerią Wojskową, innymi jednostkami resortu obrony narodowej oraz innymi cywilnymi służbami.

Plan ochrony jest dokumentem niejawnym o klauzuli odpowiadającej charakterowi i przeznaczeniu jednostki organizacyjnej i przechowywany jest w pomieszczeniu oficera dyżurnego jednostki. W innych pomieszczeniach jak na przykład w wartowni przechowuje się wyciągi z planów ochrony.

Najważniejszym obiektem jednostki organizacyjnej, w którym przechowywane są dokumenty niejawne, podlegającym szczególnej ochronie i wymagającym stosowania rygorystycznych przepisów i jak najlepszych środków ochrony fizycznej jest kancelaria tajna. Obowiązek jej zorganizowania spoczywa na kierowniku jednostki organizacyjnej, jeśli w podległej mu strukturze są wytwarzane, przetwarzane, przekazywane lub przechowywane dokumenty oznaczone klauzulą POUFNE i wyższą. Stosownie do zapisów ustawy kancelaria tajna stanowi wyodrębnioną komórkę organizacyjną podległą bezpośrednio pełnomocnikowi ochrony, odpowiedzialną za właściwe rejestrowanie, przechowywanie, obieg i wydawanie takich dokumentów uprawnionym osobom. Kancelaria tajna powinna być zorganizowana w wyodrębnionym pomieszczeniu,

zabezpieczonym zgodnie z przepisami o środkach ochrony fizycznej informacji niejawnych i być obsługiwana przez pracowników pionu ochrony.[111]

Kancelaria powinna spełniać szereg warunków bezpieczeństwa, do najważniejszych z nich należą:

- musi być zlokalizowana w budynku murowanym, z wyłączeniem poddaszy, z wejściem co najmniej ze strefy administracyjnej i posiadać wymagane przepisami grubości ścian wewnętrznych, zewnętrznych i stropów;
- okna powinny uniemożliwiać wgląd z zewnątrz i otwarcie przez osoby nieupoważnione oraz w zależności od wysokości nad poziomem terenu być zabezpieczone kratą, siatką stalową lub folią antywłamaniową;
- otwory wentylacyjne powinny być zabezpieczone siatką stalową i wyposażone w otwory rewizyjne umożliwiające kontrolę przewodów wentylacyjnych;
- drzwi wejściowe, stalowe lub drewniane obite blachą stalową, muszą być zabezpieczone przed włamaniem i wyposażone w dwa zamki, w tym jeden szyfrowy;
- powinna być wyposażona w przeciwpożarowy system alarmowy, system sygnalizujący próby siłowego otwarcia drzwi wewnętrznych i wejściowych i ruch w pomieszczeniach, system sygnalizacji napadu oraz ewentualnie w system monitorowania przy pomocy kamer drzwi i okien od zewnątrz;
- musi posiadać urządzenia do przechowywania dokumentów niejawnych, stalowe sejfy wyposażone w dwa zamki do przechowywania informacji ŚCIŚLE TAJNYCH, TAJNYCH i POUFNYCH o konstrukcji tym bardziej skomplikowanej im wyższa jest klauzula tajności przechowywanych dokumentów, szafy drewniane lub metalowe do

[111] Art. 50 ust. 2 ustawy o ochronie informacji niejawnych. Szczegółowe przepisy dotyczące organizacji kancelarii tajnych zawarte są w Rozporządzeniu Rady Ministrów z dnia 9 lutego 1999 roku w sprawie organizacji kancelarii tajnych oraz w Zarządzeniu Nr 49/MON ministra obrony narodowej z dnia 7 sierpnia 2002 roku w sprawie szczególnych zasad organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych.

przechowywania dokumentów o klauzuli ZASTRZEŻONE, urządzenia do niszczenia dokumentów.

Do najważniejszych zasad funkcjonowania kancelarii i ochrony przechowywanych w nich dokumentów niejawnych należą:

- kancelaria powinna być zorganizowana odrębnie dla dokumentów o różnych klauzulach tajności;[112]
- dopuszczalne jest tworzenie filii kancelarii w jednostce organizacyjnej;
- organizacja pracy kancelarii musi zawsze zapewniać możliwość ustalenia, gdzie w danej chwili, w jednostce organizacyjnej, znajduje się dokument niejawny, zarejestrowany w kancelarii;
- z dokumentami o klauzulach TAJNE i ŚCIŚLE TAJNE można zapoznawać się jedynie w kancelarii, mogą być wydawane poza kancelarię tylko tym upoważnionym wykonawcom, którzy mają warunki ochrony informacji stanowiących tajemnicę państwową przed nieuprawnionym ujawnieniem;
- dokumenty niejawne mogą być udostępniane jedynie osobom posiadającym odpowiednie do klauzuli udostępnianego dokumentu poświadczenie bezpieczeństwa;
- każdorazowe zapoznanie się, przez osobę uprawnioną z dokumentem stanowiącym tajemnicę państwową, podlega odnotowaniu w karcie zapoznania się z tym dokumentem

Kancelarią tajną kieruje kierownik *(żołnierz zawodowy lub pracownik cywilny wojska)*, wyznaczony przez kierownika jednostki organizacyjnej na wniosek pełnomocnika ochrony. Warunkami wyznaczenia na to stanowisko są posiadanie poświadczenia bezpieczeństwa odpowiedniego dla najwyższej klauzuli przechowywanych w kancelarii dokumentów oraz odbycie specjalistycznego przeszkolenia w zakresie ochrony informacji niejawnych.

---

[112] Możliwe jest zorganizowanie jednej kancelarii, chroniącej dokumenty o różnych klauzulach pod warunkiem, że dokumenty oznaczone różnymi klauzulami tajności są od siebie fizycznie oddzielone i obsługiwane przez osoby, które posiadają poświadczenia bezpieczeństwa upoważniające do dostępu do informacji niejawnych o najwyższej klauzuli przechowywanych dokumentów. Z przyczyn praktycznych i ekonomicznych rozwiązanie to jest powszechnie stosowane w resorcie obrony narodowej.

Do najważniejszych zadań kierownika kancelarii tajnej, ustalanych każdorazowo przez pełnomocnika ochrony należą[113]:

- oznaczanie i rejestrowanie dokumentów według zasad określonych w resorcie obrony narodowej, udostępnianie dokumentów niejawnych osobom uprawnionym oraz nadzór nad ich wewnętrznym i zewnętrznym obiegiem w jednostce organizacyjnej;
- prowadzenie wykazów osób upoważnionych do dostępu do krajowych informacji niejawnych, które posiadają odpowiednie poświadczenia bezpieczeństwa oraz wykazu osób upoważnionych do dostępu do informacji pochodzących z NATO bądź innych organizacji międzynarodowych i posiadających stosowny certyfikat bezpieczeństwa;[114]
- prowadzenie bieżącej kontroli sposobu wytwarzania oraz postępowania z dokumentami niejawnymi w jednostce organizacyjnej;
- prowadzenie, na podstawie danych otrzymywanych z Głównej Kancelarii Zagranicznej, wykazu kancelarii zagranicznych i punktów obsługi dokumentów zagranicznych w resorcie obrony narodowej, współpraca z tą kancelarią w zakresie przekazywania wykazów osób posiadających certyfikaty bezpieczeństwa i wykazów dokumentów uzyskanych z wymiany międzynarodowej.

Istotnym elementem ochrony informacji niejawnych w kancelarii tajnej są zasady ich rejestrowania i niszczenia. W celu rejestracji dokumentów i kontroli ich obiegu w jednostce organizacyjnej, w kancelarii prowadzi się tak zwane trwałe urządzenia ewidencyjne *(na przykład „Rejestr teczek dokumentów niejawnych, dzienników i książek ewidencyjnych")* oraz pomocnicze urządzenia ewidencyjne *(jest ich kilkanaście, należy do nich na przykład „Wykaz osób upoważnionych do dostępu do informacji niejawnych").*[115]

---

[113] Źródło – opracowanie własne na podstawie obowiązujących aktów normatywnych.
[114] Zasady wydawania certyfikatów bezpieczeństwa omówione są w Rozdziale II.3.
[115] Wzory urządzeń ewidencyjnych prowadzonych w kancelariach tajnych w resorcie obrony narodowej oraz szczegółowe zasady ewidencjonowania, przekazywania dokumentów niejawnych uprawnionym osobom a także zasady niszczenia dokumentów określone są w Zarządzeniu Nr 49/MON Ministra Obrony Narodowej z dnia 7 sierpnia 2002 roku.

Ze względu na specyfikę zadań wykonywanych przez jednostki wojskowe kancelarie tajne organizowane są nie tylko w miejscach ich stałej dyslokacji. Na czas ćwiczeń, w czasie realizacji zadań przez jednostkę wojskową w misjach pokojowych ONZ lub NATO oraz na okres wojny muszą być również zorganizowane i zapewniać skuteczną ochronę informacji niejawnych. Kancelaria ćwiczebna powoływana na okres ćwiczeń i szkolenia poligonowego funkcjonuje na takich samych zasadach jak stała kancelaria. Jej kierownikiem może być odpowiednio przygotowany żołnierz rezerwy, dowódca jednostki musi zapewnić wymagany poziom ochrony kancelarii zwłaszcza wówczas, gdy jest organizowana poza rejonem stałej dyslokacji jednostki wojskowej. Kancelaria na czas wojny przygotowywana jest w czasie pokoju, na podstawie wytycznych kierownika jednostki organizacyjnej, w czasie osiągania przez jednostkę wojskową wyższych stanów gotowości bojowej. Jej funkcjonowanie w okresie działań bojowych musi przewidywać zabezpieczenie dokumentów przed ich przejęciem przez przeciwnika. W takim przypadku na polecenie kierownika jednostki wojskowej kierownik kancelarii przy pomocy środków szybko niszczących musi zniszczyć dokumenty niejawne zaczynając od dokumentów operacyjnych, szyfrowych i mobilizacyjnych.

Niektóre z kancelarii tajnych resortu obrony narodowej mogą pełnić funkcję kancelarii zagranicznych a więc upoważnionych do otrzymywania, przetwarzania, przechowywania i przesyłania dokumentów pochodzących z wymiany zagranicznej *(z innych państw bądź organizacji międzynarodowych)*. Warunkiem utworzenia kancelarii zagranicznej jest otrzymanie certyfikatu Wojskowych Służb Informacyjnych.[116] Certyfikat jest wydawany po dokonaniu oceny pomieszczeń kancelarii pod względem bezpieczeństwa fizycznego przez Komisję Wojskowych Służb Informacyjnych.[117] Jeden egzemplarz certyfikatu, dla celów ewidencyjnych znajduje się w Wojskowych Służbach Informacyjnych, drugi w Głównej Kancelarii

[116] Zasady certyfikacji kancelarii zagranicznych zawarte są w Decyzji Nr 29/MON Ministra Obrony Narodowej z dnia 22 lutego 2001 roku w sprawie trybu certyfikacji i kontroli kancelarii zagranicznych, kancelarii środków i materiałów kryptograficznych, punktów obsługi dokumentów zagranicznych, stacji łączności kryptograficznej oraz pomieszczeń wydzielonych *(terminali)* teleinformatycznych w jednostkach organizacyjnych resortu obrony narodowej.

[117] Wzór certyfikatu znajduje się w Załączniku Nr 5.

Zagranicznej Ministerstwa Obrony Narodowej[118] a trzeci w certyfikowanej kancelarii zagranicznej.

3. Procedury sprawdzające przed wydaniem poświadczenia bezpieczeństwa osobowego.

Ustawa o ochronie informacji niejawnych stanowi, iż każdy kierownik jednostki organizacyjnej a więc każdy dowódca – kierownik jednostki organizacyjnej w sferze wojskowej - jest zobowiązany do określenia stanowisk lub rodzajów prac zleconych, z którymi może łączyć się dostęp do informacji niejawnych, odrębnie dla każdej klauzuli tajności[119]. Warunkiem zatrudnienia, dopuszczenia do pracy lub pełnienia służby na tego typu stanowiskach lub zlecenia pracy, z którą łączy się udostępnienie informacji niejawnych jest przeprowadzenie stosownego postępowania sprawdzającego i przeszkolenie w zakresie ochrony informacji niejawnych. Jednakże nie mogą być dopuszczone do pracy lub pełnienia służby albo do wykonywania prac zleconych, z którymi łączy się dostęp do informacji niejawnych stanowiących tajemnicę państwową osoby:

- nie posiadające obywatelstwa polskiego, z zastrzeżeniem art. 67 ust. 4 *(osoby objęte postępowaniem przed wydaniem przedsiębiorcy świadectwa bezpieczeństwa przemysłowego, z wyjątkiem pełnomocnika ochrony);*
- skazane prawomocnym wyrokiem za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą;
- które nie posiadają poświadczenia bezpieczeństwa, z wyjątkiem osób, o których mowa w art. 27 ust. 2, 3, 6 i 8 *(osoby sprawujące najwyższe*

---

[118] Obecnie, w resorcie obrony narodowej Główną Kancelarią Zagraniczną, uprawnioną do otrzymywania dokumentów o klauzuli COSMIC TOP SECRET jest kancelaria zagraniczna Wojskowych Służb Informacyjnych, Główną Kancelarią Zagraniczną uprawnioną do otrzymywania dokumentów o klauzuli NATO SECRET jest kancelaria zagraniczna znajdująca się w pionie Sekretarza Stanu – I-go zastępcy Ministra Obrony Narodowej.

[119] Rodzaje stanowisk w administracji rządowej, z którymi może łączyć się dostęp do informacji niejawnych stanowiących tajemnicę państwową i prac zleconych z wykonywaniem, których może łączyć się dostęp do takich informacji określone są w Rozporządzeniu Rady Ministrów z dnia 9 lutego 1999r. w sprawie stanowisk i rodzajów prac zleconych w organach administracji rządowej, których wykonywanie może łączyć

funkcje państwowe, posłowie, senatorowie, osoby zwolnione od obowiązku przeprowadzenia postępowania przez Prezydenta bądź Premiera RP w stanie nadzwyczajnym).[120]

W zależności od stanowiska lub zleconej pracy przeprowadza się postępowania:

- zwykłe – przy stanowiskach i pracach związanych z dostępem do informacji stanowiących tajemnicę służbową, oznaczonych klauzulami ZASTRZEŻONE i POUFNE. Postępowanie takie prowadzi pełnomocnik ochrony w jednostce organizacyjnej[121]. Podstawą wszczęcia postępowania jest pisemne polecenie kierownika jednostki organizacyjnej albo wniosek przedsiębiorcy, jednostki naukowej, lub badawczo – rozwojowej, skierowany do kierownika jednostki organizacyjnej.[122] Powinno się ono zakończyć w ciągu miesiąca od daty otrzymania pisemnego polecenia przeprowadzenia postępowania bądź daty otrzymania wniosku o przeprowadzenie postępowania;
- poszerzone – przy stanowiskach i pracach związanych z dostępem do informacji niejawnych oznaczonych klauzulą TAJNE. Postępowanie takie mogą prowadzić wyłącznie Wojskowe Służby Informacyjne. Powinno się ono zakończyć w ciągu dwóch miesięcy od daty złożenia wniosku o przeprowadzenie postępowania wraz z załączoną ankietą;
- specjalne – przy stanowiskach i pracach związanych z dostępem do informacji oznaczonych klauzulą ŚCIŚLE TAJNE. Postępowanie takie mogą prowadzić wyłącznie Wojskowe Służby Informacyjne[123]. Powinno

---

się z dostępem do informacji niejawnych stanowiących tajemnice państwową. Stosownie do tego rozporządzenia minister obrony narodowej zajmuje tego typu stanowisko w resorcie obrony narodowej.

[120] Art. 28 Ustawy o ochronie informacji niejawnych.

[121] Dopuszczalne jest prowadzenie postępowania zwykłego przez Wojskowe Służby Informacyjne wobec pełnomocnika ochrony, gdy nie ma potrzeby upoważniania go do informacji TAJNYCH, zwłaszcza przy realizacji kontraktów niejawnych NATO o klauzuli POUFNE.

[122] Pełnomocnik ochrony jednostki organizacyjnej, która zawiera umowę lub zleca zadanie, z wykonaniem których łączy się dostęp do informacji niejawnych stanowiących tajemnicę służbową może prowadzić zwykłe postępowanie sprawdzające na wniosek przedsiębiorcy, jednostki naukowej lub badawczo – rozwojowej realizujących daną umowę, zadanie. W takim wypadku może prowadzić postępowanie wobec osób zaangażowanych w realizację umowy, zadania z wyjątkiem pełnomocnika ochrony.

[123] Wyjątkiem jest system prowadzenia postępowań sprawdzających w Żandarmerii Wojskowej, która może prowadzić poszerzone i specjalne postępowania wobec osób ubiegających się o przyjęcie do służby lub pracy w jej organach;

się ono zakończyć w ciągu trzech miesięcy od daty złożenia wniosku o przeprowadzenie postępowania wraz z wypełnioną ankietą.

Przeprowadzenie każdego postępowania wymaga pisemnej zgody osoby sprawdzanej, która wypełnia szczegółową ankietę bezpieczeństwa, zawierającą szereg danych o sobie, najbliższej rodzinie i osobach trzecich[124]. W związku z tym, że w ankiecie zawarte są tego typu dane, dokument ten po wypełnieniu oznaczany jest klauzulę POUFNE.

Każde postępowanie sprawdzające ma na celu ustalenie czy osoba sprawdzana daje rękojmię zachowania tajemnicy a więc czy spełnia ustawowe wymogi i będzie gwarantować, że powierzane jej informacje będą należycie chronione przed nieuprawnionym ujawnieniem. Dlatego Ustawa o ochronie informacji niejawnych stanowi, iż w toku każdego typu postępowania ustala się czy w stosunku do osoby sprawdzanej istnieją wątpliwości dotyczące:

- uczestnictwa, współpracy lub popierania działalności szpiegowskiej, terrorystycznej, sabotażowej lub innej wymierzonej przeciwko interesom Rzeczypospolitej Polskiej;
- ukrywania lub podawania niezgodnego z prawdą informacji, które mają znaczenie dla ochrony informacji niejawnych;

  występowania okoliczności powodujących ryzyko podatności na szantaż lub wywieranie presji;
- przestrzegania konstytucyjnego porządku Rzeczypospolitej Polskiej a zwłaszcza współpracy bądź przynależności do partii politycznych lub organizacji, wymienionych w art. 13 Konstytucji RP[125];
- zagrożenia ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania kontaktu a zwłaszcza wywierania w tym celu presji;
- właściwego postępowania z informacjami niejawnymi.

---

[124] Wzór ankiety bezpieczeństwa osobowego, wprowadzony na mocy Ustawy o ochronie informacji niejawnych, znajduje się w Załączniku nr 6.

[125] Dotyczy to współpracy lub przynależności do partii, które odwołują się w swoich programach do totalitarnych metod i praktyk działania nazizmu, faszyzmu i komunizmu, a także tych, których program lub działalność zakłada lub dopuszcza nienawiść rasową i narodowościową, stosowanie przemocy w celu zdobycia władzy lub wpływu na politykę państwa albo przewiduje utajnienie struktur lub członkostwa.

Ponadto, w czasie postępowania poszerzonego i specjalnego dodatkowo należy ustalić czy istnieją wątpliwości:

- związane z wyraźną różnicą między poziomem życia a uzyskiwanymi dochodami;
- związane z ewentualnymi informacjami o chorobie psychicznej lub innych zakłóceniach czynności psychicznych, ograniczających sprawność umysłową i mogących negatywnie wpłynąć na zdolność do zajmowania stanowiska lub wykonywania prac, związanych z dostępem do informacji niejawnych stanowiących tajemnicę państwową;
- związane z uzależnieniem od alkoholu lub narkotyków.

Powyższe ustalenia są na tyle istotne, że Wojskowe Służby Informacyjne mogą zobowiązać osobę sprawdzaną do poddania się specjalistycznym badaniom i udostępnienia ich wyników na potrzeby prowadzonego postępowania. Natomiast, jeżeli w toku czynności sprawdzających nie da się usunąć wyszczególnionych powyżej wątpliwości można odmówić wydania poświadczenia bezpieczeństwa osobie sprawdzanej, dlatego że interes ochrony informacji niejawnych ma pierwszeństwo przed innymi prawnie chronionymi interesami. Dlatego też celem upewnienia się, że poświadczenie bezpieczeństwa osobowego jest wydawane osobie dającej gwarancję zachowania tajemnicy w czasie postępowania sprawdzającego przeprowadza się szereg czynności. Należą do nich:

- W toku zwykłego postępowania sprawdzającego;
  / wypełnienie ankiety bezpieczeństwa osobowego,
  / sprawdzenie, w niezbędnym zakresie, w ewidencjach, rejestrach i kartotekach, a w szczególności w Centralnym Rejestrze Skazanych oraz Kartotece Skazanych i Tymczasowo Aresztowanych, danych zawartych w ankiecie,[126]
  / sprawdzenie, wyłącznie w odniesieniu do osób kandydujących na stanowiska z dostępem do informacji niejawnych oznaczonych klauzulą

[126] Zasoby danych osobowych, zgromadzonych w Centralnym Rejestrze Skazanych na mocy Ustawy z dnia 24 maja 2000 roku o Krajowym Rejestrze Karnym, Dz. U. Nr 50, poz. 580 z późniejszymi zmianami, zostały przejęte przez Krajowy Rejestr Karny. Dlatego ilekroć w przepisach prawa jest mowa o Centralnym Rejestrze Skazanych należy przez to rozumieć Krajowy Rejestr Karny prowadzony przez Ministerstwo Sprawiedliwości.

POUFNE, w ewidencjach i kartotekach niedostępnych powszechnie, prowadzone na pisemny wniosek pełnomocnika przez Wojskowe Służby Informacyjne, danych zawartych w ankiecie,

/ sprawdzanie akt stanu cywilnego dotyczących osoby sprawdzanej,

- W toku poszerzonego postępowania sprawdzającego, Wojskowe Służby Informacyjne oprócz czynności objętych postępowaniem zwykłym, realizują dodatkowo:

/ przeprowadzenie wywiadu w miejscu zamieszkania osoby sprawdzanej,[127]

/ rozmowę z przełożonym osoby sprawdzanej oraz innymi osobami jeżeli istnieje potrzeba uzupełnienia danych zawartych w ankiecie bądź przekazanych przez osobę sprawdzaną,

/ sprawdzenie stanu i obrotów na rachunku bankowym,[128]

/ sprawdzenie zadłużenia osoby sprawdzanej, zwłaszcza wobec Skarbu Państwa, jeśli jest to konieczne w celu weryfikacji danych zawartych w ankiecie,[129]

- W toku specjalnego postępowania sprawdzającego Wojskowe Służby Informacyjne realizują czynności objęte zwykłym i poszerzonym postępowaniem a ponadto wykonują dodatkowo następujące czynności;

/ rozmowa z osobą sprawdzaną,

/ rozmowa z trzema osobami wskazanymi przez osobę sprawdzaną w celu potwierdzenia jej tożsamości i danych zawartych w ankiecie oraz przekazanych przez osobę sprawdzaną.

Jakkolwiek zakres poszerzonego i specjalnego postępowania sprawdzającego jest dosyć szeroki to jednak może się okazać, iż nawet przeprowadzenie wszystkich

---

[127] Wywiad przeprowadzają wyspecjalizowane komórki Wojskowych Służb Informacyjnych stosując w tym zakresie przepisy postępowania karnego i wydane na jego podstawie przepisy dotyczące wywiadu środowiskowego. Jest on wymagany, jeśli konieczne jest potwierdzenie danych zawartych w ankiecie. W środowisku wojskowym dopuszczalne jest odstąpienie od przeprowadzenia wywiadu i załączenie do akt postępowania opinii środowiskowej w sytuacji, gdy oficer WSI prowadzący postępowanie zna osobiście osobę sprawdzaną.

[128] Sprawdzenia dokonuje się w uzasadnionych przypadkach w trybie art. 104 ust. 2 Ustawy z dnia 29 sierpnia 1997 roku - Prawo bankowe, Dz. U. Nr 140, poz. 939 z późniejszymi zmianami.

czynności nie pozwoli na usunięcie wszystkich wątpliwości dotyczących osoby sprawdzanej. W takim wypadku Wojskowe Służby Informacyjne mają obowiązek zapewnienia osobie sprawdzanej możliwości osobistego ustosunkowania się do faktycznych przesłanek powodujących te wątpliwości. Wysłuchanie, na które osoba sprawdzana może stawić się z pełnomocnikiem musi odbyć się zgodnie z procedurami zawartymi w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Jednakże Wojskowe Służby Informacyjne mogą odstąpić od wysłuchania, jeśli jego przeprowadzenia mogłoby naruszyć zasady ochrony informacji niejawnych, stanowiących tajemnicę państwową. Dotyczy to na przykład sytuacji, gdy Wojskowe Służby Informacyjne posiadają wiarygodne informacje na temat osoby sprawdzanej, pochodzące z prowadzonych wobec niej czynności operacyjnych.

Każde postępowanie sprawdzające dokumentowane jest w formie akt postępowania sprawdzającego, prowadzone i ewidencjonowane oddzielnie[130] oraz kończy się wydaniem poświadczenia bezpieczeństwa osobowego[131] bądź odmową wydania takiego poświadczenia[132]. Zarówno pełnomocnik ochrony jak i Wojskowe Służby Informacyjne wydają poświadczenie osobie sprawdzanej powiadamiając o tym osobę upoważnioną do obsady stanowiska. Analogiczna procedura obowiązuje w przypadku odmowy wydania poświadczenia bezpieczeństwa, jednakże dostarczenie odmowy odbywa się według zasad określonych w Kodeksie Postępowania Administracyjnego, za pokwitowaniem, przez pocztę lub osobiście, w miejscu zamieszkania lub miejscu pracy.[133] Jest to wyjątek od ustawowej reguły, która stanowi, iż do postępowania sprawdzającego przed wydaniem poświadczenia

---

[129] W czasie sprawdzenia stosuje się przepisy art. 82 i art. 182 Ustawy z dnia 29 sierpnia 1997 roku – Ordynacja podatkowa, Dz. U. Nr 137, poz. 926 z późniejszymi zmianami oraz art. 33 ustawy z dnia 28 września 1991 roku o kontroli skarbowej, Dz. U. Nr 100, poz. 442 z późniejszymi zmianami.

[130] § 8 Decyzji Nr 29/MON Ministra Obrony Narodowej z dnia 8 marca 2000r. w sprawie szczegółowych zasad i trybu przeprowadzania postępowań sprawdzających, dokumentowania i archiwizacji materiałów dotyczących postępowań.

[131] Wzór poświadczenia bezpieczeństwa osobowego znajduje się w Załączniku nr 7.

[132] Wzór odmowy wydania poświadczenia bezpieczeństwa osobowego znajduje się w Załączniku nr 8. Wzory poświadczenia bezpieczeństwa i odmowy wydania poświadczenia bezpieczeństwa zostały określone w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 23 lutego 1999 roku w sprawie wzoru poświadczenia bezpieczeństwa i odmowy wydania poświadczenia bezpieczeństwa.

[133] Rozdział 8 – Doręczenia, Ustawy z dnia 14 czerwca 1960r. Kodeks Postępowania Administracyjnego, Dz. U. z 2000 roku, Nr 98, poz. 1071.

bezpieczeństwa osobowego nie stosuje się przepisów Kodeksu Postępowania Administracyjnego.

Odmowa wydania poświadczenia bezpieczeństwa, będąca zmaterializowaną formą braku rękojmii zachowania tajemnicy osoby sprawdzanej jest bardzo ważną decyzją administracyjną. Jednakże nie jest wiążąca dla osoby upoważnionej do obsady stanowiska, z którym związany jest dostęp do informacji stanowiących tajemnicę służbową, nie powoduje na przykład obligatoryjnego zwolnienia z pracy osoby ocenionej negatywnie. Natomiast w przypadku obsady stanowiska bądź zlecenia pracy osobie, której odmówiono wydania poświadczenia upoważniającego do dostępu do informacji niejawnych oznaczonych klauzulą POUFNE osoba upoważniona do obsady stanowiska jest zobowiązana powiadomić o tym Wojskowe Służby Informacyjne. W przypadku otrzymania informacji o odmowie wydania poświadczenia przez WSI jej obowiązkiem jest natychmiastowe uniemożliwienie osobie ocenionej negatywnie dostępu do informacji niejawnych.

Następne postępowanie sprawdzające wobec osoby, której odmówiono wydania poświadczenia może nastąpić dopiero po upływie roku od daty odmowy wydania poświadczenia.

Osoba, której Wojskowe Służby Informacyjne, po zakończeniu postępowania poszerzonego lub specjalnego, odmówiły wydania poświadczenia bezpieczeństwa ma prawo odwołania się od tej decyzji do prezesa Rady Ministrów[134]. Odwołanie musi być dokonane w terminie 14 dni od daty doręczenia odmowy za pośrednictwem Wojskowych Służb Informacyjnych, które zobowiązane są w nieprzekraczalnym terminie 14 dni od daty otrzymania odwołania do przesłania odwołania wraz z aktami postępowania sprawdzającego prezesowi Rady Ministrów. Zgodnie z Ustawą o ochronie informacji niejawnych prezes Rady Ministrów stwierdza w drodze postanowienia niedopuszczalność odwołania oraz uchybienie terminu do wniesienia odwołania bądź po rozpatrzeniu odwołania wydaje decyzję, w której:

---

[134] W stosunku do osób ubiegających się o przyjęcie do służby lub pracy w Żandarmerii Wojskowej, którym Żandarmerii Wojskowa odmówiła wydania poświadczenia bezpieczeństwa mają zastosowanie te same przepisy, jakie obowiązują w procedurze odwoławczej od odmowy wydania poświadczenia bezpieczeństwa przez Wojskowe Służby Informacyjne.

- utrzymuje w mocy decyzję Wojskowych Służb Informacyjnych w sprawie odmowy wydania poświadczenia bezpieczeństwa;
- nakazuje Wojskowym Służbom Informacyjnym wydać poświadczenie bezpieczeństwa.

Po rozpatrzeniu odwołania akta postępowania sprawdzającego zwracane są Wojskowym Służbom Informacyjnym, postanowienie prezesa Rady Ministrów na piśmie doręczane jest Wojskowym Służbom Informacyjnym i osobie sprawdzanej a zawiadomienie o podjętej decyzji przekazywane jest osobie upoważnionej do obsady stanowiska zajmowanego przez osobę, której odmówiono wydania poświadczenia bezpieczeństwa. Doręczenie decyzji i postanowienia odbywa się zgodnie z przepisami zawartymi w Kodeksie Postępowania Administracyjnego.

Osoba, której, po zakończeniu zwykłego postępowania sprawdzającego, pełnomocnik ochrony jednostki organizacyjnej odmówił wydania poświadczenia bezpieczeństwa ma prawo odwołania się od tej decyzji do Szefa Wojskowych Służb Informacyjnych.

Zarówno na postanowienie i decyzje prezesa Rady Ministrów jak i decyzje Szefa Wojskowych Służb Informacyjnych o utrzymaniu w mocy odmowy wydania poświadczenia bezpieczeństwa osobie sprawdzanej służy prawo wniesienia skargi do Naczelnego Sądu Administracyjnego w terminie 30 dni od daty doręczenia decyzji lub postanowienia. Skarga taka rozpoznawana jest na posiedzeniu niejawnym a wyrok uzasadnia się jedynie w przypadku uwzględnienia skargi. Po rozpatrzeniu skargi Naczelny Sąd Administracyjny zwraca Wojskowym Służbom Informacyjnym akta postępowania sprawdzającego oraz dostarcza odpis wyroku wraz z uzasadnieniem. Natomiast osobie wnoszącej skargę jak również osobie upoważnionej do obsady stanowiska doręczany jest jedynie odpis wyroku.

Zgodnie z polskim systemem prawnym, po rozpatrzeniu skargi przez Naczelny Sąd Administracyjny możliwa jest jeszcze, w wypadku ujawnienia nowych istotnych dla decyzji o odmowie wydania poświadczenia bezpieczeństwa okoliczności, rewizja nadzwyczajna. Wniosek o rewizję nadzwyczajną przeprowadza Naczelny Sąd Administracyjny na zasadach określonych dla rozpatrywania skargi wniesionej przez osobę, której odmówiono wydania

poświadczenia bezpieczeństwa. Rewizję nadzwyczajną *(kasację)* może wnieść Minister Sprawiedliwości – Prokurator Generalny a także Rzecznik Praw Obywatelskich.[135] W praktyce wygląda to następująco: osoba, w stosunku do której Naczelny Sąd Administracyjny utrzymał w mocy odmowę wydania poświadczenia bezpieczeństwa może skierować wniosek do Ministra Sprawiedliwości – Prokuratora Generalnego o złożenie na jej korzyść rewizji nadzwyczajnej *(kasacji)*. W przypadku uwzględnienia wniosku odbywa się kolejne posiedzenie Naczelnego Sądu Administracyjnego. W przypadku odmowy uwzględnienia tego wniosku przez Ministra Sprawiedliwości – Prokuratora Generalnego Rzecznik Praw Obywatelskich może wystąpić z wnioskiem o rewizję nadzwyczajną. Wystąpienie Rzecznika ma miejsce w sytuacjach wyjątkowych, gdy osoba, której odmowa dotyczy jest osobą bezradną a naruszenie jej praw wydaje się oczywiste.[136]

Zgodnie z Ustawą o ochronie informacji niejawnych poświadczenie bezpieczeństwa jest ważne przez okres:

- 10 lat w przypadku upoważnienia do dostępu do informacji stanowiących tajemnicę służbową oznaczonych klauzulami ZASTRZEŻONE i POUFNE;
- 5 lat w przypadku upoważnienia do dostępu do informacji stanowiących tajemnicę państwową oznaczonych klauzulą TAJNE;
- 3 lat w przypadku upoważnienia do dostępu do informacji stanowiących tajemnicę państwową o klauzuli ŚCIŚLE TAJNE.

Po upływie wyszczególnionych powyżej terminów następuje wszczęcie kolejnego postępowania sprawdzającego, na podstawie polecenia kierownika jednostki organizacyjnej *(w przypadku zwykłego postępowania sprawdzającego)* bądź wniosku do Wojskowych Służb Informacyjnych *(w przypadku postępowań poszerzonych i specjalnych)*. Polecenie powinno być wydane bądź wniosek o wszczęcie kolejnego postępowania winien być złożony co najmniej na 6 miesięcy przed upływem ważności posiadanego poświadczenia.

---

[135] Art. 521 Kodeksu Postępowania Karnego.

[136] Uprawnienia Rzecznika Praw Obywatelskich określone są w Ustawie z dnia 15 lipca 1987 roku o Rzeczniku Praw Obywatelskich, Dz. U. z 2001 roku, Nr 109, poz. 471.

Wszczęcie postępowania może nastąpić wcześniej. Dotyczy to przypadku, gdy w odniesieniu do osoby posiadającej poświadczenie ujawnione zostaną nowe fakty, świadczące o tym, iż nie daje ona rękojmii zachowania tajemnicy. Pełnomocnik bądź Wojskowe Służby Informacyjne wszczynają wówczas postępowanie, które nie wymaga wypełnienia nowej ankiety bezpieczeństwa, powiadamiając o tym fakcie osobę sprawdzaną i osobę odpowiedzialną za obsadę stanowiska. Może ona ograniczyć w tym przypadku dostęp do informacji niejawnych osobie objętej nowym postępowaniem.

Akta zakończonych postępowań sprawdzających przechowywane są przez pełnomocnika ochrony przez 10 lat w jednostce organizacyjnej, w której przeprowadzono postępowanie. Po tym okresie są przekazywane do właściwego archiwum wojskowego i nadaje się im klauzulę B-20, to znaczy przechowywane są jeszcze przez okres dwudziestu lat. O przekazaniu akt pełnomocnik ochrony zawiadamia w terminie 7 dni właściwą terytorialnie jednostkę organizacyjną Wojskowych Służb Informacyjnych.

Ustawa stanowi, iż w czasie przechowywania w jednostce organizacyjnej akta postępowań sprawdzających mogą być zostać udostępnione do wglądu jedynie:

- osobie sprawdzanej;
- na żądanie sądu lub prokuratora w celu ścigania karnego, albo prezesowi Rady Ministrów, szefowi Wojskowych Służb Informacyjnych, Komendantowi Głównemu Żandarmerii Wojskowej w celu rozpatrzenia odwołania oraz Naczelnemu Sądowi Administracyjnemu w związku z rozpatrywaniem skargi;
- osobie upoważnionej do obsady stanowiska lub Wojskowym Służbom Informacyjnym dla celów postępowania sprawdzającego.

Akta postępowań sprawdzających przeprowadzonych przez Wojskowe Służby Informacyjne przechowywane są jako wyodrębniona część w archiwach terytorialnie właściwych jednostek organizacyjnych WSI.

W związku z tym, że Wojskowe Służby Informacyjne muszą posiadać wiedzę na temat ilości przeprowadzonych postępowań, choćby na potrzeby ocen i

analiz opracowywanych dla Kolegium do spraw Służb Specjalnych, mocą ustawy zostały zobowiązane do prowadzenia ewidencji:

- osób, które uzyskały poświadczenie bezpieczeństwa osobowego;
- osób, które zajmują stanowiska lub wykonują prace, z którymi łączy się dostęp do informacji oznaczonych klauzulą POUFNE lub stanowiących tajemnicę państwową;
- osób, którym odmówiono wydania poświadczenia bezpieczeństwa osobowego.

Dane z ewidencji oraz akta zakończonych przez pełnomocnika postępowań sprawdzających podlegają ustawowej ochronie, dlatego też mogą być udostępniane wyłącznie na żądanie sądu lub prokuratora w celu ścigania karnego lub Wojskowym Służbom Informacyjnym dla celów postępowania sprawdzającego a także prezesowi Rady Ministrów, szefowi Wojskowych Służb Informacyjnych w celu rozpatrzenia odwołania oraz Naczelnemu Sądowi Administracyjnemu w związku z rozpatrywaniem skargi. Analogiczne zasady obowiązują przy udostępnianiu danych z ewidencji i akt poszerzonych i specjalnych postępowań, przeprowadzonych przez właściwe terytorialnie jednostki organizacyjne Wojskowych Służb Informacyjnych.

Dane ewidencyjne mogą obejmować wyłącznie:

- w odniesieniu do osoby – jej imię i nazwisko, imię ojca, datę i miejsce urodzenia, adres miejsca zamieszkania lub pobytu, nazwę i adres jednostki organizacyjnej, w której osoba jest zatrudniona, nazwę komórki organizacyjnej i stanowiska oraz sygnaturę akt postępowania sprawdzającego;
- w odniesieniu do stanowiska lub pracy zleconej – datę objęcia stanowiska lub rozpoczęcia pracy, określenie z dostępem do jakich informacji niejawnych łączy się to stanowisko, datę wydania i numer poświadczenia bezpieczeństwa.[137]

Dane z ewidencji przekazuje się na pisemne żądanie sądu, prokuratora lub Wojskowych Służb Informacyjnych, zawierające oznaczenie zakresu żądanych

[137] Art. 42 ust. 6 Ustawy o ochronie informacji niejawnych.

danych. Są one udostępniane w formie pisemnej (*bądź przekazane za pomocą systemu lub sieci teleinformatycznej)* oraz w terminie i w zakresie określonym w żądaniu. Osobą uprawnioną do udostępniania danych z ewidencji jest szef Wojskowych Służb informacyjnych lub upoważniony przez niego żołnierz[138].

Od początku obowiązywania ustawy pełnomocnicy ochrony w jednostkach organizacyjnych Sił Zbrojnych wydali kilkakrotnie mniej poświadczeń bezpieczeństwa osobowego niż Wojskowe Służby Informacyjne. Ten stan rzeczy wynika przede wszystkim z faktu, iż analizowana ustawa stanowi, że „.... wydane, na podstawie dotychczasowych przepisów upoważnienia do dostępu do wiadomości stanowiących tajemnicę państwową lub służbową:

- osobom na stanowiskach objętych wymogiem przeprowadzenia specjalnego postępowania sprawdzającego – tracą ważność po 12 miesiącach od dnia wejścia w życie ustawy *(a więc 11 marca 2000 roku)*;
- osobom na stanowiskach objętych wymogiem przeprowadzenia poszerzonego postępowania sprawdzającego – tracą ważność po 18 miesiącach od dnia wejścia w życie ustawy *(a więc 11 września 2000 roku)*;
- osobom na stanowiskach objętych wymogiem przeprowadzenia zwykłego postępowania sprawdzającego – tracą ważność po 24 miesiącach od dnia wejścia w życie ustawy *(a więc 11 marca 2001 roku)*.[139]

Powyższa regulacja spowodowała, iż pełnomocnicy ochrony nie musieli śpieszyć się z przeprowadzeniem postępowań i wydaniem poświadczeń bezpieczeństwa osobowego tak jak było to w przypadku Wojskowych Służb Informacyjnych, zwłaszcza w zakresie upoważniania osób do dostępu do informacji ŚCIŚLE TAJNYCH.

Inną przyczyną znacznej różnicy w ilości zrealizowanych postępowań było to, iż pomimo ustawowo określonego obowiązku powołania pełnomocników w terminie 3 miesięcy od dnia wejścia w życie ustawy o ochronie informacji

---

[138] Tryb udostępniania danych z ewidencji określony jest w Rozporządzeniu Prezesa Rady Ministrów z dnia 25 lutego 1999r. w sprawie sposobu i trybu udostępniania danych z ewidencji.
[139] Art. 87 Ustawy o ochronie informacji niejawnych.

niejawnych a więc do połowy 1999 roku, etatowi pełnomocnicy w jednostkach organizacyjnych resortu obrony narodowej zaczęli funkcjonować dopiero od 1 stycznia 2001 roku.

Ponadto, wydaje się, iż w początkowym okresie obowiązywania ustawy o ochronie informacji niejawnych kierownicy jednostek organizacyjnych resortu obrony narodowej, często z inspiracji bądź za namową pełnomocników zawyżali poziom dostępu do informacji niejawnych, obowiązujący na konkretnych stanowiskach służbowych tylko po to, aby przerzucić obowiązek przeprowadzenia postępowania sprawdzającego na Wojskowe Służby Informacyjne jako służbę ochrony państwa. Praktyka ta okazała się w wielu przypadkach krótkowzroczną a jej skutkiem było nieuzasadnione zawyżanie poziomu dostępu do informacji niejawnych na stanowiskach, które w istocie wcale tego nie wymagały.

W trakcie prowadzonych przez pełnomocników ochrony i Wojskowe Służby Informacyjne postępowań sprawdzających przed wydaniem poświadczenia bezpieczeństwa osobowego występuje szereg trudności, które sprawiają, iż nie jest możliwym zakończenie postępowań sprawdzających w ustawowo przewidzianych terminach *(1 miesiąc dla zwykłego, 2 miesiące dla poszerzonego i 3 miesiące dla specjalnego postępowania sprawdzającego).* Do zasadniczych przyczyn, uniemożliwiających sfinalizowanie postępowań w terminach ustawowych należą:

- długi okres oczekiwania na wyniki sprawdzeń w kartotekach powszechnie niedostępnych, wyniki wywiadów prowadzonych w miejscach zamieszkania osoby sprawdzanej oraz na zapytania z urzędów stanu cywilnego;
- trudności z przeprowadzeniem rozmów z osobami sprawdzanymi oraz polecającymi, które w trakcie postępowania sprawdzającego zmieniają miejsce pełnienia służby, co wynika między innymi z reorganizacji Sił Zbrojnych, wyjazdów za granicę celem wykonywania obowiązków w strukturach NATO lub w misjach pokojowych lub uczestnictwa w długotrwałych formach szkolenia takich jak poligony czy ćwiczenia poza miejscem stałej dyslokacji;

- nie dotrzymywanie przez kierowników jednostek organizacyjnych ustawowego obowiązku występowania z wnioskiem o przeprowadzenie postępowania sprawdzającego na co najmniej 6 miesięcy przed wygaśnięciem terminu uprzednio wydanego poświadczenia bądź upoważnienia;
- lawinowy napływ, w krótkim czasie, wniosków o przeprowadzenie postępowań przed upływem terminu ważności wcześniej wydanych upoważnień do dostępu do informacji TAJNYCH i ŚCIŚLE TAJNYCH *(miało to na przykład miejsce przed 11 września 2000 roku i 11 marca 2001 roku);*
- konieczność prowadzenia kolejnych postępowań wobec tych samych osób w związku z wyznaczeniem na inne stanowisko służbowe wymagające wyższego poziomu dostępu do informacji niejawnych bądź w związku z podwyższeniem poziomu dostępu, błędnie określonego przy pierwszym wnioskowaniu o przeprowadzenie postępowania sprawdzającego;
- zawyżanie klauzul tajności dokumentów, znajdujących się w jednostce organizacyjnej, co wymaga przeprowadzenia stosownych postępowań. Typowym przykładem są tabele sygnałowe używane w jednostkach wojskowych przez służby dyżurne. Dla wielu żołnierzy zawodowych tabele te są jedynym dokumentem o klauzuli TAJNE, z którymi mają styczność. Biorąc pod uwagę ilość osób pełniących służbę dyżurną w jednostkach wojskowych można sobie wyobrazić jak dużą ilość postępowań należy wobec tych osób przeprowadzić.[140]

4. Regulacje dotyczące postępowań sprawdzających przed wydaniem świadectwa bezpieczeństwa przemysłowego.

Stosownie do zapisów Ustawy o ochronie informacji niejawnych przedsiębiorcy, jednostki naukowe lub badawczo – rozwojowe, ubiegający się o zawarcie umowy związanej z dostępem do informacji niejawnych albo wykonujący

[140] Źródło – opracowanie własne, na podstawie osobistych ocen i obserwacji.

zadania na rzecz obronności i bezpieczeństwa państwa, związane z dostępem do informacji niejawnych, mają obowiązek ochrony tych informacji.[141] Wymóg ten dotyczy zarówno przedsiębiorców, którzy dopiero ubiegają się o kontrakt na rzecz obronności jak i tych, którzy w momencie wejścia w życie ustawy już realizowali prace niejawne na zamówienia jednostek organizacyjnych resortu obrony narodowej.

Dodatkowym wymogiem, w przypadku gdy realizacja prac czy umowy na rzecz obronności łączy się z dostępem do informacji niejawnych stanowiących tajemnicę państwową jest uzyskanie świadectwa bezpieczeństwa przemysłowego. Świadectwo jest wymagane, gdy przedsiębiorca ubiega się o realizację umowy bądź z chwilą wejścia w życie ustawy już realizował prace na rzecz obronności, które łączyły się z udostępnianiem informacji stanowiących tajemnicę państwową. Przy realizacji umów na rzecz innych państw lub organizacji międzynarodowych dodatkowo należy uwzględniać wymogi, jakie stawiane są przez zapisy umów międzynarodowych. Bardzo istotnym jest na przykład fakt, iż w odniesieniu do kontraktów natowskich wymagane jest świadectwo bezpieczeństwa przemysłowego już wówczas, gdy przedsiębiorcy udostępniane są informacje o klauzuli CONFIDENTIAL, bowiem tak stanowią przepisy bezpieczeństwa NATO.[142]

Obowiązkiem zleceniodawcy wojskowego[143] zawierającego z przedsiębiorcą umowę jest dopilnowanie, aby znalazły się w niej następujące elementy:

- szczegółowe wymagania dotyczące ochrony informacji niejawnych stanowiących tajemnicę państwową lub służbową, zwane „instrukcją bezpieczeństwa przemysłowego". Wymagania muszą odpowiadać ilości przekazywanych przedsiębiorcy informacji, ich klauzuli tajności oraz liczby osób, którym będą udostępniane;
- skutki oraz zakres odpowiedzialności obu stron umowy z tytułu niewykonania lub niewłaściwego wykonania obowiązków wynikających

---

[141] Art. 65 Ustawy o ochronie informacji niejawnych.

[142] Regulacje natowskie w sferze bezpieczeństwa przemysłowego omówione są w Rozdziale III.

[143] Zleceniodawcą wojskowym jest uprawniona do podpisywania umów, dysponująca środkami budżetowymi, jednostka organizacyjna resortu obrony narodowej jak na przykład Departament Zaopatrywania Sił Zbrojnych, Dowództwo Wojsk Lądowych, dowódca jednostki wojskowej.

z ustawy o ochronie informacji niejawnych oraz z instrukcji bezpieczeństwa przemysłowego.

Ponadto zleceniodawca jest zobowiązany do wyznaczenia osoby odpowiedzialnej za nadzorowanie, kontrolę, szkolenie i doradztwo w zakresie wykonywania przez przedsiębiorcę, jednostkę naukową lub badawczo – rozwojową obowiązku ochrony przekazanych informacji niejawnych.

Niezależnie od powyższych czynności, jeśli realizacja umowy wiąże się z udostępnianiem wykonawcy informacji niejawnych stanowiących tajemnicę państwową Wojskowe Służby Informacyjne przeprowadzają postępowanie sprawdzające mające na celu ocenę rękojmi zachowania tajemnicy a także sprawdzenie zdolności finansowej i organizacyjnej przedsiębiorcy, jednostki naukowej lub badawczo – rozwojowej do skutecznej ochrony informacji niejawnych.

Zgodnie z Ustawą o ochronie informacji niejawnych, Wojskowe Służby Informacyjne są właściwe do przeprowadzania postępowań sprawdzających przed wydaniem świadectwa bezpieczeństwa przemysłowego wobec:

- przedsiębiorców, jednostek naukowych lub badawczo-rozwojowych, których organem założycielskim jest minister obrony narodowej, w związku z realizacją umów zarówno w kraju jak i za granicą;
- innych jednostek organizacyjnych w zakresie, w jakim realizują one, w kraju lub za granicą, produkcję lub usługi, stanowiące tajemnicę państwową ze względu na obronność państwa i potrzeby Sił Zbrojnych;
- przedsiębiorców zajmujących się obrotem wyrobami, technologiami i licencjami objętymi tajemnicą państwową ze względu na obronność państwa, jeżeli uczestnikami tego obrotu są Siły Zbrojne lub jednostki organizacyjne podległe ministrowi obrony narodowej.

Postępowanie sprawdzające wobec przedsiębiorcy, jednostki naukowej lub badawczo – rozwojowej prowadzone, przez Wojskowe Służby Informacyjne z urzędu bądź na wniosek uprawnionej jednostki organizacyjnej resortu obrony narodowej obejmuje:

- sprawdzenie osób zajmujących stanowiska związane z kierowaniem, wykonaniem umowy lub z jej bezpośrednią realizacją;
- sprawdzenie innych osób, uczestniczących w czynnościach mających na celu zawarcie umowy, jeśli są one związane z dostępem do informacji niejawnych;
- sprawdzenie osób zatrudnionych w pionie ochrony[144];
- sprawdzenie działającego na rzecz zleceniodawcy przedsiębiorcy, który uzyskał koncesję na prowadzenie działalności gospodarczej w zakresie wykonywania usług ochrony mienia i osób;
- sprawdzenie struktury i pochodzenia kapitału przedsiębiorcy;
- sprawdzenie struktury organizacyjnej przedsiębiorcy, jednostki naukowej lub badawczo – rozwojowej oraz ich władz;
- sprawdzenie sytuacji finansowej i źródeł pochodzenia środków finansowych.

Z wnioskiem o przeprowadzenie postępowania sprawdzającego zwraca się do Wojskowych Służb Informacyjnych zleceniodawca wojskowy.[145] Należy w nim podać:

- adres jednostki organizacyjnej składającej wniosek;
- przedmiot umowy lub zadanie, nazwę i adres przedsiębiorcy, jednostki naukowej lub badawczo – rozwojowej, której jednostka organizacyjna zamierza zlecić lub zleciła wykonanie umowy lub zadania;
- najwyższą konieczną klauzulę tajności informacji niejawnych, do których dostęp będzie łączyć się z wykonaniem umowy lub zadania.

Do wniosku załącza się kwestionariusz bezpieczeństwa przemysłowego,[146] stanowiący dla Wojskowych Służb Informacyjnych podstawowe źródło informacji

---

[144] Osoby wyszczególnione w powyższych punktach, z wyjątkiem osoby zajmującej stanowisko pełnomocnika nie muszą posiadać obywatelstwa polskiego.

[145] Obowiązek przekazywania wniosku za pośrednictwem zleceniodawcy został wprowadzony przez nowelizację ustawy w kwietniu 2001 roku. Zgodnie z pierwszą wersją ustawy z wnioskiem o przeprowadzenie postępowania, do Wojskowych Służb Informacyjnych występowali bezpośrednio przedsiębiorcy.

[146] Wzór kwestionariusza bezpieczeństwa przemysłowego, wprowadzony mocą Rozporządzenia Rady Ministrów z dnia 9 lutego 1999 roku w sprawie wzorów: kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, odmowy wydania świadectwa bezpieczeństwa przemysłowego, znajduje się w Załączniku Nr 9.

o przedsiębiorcy, jednostce naukowej lub badawczo – rozwojowej i materiał służący do przeprowadzenia wymaganych analiz. Dlatego kwestionariusz bezpieczeństwa przemysłowego musi zawierać:

- dane dotyczące statusu prawnego;
- dane o strukturze organizacyjnej i kapitałowej;
- dane dotyczące władz lub organów zarządzających;
- wykaz pracowników uprawnionych do dostępu do informacji niejawnych;
- wykaz pracowników, którzy powinni mieć dostęp do informacji niejawnych, w związku z postępowaniem zmierzającym do zawarcia umowy lub jej wykonaniem;
- dane dotyczące systemu ochrony osób, materiałów oraz obiektów;
- wykaz osób, które będą odpowiedzialne za ochronę przekazanych informacji niejawnych;
- czytelny podpis osoby upoważnionej do składania oświadczeń woli w imieniu przedsiębiorcy, kierownika jednostki naukowej lub badawczo – rozwojowej.

Razem z kwestionariuszem przesyłane są ankiety bezpieczeństwa osobowego z wnioskami o przeprowadzenie postępowania sprawdzającego przed wydaniem poświadczenia bezpieczeństwa osobowego lub kopie posiadanych przez te osoby poświadczeń bezpieczeństwa.

O każdej zmianie danych zawartych w kwestionariuszu bezpieczeństwa przedsiębiorca, jednostka naukowa lub badawczo – rozwojowa są obowiązani niezwłocznie informować zarówno Wojskowe Służby Informacyjne jak i zleceniodawcę. Obowiązek ten dotyczy w szczególności danych dotyczących kondycji finansowej a także ogłoszenia upadłości, likwidacji lub rozwiązania, wypowiedzenia umowy bądź potrzeby zawarcia umowy z podwykonawcą.

Wojskowe Służby Informacyjne, w ramach czynności wykonywanych podczas postępowania sprawdzającego przed wydaniem świadectwa bezpieczeństwa przemysłowego są zobowiązane do:

- sprawdzenia poprawności wypełnienia kwestionariusza bezpieczeństwa przemysłowego oraz analizy i weryfikacji zawartych w nim danych. W wypadku niewłaściwego wypełnienia kwestionariusza jest on odsyłany, za pośrednictwem zleceniodawcy, do uzupełnienia;
- sprawdzenia czy został wyznaczony pełnomocnik do spraw ochrony informacji niejawnych oraz czy zorganizowano pion ochrony;
- sprawdzenia, w zakresie bezpieczeństwa osobowego, czy wszystkie osoby związane z wykonywaniem umowy oraz z zapewnieniem bezpieczeństwa jej realizacji posiadają aktualne, ważne poświadczenia bezpieczeństwa uprawniające do dostępu do dokumentów o odpowiedniej klauzuli tajności *(w przypadku, gdy osoby wymienione w kwestionariuszu bezpieczeństwa przemysłowego nie posiadają poświadczeń bezpieczeństwa w pierwszej kolejności przeprowadza się wobec nich postępowania sprawdzające w celu wydania stosownych poświadczeń);*
- przeprowadzenia ustaleń dotyczących struktury i pochodzenia kapitału, struktury organizacyjnej oraz jej władz *(zarząd, rada nadzorcza)*, sytuacji finansowej *(zadłużenia, posiadane wierzytelności)*, wyników rocznych bilansów ekonomiczno-finansowych za okres dwóch ostatnich lat rozliczeniowych.

Po przeprowadzonej analizie i uzyskaniu odpowiedzi z właściwych urzędów, organów kontroli skarbowej i podatkowej w Wojskowych Służbach Informacyjnych powoływany jest zespół specjalistów do dokonania sprawdzenia systemu ochrony informacji niejawnych w siedzibie przedsiębiorcy, jednostki naukowej lub badawczo – rozwojowej. Zespół skupiający ekspertów w dziedzinach bezpieczeństwa osobowego, fizycznego i teleinformatycznego dokonuje porównania danych zawartych w przekazanych materiałach ze stanem faktycznym w siedzibie podmiotu ubiegającego się o wydanie świadectwa bezpieczeństwa przemysłowego.

W zakresie bezpieczeństwa fizycznego sprawdza się czy:

- wydzielone zostały strefy bezpieczeństwa podlegające szczególnej ochronie;

- wokół stref bezpieczeństwa wydzielone zostały strefy administracyjne;
- funkcjonuje system wydawania przepustek lub inny systemu określający uprawnienia do wejścia, przebywania i wyjścia ze strefy bezpieczeństwa;
- funkcjonuje zorganizowana zgodnie ze stosownymi przepisami kancelaria tajna;
- wyposażenie i urządzenia służące do ochrony informacji niejawnych posiadają przyznane, na podstawie odrębnych przepisów, certyfikaty lub świadectwa kwalifikacyjne;
- opracowano plan ochrony fizycznej.

W zakresie bezpieczeństwa teleinformatycznego sprawdza się czy:

- systemy lub sieci teleinformatyczne, służące do wytwarzania, przechowywania przetwarzania lub przekazywania informacji niejawnych posiadają certyfikaty wydane przez Jednostkę Certyfikującą Wyroby w Wojskowych Służbach Informacyjnych;[147]
- do wytwarzania dokumentów zawierających informacje niejawne stosowane są bezpieczne zestawy komputerowe, np. spełniające wymogi amerykańskiej normy TEMPEST[148];
- czy powołano administratora systemu, inspektora bezpieczeństwa teleinformatycznego.

W zakresie bezpieczeństwa osobowego sprawdza się czy:

- powołany jest pełnomocnik ochrony;
- osoby zaangażowane w realizację umowy posiadają wymagane poświadczenia bezpieczeństwa osobowego.

W przypadku pozytywnego wyniku postępowania sprawdzającego, zespół kontrolny wnioskuje do szefa Wojskowych Służb Informacyjnych o wydanie świadectwa bezpieczeństwa przemysłowego potwierdzającego zdolność przedsiębiorcy, jednostki naukowej lub badawczo – rozwojowej do zapewnienia ochrony informacji niejawnych przed nieuprawnionym ujawnieniem w trakcie

---

[147] Tryb certyfikacji systemów i sieci teleinformatycznych opisany jest w Rozdziale II/5.

[148] Norma TEMPEST *(ang. temporary emanation and spurious transmission)* została nadana programowi ochrony przed niekontrolowaną emisją ujawniającą, na przykład z komputerów, który powstał w latach 50-tych w USA na zlecenie Pentagonu. Na przestrzeni lat standard ten był wielokrotnie rewidowany i publikowany pod różnymi nazwami /NAG1A, FS222, NACSIM 5100, NSCD,

realizacji umowy na rzecz resortu obrony narodowej. W przypadku negatywnej oceny zespołu kontrolnego szef Wojskowych Służb Informacyjnych odmawia wydania świadectwa bezpieczeństwa przemysłowego. Oprócz negatywnej oceny zespołu kontrolnego podstawę do wydania odmowy może stanowić świadome podanie nieprawdziwych danych, ich zatajenie w kwestionariuszu lub nie przekazanie Wojskowym Służbom Informacyjnym istotnych informacji, na przykład o kondycji finansowej.

Zarówno świadectwo bezpieczeństwa przemysłowego jak i odmowa[149] muszą zawierać:

- określenie, iż Wojskowe Służby Informacyjne są służbą ochrony państwa, właściwą do wydania bądź odmowy wydania świadectwa;
- miejsce i datę wystawienia;
- nazwę przedsiębiorcy, jednostki naukowej lub badawczo – rozwojowej i ich siedzibę;
- podstawę prawną wydania;
- stwierdzenie o wydaniu świadectwa bezpieczeństwa przemysłowego albo o odmowie;
- imienną pieczęć i czytelny podpis szefa Wojskowych Służb Informacyjnych.

W związku z tym, iż zgodnie z przyjętymi w ustawie rozwiązaniami Wojskowe Służby Informacyjne wydają świadectwa bezpieczeństwa przemysłowego każdorazowo do realizowanej umowy bądź zadań wykonywanych na rzecz obronności i bezpieczeństwa państwa, ważność świadectwa bezpieczeństwa przemysłowego upływa z chwilą zakończenia realizacji danej umowy bądź zadania. Do każdej następnej umowy wymagane jest nowe świadectwo bezpieczeństwa przemysłowego. Jeżeli w trakcie realizacji umowy przedsiębiorca, jednostka naukowa lub badawczo – rozwojowa poinformują o

---

[149] Wzory świadectwa bezpieczeństwa przemysłowego i odmowy wydania świadectwa bezpieczeństwa przemysłowego, wprowadzone mocą Rozporządzenia Rady Ministrów z dnia 9 lutego 1999 roku w sprawie wzorów: kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, odmowy wydania świadectwa bezpieczeństwa przemysłowego znajdują się odpowiednio w Załącznikach Nr 10 i 11.

istotnych, wpływających na zdolność ochrony informacji niejawnych faktach bądź Wojskowe Służby Informacyjne, nadzorując realizację umowy ustalą tego typu fakty, szef Wojskowych Służb Informacyjnych może cofnąć wydane świadectwo bezpieczeństwa przemysłowego. Decyzja o odmowie wydania świadectwa bezpieczeństwa przemysłowego nie wymaga uzasadnienia. Jednakże dopuszczalnym jest, o ile nie zagraża to istotnym interesom państwa, udostępnienie przez Wojskowe Służby Informacyjne przedstawicielowi przedsiębiorcy, jednostki naukowej lub badawczo – rozwojowej danych zgromadzonych w postępowaniu sprawdzającym, które stanowiły podstawę odmowy.

Materiały zgromadzone przez Wojskowe Służby Informacyjne w czasie postępowania sprawdzającego przed wydaniem świadectwa bezpieczeństwa przemysłowego podlegają ochronie, ich udostępnianie jest możliwe wyłącznie na żądanie sądu lub prokuratora w celu ścigania karnego albo prezydentowi Rzeczypospolitej Polskiej lub prezesowi Rady Ministrów – gdy wymaga tego istotny interes Rzeczypospolitej Polskiej.[150]

Za przeprowadzenie postępowania sprawdzającego i wydanie świadectwa bezpieczeństwa przemysłowego pobiera się opłaty. Ich wysokość określona została w Rozporządzeniu Prezesa Rady Ministrów z dnia 13 lipca 2001 r. w sprawie wysokości opłat za przeprowadzenie postępowania sprawdzającego przez służbę ochrony państwa oraz za wydanie świadectwa bezpieczeństwa przemysłowego[151].

Dotychczasowe doświadczenia związane z prowadzeniem postępowań sprawdzających przed wydaniem świadectwa bezpieczeństwa przemysłowego pozwalają na stwierdzenie, iż dziedzina ta jest bardzo absorbującą sferą odpowiedzialności Wojskowych Służb Informacyjnych.

Interesującym faktem jest, iż w początkowym okresie obowiązywania Ustawy o ochronie informacji niejawnych można było zaobserwować zjawisko lawinowego nadsyłania kwestionariuszy bezpieczeństwa przemysłowego przez przedsiębiorców, którzy mieli trudności z interpretacją zapisów ustawy bądź chcieli tą drogą uzyskać informacje na poczet planowanego w przyszłości udziału w

---

[150] Art. 74, ust. 2 Ustawy o ochronie informacji niejawnych.

[151] Wysokość kwot pobieranych przez Wojskowe Służby Informacyjne za realizację poszczególnych czynności podana jest w Załączniku Nr 12.

przetargu na rzecz resortu obrony narodowej, związanego z udostępnianiem informacji niejawnych stanowiących tajemnicę państwową. Nowelizacja ustawy z kwietnia 2001 roku, wprowadzająca obowiązek nadsyłania kwestionariuszy poprzez zleceniodawcę wojskowego ograniczyła znacznie ilość kierowanych do Wojskowych Służb Informacyjnych wniosków. Przyczynił się również do tego znaczny wzrost poziomu wiedzy w tej dziedzinie zarówno wśród przedsiębiorców jak i zleceniodawców wojskowych. Wzrostowi temu z pewnością służyła działalność szkoleniowa i doradcza Wojskowych Służb Informacyjnych.

W przyszłości należy liczyć się z dużą liczbą wniosków kierowanych do Wojskowych Służb Informacyjnych o przeprowadzenie postępowania przed wydaniem świadectwa bezpieczeństwa przemysłowego. Spodziewać się też należy znacznego wzrostu ilości prowadzonych postępowań i wydawanych certyfikatów bezpieczeństwa przemysłowego NATO w związku z wchodzeniem polskich firm na rynki zagraniczne, ich udziałem w przetargach i realizacją kontraktów, które mają wspomagać wojskową strukturę Paktu Północnoatlantyckiego. Kontrakty te są nadzorowane przez Komitet Infrastruktury NATO *(ang Infrastructure Committee)* i są opłacane z funduszu inwestycyjnego NATO *(ang. NATO Security Investment Programme)*.[152] W wypadku prowadzenia postępowań sprawdzających związanych z kontraktami natowskimi Wojskowe Służby Informacyjne realizują czynności wynikające z norm polskiego prawa i przepisów NATO w tym zakresie.[153]

5. Bezpieczeństwo wytwarzania, przetwarzania, przechowywania i przesyłania informacji niejawnych.

Systemy i sieci teleinformatyczne, służące do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych podlegają szczególnej ochronie, muszą być zorganizowane w sposób wykluczający nieuprawnione

[152] Wraz z wstąpieniem do Sojuszu Polska uzyskała możliwość udziału w tym programie. Poprzez wniesienie określonej kontrybucji przez nasz kraj, polskie firmy uzyskały prawo do udziału w przetargach, ogłaszanych w ramach programu. Kontrakty mogą dotyczyć prac realizowanych na terenie wszystkich państw członkowskich NATO. Zgodnie z oficjalnymi deklaracjami wysokich rangą przedstawicieli Sojuszu i planami wydatkowania sojuszniczych pieniędzy do 2006 roku powinna zostać wydatkowana kwota około 600 milionów dolarów na modernizację i wyposażenie polskiej armii i jej infrastruktury.

[153] Obowiązujące w NATO regulacje dotyczące bezpieczeństwa przemysłowego opisane są w Rozdziale III/3.

ujawnienie tych informacji a także przypadkowe lub świadome narażenie ich bezpieczeństwa.[154]

Bezpieczeństwo teleinformatyczne zapewnia się poprzez[155]:

- ***ochronę fizyczną*** a więc ulokowanie urządzeń systemu lub sieci teleinformatycznej w strefach bezpieczeństwa *(w zależności od klauzuli tajności przetwarzanych informacji niejawnych)* oraz instalację środków zabezpieczających pomieszczenia, w których się one znajdują, przed nieuprawnionym dostępem, podglądem i podsłuchem;
- ***ochronę elektromagnetyczną*** a więc umieszczenie urządzeń, połączeń i linii w strefach bezpieczeństwa gwarantujących spełnienie wymogów zabezpieczenia elektromagnetycznego lub zastosowanie urządzeń, połączeń i linii o obniżonym poziomie emisji albo ich ekranowanie i filtrowanie oraz filtrowanie zewnętrznych linii zasilających i sygnałowych;
- ***ochronę kryptograficzną*** a więc stosowanie metod i środków zabezpieczających informacje niejawne stanowiące tajemnicę państwową przez ich szyfrowanie oraz stosowanie innych mechanizmów kryptograficznych gwarantujących ich integralność i zabezpieczenie przed nieuprawnionym ujawnieniem lub uwierzytelnienie podmiotów, lub uwierzytelnienie informacji[156] ;
- ***bezpieczeństwo transmisji*** a więc szyfrowanie informacji niejawnych przekazywanych w formie elektronicznej poza strefy bezpieczeństwa. W przypadku podłączenia systemu lub sieci, przetwarzającej informacje niejawne stanowiące tajemnicę państwową do powszechnie dostępnego urządzenia systemu lub sieci muszą być zastosowane środki ochrony kryptograficznej. W przypadku podłączenia systemu lub sieci przetwarzających tajemnicę służbową należy stosować właściwe mechanizmy kontroli dostępu;

---

[154] Art. 60 Ustawy o ochronie informacji niejawnych.

[155] Szczegółowe zasady bezpieczeństwa teleinformatycznego zawarte są w Rozporządzeniu Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych.

[156] Uwierzytelnienie to usługa lub funkcja kryptograficzna pozwalająca sprawdzić i potwierdzić autentyczność wymienianych informacji lub podmiotów uczestniczących w wymianie.

- ***kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej*** a więc wyposażenie systemu lub sieci w mechanizmy kontroli dostępu stosownie do klauzuli tajności informacji niejawnych przetwarzanych w tych systemach lub sieciach. W tym celu kierownik jednostki organizacyjnej określa warunki i sposób przydzielenia uprawnień ich użytkownikom a administrator warunki oraz sposób przydzielania tym użytkownikom kont i haseł. Zapewnia on ponadto właściwe wykorzystanie mechanizmów kontroli dostępu.

Z uwagi na fakt, iż ochrona informacji przetwarzanych w systemach i sieciach teleinformatycznych jest niezwykle ważną i ogromną zarazem sferą odpowiedzialności osób funkcyjnych, zadania w dziedzinie bezpieczeństwa teleinformatycznego w jednostkach organizacyjnych resortu obrony narodowej realizuje szereg osób. Należą do nich[157]:

- ***kierownik jednostki organizacyjnej***, który z mocy ustawy odpowiada za eksploatację i bezpieczeństwo systemów i sieci teleinformatycznych. Jest on zobowiązany do wyznaczenia;
  - / osoby lub zespołu osób odpowiedzialnych za funkcjonowanie systemu lub sieci teleinformatycznej oraz za przestrzeganie zasad i wymagań bezpieczeństwa, zwanych administratorem systemu[158],
  - / pracownika pionu ochrony, który pełni funkcję inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnego za bieżącą kontrolę zgodności funkcjonowania systemu lub sieci ze szczególnymi wymaganiami bezpieczeństwa,

  Obie wymienione osoby funkcyjne wchodzą w skład pionu ochrony w jednostce organizacyjnej i dlatego muszą spełniać wymagania stawiane

---

[157] Osoby funkcyjne i przypisane im zadania w dziedzinie bezpieczeństwa teleinformatycznego określone są w Decyzji Nr 181/MON Ministra Obrony Narodowej z dnia 6 października 2000 roku w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej.

[158] Zasady powoływania administratorów systemów i sieci teleinformatycznych w resorcie obrony narodowej określone są w Decyzji Nr 30/MON Ministra Obrony Narodowej z dnia 8 marca 2000 roku w sprawie powołania pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów i sieci teleinformatycznych oraz utworzenia pionów ochrony w jednostkach organizacyjnych resortu obrony narodowej.

pracownikom pionu ochrony takie jak posiadanie polskiego obywatelstwa, posiadanie poświadczenia bezpieczeństwa oraz odbycie przeszkolenia w zakresie ochrony informacji niejawnych. W odniesieniu do nich jednakże jest to wymóg przeszkolenia specjalistycznego przez Wojskowe Służby Informacyjne, w trakcie którego przekazywane są im informacje o stosunkowo wysokim stopniu specjalizacji.

- ***pełnomocnik ochrony***, odpowiadający za ochronę systemów i sieci teleinformatycznych, z wyłączeniem organizacyjnych, technicznych i programowych aspektów ochrony kryptograficznej. Do jego obowiązków należy między innymi;
  - / zapewnienie przestrzegania zasad ochrony informacji niejawnych przetwarzanych w systemie lub sieci a zwłaszcza właściwego obiegu dokumentów,
  - / dbałość o bezpieczeństwo fizyczne obszaru, w którym usytuowany jest system lub sieć *(strefa bezpieczeństwa i usytuowane w niej pomieszczenia)*,
  - / zapewnienie dostępu do systemu wyłącznie osobom upoważnionym, posiadającym poświadczenie bezpieczeństwa odpowiednie do wymaganego poziomu tajności przetwarzanych informacji,
  - / szkolenie i kontrola znajomości procedur bezpieczeństwa przez użytkowników systemu,
  - / nadzór nad konfiguracją systemu lub sieci, przemieszczaniem sprzętu i jego ewidencją,
  - / współudział w opracowywaniu programów organizacyjno – użytkowych, projektów technicznych budowanych systemów i sieci oraz szczególnych wymagań bezpieczeństwa,
  - / współdziałanie z Wojskowymi Służbami Informacyjnymi i właściwymi organami bezpieczeństwa systemów łączności i informatyki w sprawach bezpieczeństwa teleinformatycznego,

- ***administrator*** systemu lub sieci teleinformatycznej, odpowiadający między innymi za;
  - / codzienną obsługę techniczną i sprawdzanie poprawności działania urządzeń systemu lub sieci,
  - / opracowywanie projektów szczególnych wymagań bezpieczeństwa oraz ich uaktualnianie w trakcie eksploatacji systemu lub sieci,
  - / wdrażanie procedur bezpieczeństwa określonych w szczególnych wymaganiach bezpieczeństwa i nadzór nad funkcjonowaniem systemu lub sieci,
  - / wdrażanie procedur ochrony antywirusowej,
  - / opracowywanie planów awaryjnych i planu napraw systemu lub sieci,
  - / informowanie pełnomocnika ochrony oraz właściwego organu systemów łączności i informatyki o stwierdzonych naruszeniach bezpieczeństwa systemu lub sieci oraz o wykrytych wirusach a także występowanie z propozycjami zmian mających na celu poprawę bezpieczeństwa systemu lub sieci.

- ***organy bezpieczeństwa teleinformacyjnego:***

Centrum Analiz Kryptograficznych i Bezpieczeństwa Teleinformacyjnego, pozostające w strukturze Wojskowych Służb Informacyjnych, odpowiadające między innymi za;

- opracowywanie projektów dokumentów w sprawie ogólnych zasad bezpieczeństwa teleinformatycznego dla urządzeń, systemów i sieci,
- okresową *(1 raz na rok)* oraz doraźną ocenę stanu bezpieczeństwa systemów i sieci teleinformatycznych w resorcie obrony narodowej,
- badanie i ocenę urządzeń i narzędzi kryptograficznych oraz mechanizmów ich zabezpieczeń oraz systemów i sieci łączności

specjalnej, kodowej oraz utajnionej w ramach procesu certyfikacyjnego,[159]

- udział w opiniowaniu szczególnych wymagań bezpieczeństwa dla systemu lub sieci teleinformatycznej,
- generację i dystrybucję dokumentów kluczowych oraz haseł dostępu,
- odbiór, zarządzanie i dystrybucję urządzeń kryptograficznych, publikacji kryptograficznych i dokumentów kluczowych uzyskiwanych z wymiany międzynarodowej,
- szkolenie osób dokonujących odbioru technicznego urządzeń kryptograficznych,
- współpracę z Departamentem Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego, instytucją zajmującą analogiczną do Centrum Analiz Kryptograficznych i Bezpieczeństwa Teleinformacyjnego pozycję w służbie ochrony państwa, odpowiadającej za sferę cywilną.

Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki pozostające w strukturze Sztabu Generalnego WP, odpowiadające między innymi za;

- koordynację działalności organów bezpieczeństwa systemów łączności i informatyki rodzajów Sił Zbrojnych i Dowództwa Garnizonu Warszawa,
- planowanie, organizowanie, prognozowanie rozwoju, eksploatację i nadzór nad funkcjonowaniem systemów łączności specjalnej, kodowej i utajnionej oraz kryptograficznej ochrony systemów i sieci teleinformatycznych na potrzeby resortu obrony narodowej, ćwiczeń oraz Wojennego Systemu Dowodzenia,
- wprowadzanie, rozdział, ewidencję, wycofywanie oraz nadzór nad niszczeniem technicznych i programowych środków ochrony informacji,

[159] W celu certyfikacji urządzeń i narzędzi kryptograficznych w Centrum Analiz Kryptograficznych i Bezpieczeństwa Teleinformacyjnego funkcjonuje Laboratorium Bezpieczeństwa Teleinformatycznego.

- zarządzanie bezpieczeństwem, dystrybucję dokumentów szyfrowych, kodowych i kluczowych oraz ich ewidencję,
- kontrolowanie podległych organów bezpieczeństwa systemów łączności i informatyki w zakresie organizacji, funkcjonowania i eksploatacji systemów ochrony kryptograficznej, łączności szyfrowej, kodowej i utajnionej,
- wydawanie i prowadzenie ewidencji pozwoleń na eksploatację sprzętu łączności specjalnej i utajnionej,
- udział w opiniowaniu szczególnych wymagań dla systemów i sieci teleinformatycznych opracowywanych w resorcie obrony narodowej.

organy bezpieczeństwa systemów łączności i informatyki powoływane, w zależności od potrzeb na szczeblu jednostki organizacyjnej. Wykonują zadania przypisane dla Wojskowego Biura Łączności i Informatyki stosownie do zakresu kompetencji na swoim szczeblu organizacyjnym. Są one zobowiązane do współpracy z pełnomocnikami ochrony w celu zapewnienia kompleksowej ochrony informacji niejawnych przetwarzanych w systemach i sieciach teleinformatycznych w jednostce organizacyjnej.

- ***Wojskowe Służby Informacyjne*** właściwe do;
  - określania ogólnych zasad bezpieczeństwa teleinformatycznego w resorcie obrony narodowej,
  - potwierdzania przydatności algorytmów kryptograficznych[160], kluczy kryptograficznych[161], innych parametrów zabezpieczenia w tym haseł dostępu,
  - opiniowania i akceptowania szczególnych wymagań bezpieczeństwa dla systemów i sieci teleinformatycznych, w których przetwarzane są informacje niejawne stanowiące tajemnicę służbową,

---

[160] Algorytm kryptograficzny to metoda działania, przekształcająca dane w celu ukrycia lub ujawnienia ich zawartości informacyjnej.

[161] Klucz kryptograficzny to ciąg symboli, od którego w sposób istotny zależy wynik działania algorytmu kryptograficznego.

- opiniowania i zatwierdzania szczególnych wymagań bezpieczeństwa dla systemów i sieci teleinformatycznych, w których przetwarzane są informacje niejawne stanowiące tajemnicę państwową,
- prowadzenia czynności w ramach procesu certyfikacji i wydawania certyfikatów dla systemów i sieci teleinformatycznych,
- prowadzenia szkolenia specjalistycznego dla administratorów systemu lub sieci teleinformatycznej i inspektorów bezpieczeństwa teleinformatycznego,
- kontroli ochrony systemów i sieci oraz przestrzegania przepisów wydanych w tym zakresie.

System lub sieć teleinformatyczna przetwarzające informacje niejawne muszą być tak zaprojektowane, zorganizowane i eksploatowane, aby uniemożliwiały dostęp jednej osoby do wszystkich zasobów systemu lub sieci a zwłaszcza do urządzeń, danych i oprogramowania. Wymogi stawiane systemowi lub sieci muszą być szczegółowo opracowane w formie podstawowych dokumentów w dziedzinie bezpieczeństwa teleinformatycznego, jakimi są „Szczególne wymagania bezpieczeństwa"[162] i „Procedury bezpieczeństwa".[163] W związku z tym, że są to dokumenty wzajemnie się uzupełniające najczęściej stanowią jeden kompleksowy dokument. Zasady jego opracowywania zostały szczegółowo określone w „Metodyce opracowywania szczególnych wymagań bezpieczeństwa dla systemów i sieci teleinformatycznych", przygotowanej przez specjalistów Sztabu Generalnego Wojska Polskiego.[164] Celem ujednolicenia przygotowywanych dokumentów Metodyka jest wykorzystywana zarówno w jednostkach organizacyjnych Sił Zbrojnych jak również przez przedsiębiorców, jednostki naukowe i badawczo – rozwojowe, realizujących kontrakty niejawne lub wykonujących prace związane z bezpieczeństwem i obronnością państwa.

---

[162] Szczególne wymagania bezpieczeństwa systemu lub sieci teleinformatycznej to pełny i wszechstronny opis ich budowy, zasad działania i eksploatacji wraz z procedurami bezpieczeństwa, które obowiązkowo muszą być spełnione w czasie projektowania, budowy i działania tego systemu lub sieci.

[163] Procedury bezpieczeństwa to dokument zawierający zasady i sposób postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych oraz określają zakres odpowiedzialności użytkowników i pracowników mających dostęp do systemu lub sieci.

[164] Dokument niejawny, wprowadzony do użytku zarządzeniem Szefa Sztabu Generalnego z dnia 26.01.2000r. Jego postanowienia nie są omawiane w niniejszej pracy.

W szczególnych wymaganiach bezpieczeństwa muszą się znaleźć:

- ***charakterystyka systemu lub sieci*** określająca klauzulę tajności przetwarzanych informacji i kategorie uprawnień użytkowników w zakresie dostępu do nich;
- ***dane o budowie systemu lub sieci*** informujące o lokalizacji, typie wykorzystywanych urządzeń i oprogramowania, metodzie realizacji wewnętrznych i zewnętrznych połączeń, konfiguracji sprzętowej i środowisku w jakim będzie eksploatowany system lub sieć;
- ***określenie środków ochrony*** zapewniających bezpieczeństwo informacji niejawnych, przetwarzanych w systemie lub sieci przed możliwością narażenia ich bezpieczeństwa a zwłaszcza przed nieuprawnionym ujawnieniem. Muszą one wskazywać osoby odpowiedzialne za bezpieczeństwo systemu lub sieci, ustanawiać procedury bezpieczeństwa obowiązujące w trakcie eksploatacji i kontroli oraz określać wymagania w zakresie szkoleń dla administratora, inspektora i użytkowników systemu lub sieci;
- ***zadania*** administratora systemu lub sieci teleinformatycznej i inspektora bezpieczeństwa teleinformatycznego.

Szczególne wymagania bezpieczeństwa systemów lub sieci teleinformatycznych, przeznaczonych do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych stanowiących tajemnicę służbową przedstawiane są do akceptacji Wojskowym Służbom Informacyjnym. Nie wniesienie uwag do tych wymagań w terminie 30 dni od daty ich przedstawienia uprawnia do uruchomienia systemu lub sieci.

W przypadku, gdy szczególne wymagania bezpieczeństwa obejmują środki ochrony kryptograficznej, elektromagnetycznej, technicznej i organizacyjnej odpowiednie dla danego systemu lub sieci, w której mają być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne stanowiące tajemnicę państwową muszą one być zatwierdzone przez Wojskowe Służby Informacyjne w terminie 30 dni od dnia ich przekazania.

Pozytywna ocena szczególnych wymagań bezpieczeństwa upoważnia jedynie do uruchomienia systemu lub sieci przetwarzających informacje niejawne stanowiące tajemnicę służbową. W przypadku tajemnicy państwowej wymagany jest certyfikat wydany przez Wojskowe Służby Informacyjne. Certyfikat wydaje się na podstawie:

- badania i oceny zdolności systemu lub sieci teleinformatycznej do ochrony informacji niejawnych przed nieuprawnionym ujawnieniem oraz przed możliwością narażenia ich bezpieczeństwa;
- przeprowadzonych zgodnie z ustawą postępowań sprawdzających;
- zatwierdzonych przez Wojskowe Służby Informacyjne szczególnych wymagań bezpieczeństwa.[165]

W celu certyfikacji systemów i sieci teleinformatycznych w Wojskowych Służbach Informacyjnych powołana została Jednostka Certyfikująca Wyroby[166]. Celem jej działania jest:

- realizacja zadań, określonych dla Wojskowych Służb Informacyjnych jako służby ochrony państwa w ustawie o ochronie informacji niejawnych;
- certyfikacja wyrobów specjalnych służących do ochrony informacji niejawnych, które nie mogą być nabywane, na potrzeby resortu obrony narodowej, bez posiadania stosownego certyfikatu[167].

Do zadań Jednostki Certyfikującej Wyroby należy:

- wykonywanie czynności warunkujących wydanie certyfikatu typu i zgodności dla urządzenia lub narzędzia kryptograficznego, wchodzącego w skład systemu lub sieci teleinformatycznej, służącego do wytwarzania, przechowywania, przetwarzania lub przekazywania informacji

---

[165] Art. 62 Ustawy o ochronie informacji niejawnych.

[166] Decyzja Nr 100/MON Ministra Obrony Narodowej z dnia 6 czerwca 2000 roku w sprawie jednostki certyfikującej właściwej w Ministerstwie Obrony Narodowej do certyfikacji wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych.

[167] Wyroby te są wyszczególnione w Rozporządzeniu Ministra Obrony Narodowej z dnia 26 września 2001 roku w sprawie wyrobów, które nie mogą być nabywane bez certyfikatu, Dz. U. Nr 113, poz. 1213. Należą do nich: urządzenia *(i ich wyposażenie specjalne)* zobrazowania, przetwarzania, przechowywania i transmisji informacji niejawnej *(w zakresie bezpieczeństwa emisji)* w tym; kabiny ekranujące, indywidualne osłony ekranujące i przetworniki elektroakustyczne ekranowane.

niejawnych stanowiących tajemnicę państwową o klauzulach ŚCIŚLE TAJNE i TAJNE lub służbową o klauzuli POUFNE;

- organizowanie i prowadzenie badań warunkujących wydanie certyfikatu zgodności dla systemu lub sieci teleinformatycznej, służących do wytwarzania, przechowywania, przetwarzania lub przekazywania informacji niejawnych stanowiących tajemnicę państwową, w tym;
  / organizowanie oceny i zatwierdzanie szczególnych wymagań bezpieczeństwa systemu lub sieci teleinformatycznej,
  / organizowanie badań poziomów zabezpieczenia miejsca przewidywanej instalacji systemu lub sieci teleinformatycznej,
  / badanie i ocenę zdolności systemu lub sieci teleinformatycznych do ochrony informacji niejawnych przed nieuprawnionym ujawnieniem oraz przed możliwością narażenia ich bezpieczeństwa,
  / przeprowadzenie postępowania sprawdzającego,
- na podstawie wyników przeprowadzonych badań, ocen i postępowania sprawdzającego wydawanie;
  / certyfikatów typu[168] i zgodności[169] dla urządzeń lub narzędzi kryptograficznych wchodzących w skład systemu lub sieci teleinformatycznej, służących do wytwarzania, przechowywania, przetwarzania lub przekazywania informacji niejawnych stanowiących tajemnicę państwową i służbową o klauzuli POUFNE,
  / certyfikatów zgodności[170] dla systemów lub sieci teleinformatycznych, służących do wytwarzania, przechowywania,

---

[168] Certyfikat typu dla urządzenia jest to dokument gwarantujący, iż przedmiot oceny spełnia określone parametry techniczne oraz wymagania związane z zabezpieczeniem systemu lub sieci teleinformatycznej służących do przetwarzania informacji niejawnych. Uzyskanie certyfikatu typu uprawnia do umieszczenia przedmiotu oceny na liście produktów preferowanych i do ewentualnego stosowania w resorcie obrony narodowej, nie zobowiązuje jednak do jego zakupu i obligatoryjnego stosowania.

[169] Certyfikat zgodności dla urządzenia jest to dokument potwierdzający zgodność wykonania danego egzemplarza przedmiotu oceny z określonymi normami, wytycznymi lub dokumentami normatywnymi.

[170] Certyfikat zgodności dla systemu lub sieci teleinformatycznej to dokument wydany zgodnie z zasadami certyfikacji, wykazujący, że zapewniono odpowiedni stopień zaufania, iż należycie zidentyfikowany wyrób, proces lub usługa są zgodne z określoną normą lub z właściwymi przepisami prawnymi – zgodnie z Ustawą o badaniach i certyfikacji, Dz. U. z 1993 roku, Nr 55, poz. 250 z późniejszymi zmianami. Wzór certyfikatu dla systemu lub sieci teleinformatycznej znajduje się w Załączniku Nr 13.

przetwarzania lub przekazywania informacji niejawnych stanowiących tajemnicę państwową,

/ wykonywanie czynności związanych z certyfikacją i wydawanie certyfikatów dla innych wyrobów o przeznaczeniu specjalnym służących do ochrony informacji niejawnych.

W procesie certyfikacji wyrobów o przeznaczeniu specjalnym służących do ochrony informacji niejawnych Jednostka Certyfikująca Wyroby korzysta z uznanych przez nią laboratoriów badawczych. Aktualnie są to:

- Laboratorium Kompatybilności Elektromagnetycznej Wojskowego Instytutu Łączności *(zakres badań obejmuje między innymi komputery klasy TEMPEST, kabiny ekranujące, indywidualne osłony ekranujące)*;
- Laboratorium Bezpieczeństwa Teleinformatycznego Centrum Analiz Kryptograficznych i Bezpieczeństwa Teleinformacyjnego *(zakres badań obejmuje urządzenia i narzędzia kryptograficzne)*.

W procesie certyfikacji Jednostka Certyfikująca Wyroby może uznać, bez prowadzenia badań, certyfikat wydany przez inną jednostkę certyfikującą. Dotyczy to zwłaszcza certyfikatów wydawanych przez Jednostkę Certyfikującą Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego. Każdy tego typu przypadek jest rozpatrywany w trybie indywidualnym. Uznanie certyfikatu odbywać się może bezwarunkowo bądź na przykład po zapoznaniu się z raportem z badań, które były podstawą wydania certyfikatu przez Jednostkę Certyfikującą, funkcjonującą w ABW. Na takich samych zasadach może być uznany certyfikat dla urządzenia wydany przez jednostkę certyfikującą innej Krajowej Władzy Bezpieczeństwa państwa członkowskiego NATO.

Certyfikacja urządzeń i narzędzi kryptograficznych oraz systemów i sieci teleinformatycznych odbywa się na zasadach odpłatności.[171] Opłaty pobierane są za

[171] Stosownie do Rozporządzenia Prezesa Rady Ministrów z dnia 16 lipca 2001 roku w sprawie wysokości opłat za przeprowadzenie przez służbę ochrony państwa czynności warunkujących wydanie certyfikatu dla systemu lub sieci teleinformatycznej, urządzenia lub narzędzia kryptograficznego oraz za wydanie tych certyfikatów.

czynności poprzedzające wydanie certyfikatu oraz za jego wydanie.[172] W przypadku jednostek budżetowych, w tym funkcjonujących w resorcie obrony narodowej opłaty pobierane są jedynie za wydanie certyfikatu, nie muszą one płacić za czynności poprzedzające jego wydanie.

Pomimo tego, iż większość osób funkcyjnych resortu obrony narodowej zdaje sobie sprawę z wyjątkowej wagi wszystkich aspektów bezpieczeństwa teleinformatycznego dla właściwego funkcjonowania Sił Zbrojnych wydaje się, że wiele jest jeszcze w tej dziedzinie do zrobienia. Dotychczasowa praktyka realizacji zapisów ustawy i dokumentów normatywnych w sferze bezpieczeństwa informacji pozwala na postawienie tezy, iż nie wszystkie zalecenia są w pełni wykonane a do realizowanych przedsięwzięć Wojskowe Służby Informacyjne mają bardzo dużo zastrzeżeń. Co prawda administratorzy systemów oraz inspektorzy bezpieczeństwa teleinformatycznego zostali wyznaczeni w zdecydowanej większości jednostek organizacyjnych, w większości jednostek wyznaczono poziomy zabezpieczenia miejsca a dla systemów lub sieci opracowano szczególne wymagania proces certyfikacji nie został wszędzie zakończony.

Kierownicy jednostek organizacyjnych, często pomimo spełnienia ustawowych wymogów dotyczących bezpieczeństwa fizycznego nie zgłaszają do certyfikacji przygotowanych lub już funkcjonujących systemów czy sieci. Dzieje się tak pomimo faktu, iż wielu z nich zdaje sobie sprawę z odpowiedzialności za ewentualne ujawnienie informacji w funkcjonujących sieciach i systemach. Jak wspomniano na wstępie odpowiedzialność za bezpieczeństwo teleinformatyczne ponosi bowiem jednoosobowo kierownik jednostki organizacyjnej.

W sferze bezpieczeństwa teleinformatycznego istnieje szereg zagrożeń, na które powinny zwracać uwagę wszystkie osoby odpowiedzialne za ochronę informacji niejawnych przetwarzanych w systemach i sieciach teleinformatycznych. Należą do nich między innymi:

- wykorzystywanie systemów i sieci nie posiadających odpowiednich zabezpieczeń sprzętowych czy programowych;

---

[172] Wykaz i wysokość aktualnie pobieranych przez Jednostkę Certyfikującą Wyroby opłat za czynności związane z certyfikacją urządzeń, sieci i systemów teleinformatycznych oraz za wydanie certyfikatów znajduje się w Załączniku Nr 14.

- łączenie między sobą systemów jawnych i niejawnych bez zastosowania odpowiednich zabezpieczeń informacji lub narzędzi kryptograficznych;
- bezpośrednie łączenie komputerów pracujących w systemie lub sieci z ogólnodostępną siecią Internet;
- dokonywanie zmian w konfiguracji sprzętu i nieautoryzowane przemieszczanie elementów systemu lub sieci do innych pomieszczeń;
- brak lub wykorzystywanie nie aktualizowanego oprogramowania antywirusowego;
- nagminne wykorzystywanie przypadkowych, w tym nie rejestrowanych dyskietek do pracy w systemie lub sieci oraz do przenoszenia plików pomiędzy różnymi komputerami bez kontrolowania ich z wykorzystaniem licencjonowanego i aktualnego oprogramowania antywirusowego;
- oddawanie do naprawy sprzętu komputerowego wraz z nośnikami informacji bez wcześniejszego sprawdzenia i skasowania ich zawartości;
- serwisowanie sprzętu komputerowego przeznaczonego do przetwarzania informacji niejawnych, przez osoby nie posiadające poświadczeń bezpieczeństwa, odpowiednich do klauzuli tajności przetwarzanych w systemie lub sieci informacji niejawnych;
- stosowanie prostych haseł dostępu lub przechowywanie ich w miejscu umożliwiającym dostęp osób trzecich;
- niewłaściwe przechowywanie nośników informacji;
- instalowanie przez użytkowników przypadkowego, często nie licencjonowanego oprogramowania *(np. z płyt CD-ROM dołączanych do czasopism komputerowych lub oprogramowania „pirackiego" zakupionego na giełdach komputerowych lub wręcz skopiowanego z wykorzystaniem sieci Internet).*[173]

W nieco przewrotnej, jednak potwierdzonej doświadczeniem specjalistów ocenie, iż największym zagrożeniem dla informacji niejawnych wytwarzanych,

[173] Źródło – opracowanie własne, na podstawie doświadczeń nabytych w czasie sprawowania obowiązków kierownika Jednostki Certyfikującej Wyroby w Wojskowych Służbach Informacyjnych.

przetwarzanych, przechowywanych lub przesyłanych z wykorzystaniem systemów lub sieci teleinformatycznych stanowią ich użytkownicy jest dużo prawdy. Godnym podkreślenia jest też to, że użytkownicy powodują szereg zagrożeń nie poprzez celowe działanie lecz przede wszystkim przez brak kompetencji, znajomości podstawowych zasad bezpiecznej obsługi urządzeń wchodzących w skład sieci czy systemów teleinformatycznych czy też odpowiednich umiejętności.

6. Działalność szkoleniowa i kontrolna w sferze ochrony informacji niejawnych.

Przeszkolenie w zakresie ochrony informacji niejawnych jest obok uzyskania stosownego poświadczenia bezpieczeństwa osobowego warunkiem umożliwiającym pracę, pełnienie służby na określonym stanowisku lub wykonywanie prac zleconych, z którymi łączy się dostęp do informacji niejawnych. Za szkolenie odpowiadają Wojskowe Służby Informacyjne i pełnomocnicy ochrony. Celem szkolenia jest zapoznanie z:

- zagrożeniami ze strony obcych służb specjalnych działających przeciwko Rzeczypospolitej Polskiej i państwom sojuszniczym, a także z zagrożeniami ze strony organizacji terrorystycznych;
- przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności za ich ujawnienie;
- zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby;
- sposobami ochrony informacji niejawnych stanowiących tajemnicę państwową oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia;
- odpowiedzialnością karną, dyscyplinarną i służbową za naruszenie przepisów o ochronie informacji niejawnych.[174]

W resorcie obrony narodowej prowadzi się następujące szkolenia w zakresie ochrony informacji niejawnych[175]:

---

[174] Art. 54 ust. 1 Ustawy o ochronie informacji niejawnych.

- ***podstawowe,*** którym objęte są osoby, po uzyskaniu przez nie po raz pierwszy poświadczenia bezpieczeństwa (*w uzasadnionych przypadkach nawet przed wydaniem poświadczenia bezpieczeństwa)*, przed dopuszczeniem do pracy lub pełnienia służby na stanowisku, z którym łączy się dostęp do informacji niejawnych. Szkolenie tego typu organizuje pełnomocnik ochrony;
- ***uzupełniające,*** którym obejmuje się wszystkie osoby posiadające poświadczenia bezpieczeństwa. Celem jest doskonalenie i rozszerzenie zakresu wiedzy otrzymanej w czasie szkolenia podstawowego. Szkolenie tego typu organizuje pełnomocnik ochrony raz w roku lub częściej oraz w przypadku zmiany przepisów o ochronie informacji niejawnych. Program szkolenia zatwierdzany jest przez kierownika jednostki organizacyjnej;
- ***specjalistyczne,*** którym obejmuje się osoby przewidziane do objęcia stanowiska lub pełnienia funkcji:
  - / pełnomocnika ds. ochrony informacji niejawnych,
  - / kierownika i zastępcy kierownika kancelarii tajnej oraz zagranicznej,
  - / kancelisty kancelarii tajnej,
  - / pracownika pionu ochrony odpowiedzialnego za bieżącą kontrolę zgodności funkcjonowania systemów i sieci teleinformatycznych ze szczególnymi wymaganiami bezpieczeństwa,
  - / osoby odpowiedzialnej za nadzór, kontrolę, szkolenie i doradztwo w zakresie bezpieczeństwa przemysłowego.

Szkolenie specjalistyczne organizowane jest w wyznaczonych w resorcie obrony narodowej ośrodkach przez oficerów Wojskowych Służb Informacyjnych *(za wyjątkiem szkoleń dla personelu kancelarii tajnych i zagranicznych)* na podstawie opracowanego przez szefa Wojskowych Służb Informacyjnych programu szkolenia. Szkoleniem specjalistycznym mogą być również objęte odpłatnie osoby zatrudnione u przedsiębiorcy, w jednostce naukowej lub badawczo – rozwojowej,

---

[175] Szczegółowe zasady organizacji i prowadzenia szkolenia w zakresie informacji niejawnych w resorcie obrony narodowej określone są w Decyzji Nr 16/MON Ministra Obrony Narodowej z dnia 25 stycznia 2001 roku w sprawie szkolenia w zakresie ochrony informacji niejawnych.

starającej się o zawarcie umowy lub wykonującej umowę na rzecz resortu obrony narodowej, z wykonaniem której łączy się dostęp do informacji niejawnych.

Należy dodać, iż obowiązki Wojskowych Służb Informacyjnych w zakresie szkolenia wynikają z delegacji Ustawy o ochronie informacji niejawnych, określających konieczność szkolenia jako jedną z podstawowych powinności służby ochrony państwa.

Odbycie przeszkolenia jest dokumentowane wydanym osobie szkolonej zaświadczeniem o odbyciu przeszkolenia.[176]

Kontrola stanu ochrony informacji niejawnych oraz kontrola przestrzegania przepisów wydanych w tym zakresie to jedna z najważniejszych powinności Wojskowych Służb Informacyjnych[177]. Typowa kontrola obejmuje badanie:

- stanu zabezpieczenia informacji niejawnych w jednostce organizacyjnej;
- przestrzegania zasad ochrony informacji niejawnych przez osoby, które z tytułu wykonywanych obowiązków mają dostęp do informacji niejawnych;
- stanu zabezpieczenia sieci lub systemów teleinformatycznych służących do wytwarzania, przechowywania, przetwarzania lub przekazywania informacji niejawnych.

Kontrole prowadzone są na podstawie rocznego planu kontroli zatwierdzonego przez szefa Wojskowych Służb Informacyjnych. Z uwagi na fakt, iż w resorcie obrony narodowej prowadzone są kontrole w każdej dziedzinie działalności służbowej przy ich organizacji należy uwzględniać zarówno ogólne przepisy dotyczące działalności kontrolnej[178] jak i szczegółowe zasady dotyczące sprawowania nadzoru nad stanem ochrony informacji niejawnych w resorcie

---

[176] Wzory zaświadczeń wydawanych przez pełnomocnika i Wojskowe Służby Informacyjne zostały wprowadzone Rozporządzeniem ministra Spraw Wewnętrznych i Administracji z dnia 23 lutego 1999 roku w sprawie wzoru zaświadczenia stwierdzającego odbycie przeszkolenia w zakresie ochrony informacji niejawnych. Wzór zaświadczenia wydawanego przez Wojskowe Służby Informacyjne znajduje się w Załączniku Nr 15.

[177] Zasady prowadzenia kontroli przez służby ochrony państwa określone są w Rozporządzeniu Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie szczegółowego trybu prowadzenia przez służby ochrony państwa kontroli w zakresie ochrony informacji niejawnych stanowiących tajemnicę państwową, Dz. U. Z 1999 roku, Nr 18, poz. 160.

[178] Tryb prowadzenia kontroli w resorcie obrony narodowej reguluje Decyzja Nr 191/MON Ministra Obrony Narodowej z dnia 12 października 1999 roku w sprawie działalności kontrolnej w resorcie Obrony Narodowej, Dziennik. Rozkazów MON z 1999 roku, poz. 89.

Obrony Narodowej[179]. Ponadto kontrole planowane przez Wojskowe Służby Informacyjne muszą być uzgadniane z odpowiednimi komórkami organizacyjnymi resortu obrony narodowej, odpowiadającymi za całokształt działalności kontrolnej w Siłach Zbrojnych RP, na przykład z Departamentem Kontroli MON.

Celem kontroli jest sprawdzenie i ocena stanu przestrzegania przepisów o ochronie informacji niejawnych, ustalenie przyczyn ujawnionych naruszeń zasad ochrony informacji oraz sformułowanie wniosków i zaleceń w sprawie doskonalenia systemu ochrony informacji niejawnych. W zależności od rodzaju kontroli są one organizowane i prowadzone zarówno przez pełnomocnika i podległy mu pion ochrony jak i przez Wojskowe Służby Informacyjne.

W resorcie obrony narodowej prowadzone są następujące kontrole:

- ***bieżące*** – które mają na celu sprawowanie ciągłego nadzoru nad przestrzeganiem przepisów w zakresie ochrony informacji niejawnych. Prowadzone są przez bezpośrednich przełożonych wykonawców oraz przez pion ochrony;
- ***wyrywkowe*** – mające na celu sprawdzenie zgodności ze stanem ewidencyjnym informacji stanowiących tajemnicę państwową oraz pochodzących z wymiany międzynarodowej a także sprawdzenie przestrzegania przepisów dotyczących ewidencji i obiegu dokumentów. Kontrole wyrywkowe prowadzi pion ochrony na podstawie planu zatwierdzonego przez kierownika jednostki organizacyjnej;
- ***półroczne*** – których celem jest sprawdzenie zgodności ze stanem ewidencyjnym nośników informacji niejawnych posiadanych przez wykonawców, przestrzegania przepisów o ochronie informacji niejawnych w zakresie wytwarzania, ewidencji, przechowywania i niszczenia nośników informacji niejawnych oraz wykonania zaleceń pokontrolnych z wcześniej przeprowadzonych kontroli. Kontrole półroczne muszą być przeprowadzone do 30 czerwca każdego roku i udokumentowane w formie

[179] Decyzja Nr 182/MON Ministra Obrony Narodowej z dnia 8 marca 2000 roku w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej.

notatki przez przełożonych w stosunku do podległych bezpośrednio wykonawców;

- ***roczne*** - będące podstawową formą sprawdzenia realizacji zadań w zakresie ochrony informacji niejawnych przez jednostkę organizacyjną, prowadzone są przez komisję powołaną rozkazem *(decyzją)* kierownika jednostki organizacyjnej. Do końca lutego każdego roku kierownicy jednostek organizacyjnych są zobowiązani do przesłania meldunków o wynikach kontroli rocznej swym przełożonym. Meldunki zbiorcze o wynikach kontroli rocznych gromadzi szef Wojskowych Służb Informacyjnych. W terminie do 15 kwietnia następnego roku kalendarzowego meldunki te, przesyłają:
  - / osoby zajmujące kierownicze stanowiska w Ministerstwie Obrony Narodowej – za bezpośrednio podległe jednostki organizacyjne,
  - / pełnomocnik ministra obrony narodowej ds. ochrony informacji niejawnych - za Urząd Ministra Obrony Narodowej,
  - / dowódcy rodzajów Sił Zbrojnych i Dowódca Garnizonu Warszawa za podległe jednostki organizacyjne,
  - / kierownicy jednostek organizacyjnych bezpośrednio podległych ministrowi obrony narodowej,
  - / kierownicy komórek organizacyjnych Ministerstwa Obrony Narodowej – za podległe jednostki organizacyjne.
- ***problemowe*** – będące zasadniczą formą sprawdzenia stanu ochrony informacji niejawnych, do zarządzania i prowadzenia których uprawnieni są szef Wojskowych Służb Informacyjnych oraz Dyrektor Departamentu Kontroli a ponadto;
  - / Sekretarz Stanu – I Zastępca Ministra Obrony Narodowej, podsekretarze stanu, Dyrektor Generalny w podległych komórkach organizacyjnych oraz bezpośrednio podległych jednostkach organizacyjnych,
  - / Szef Sztabu Generalnego WP w podległych komórkach organizacyjnych oraz bezpośrednio podległych jednostkach

organizacyjnych a także jednostkach organizacyjnych podległych dowódcom rodzajów Sił Zbrojnych i dowódcy Garnizonu Warszawa,

/ kierownicy komórek organizacyjnych Ministerstwa Obrony Narodowej w bezpośrednio podległych jednostkach organizacyjnych.

W czasie kontroli problemowej zazwyczaj sprawdza się;

/ wykonanie zaleceń z wcześniej przeprowadzonych kontroli,

/ sposób realizacji zadań w zakresie ochrony informacji niejawnych,

/ działalność pionu ochrony, kancelarii tajnej i zagranicznej oraz ich filii,

/ postępowanie z informacjami niejawnymi w innych komórkach organizacyjnych, takich jak biblioteka, powielarnia i innych,

/ postępowanie wykonawców i wykonawców technicznych z informacjami niejawnymi i ich nośnikami,

/ ochronę informacji niejawnych w systemach i sieciach teleinformatycznych,

/ realizację zadań w zakresie ochrony fizycznej jednostki organizacyjnej w części związanej z ochroną informacji niejawnych.

Kontrolę problemową stanu ochrony informacji niejawnych w jednostce organizacyjnej przeprowadza się nie rzadziej niż na pięć lat.

Oprócz prowadzenia wyszczególnionych powyżej kontroli w sferze ochrony informacji niejawnych kierownicy jednostek organizacyjnych mają obowiązek opracowania co najmniej raz w roku ocenę stanu ochrony informacji niejawnych. Podstawę do opracowania tego dokumentu stanowią:

- wyniki kontroli stanu ochrony informacji niejawnych;
- meldunki o ujawnieniu informacji niejawnych osobom nieupoważnionym lub naruszeniu przepisów o ochronie informacji niejawnych;
- wystąpienia lub orzeczenia prokuratorów oraz sądów wojskowych;
- oceny stanu ochrony informacji nadesłane przez podległe jednostki organizacyjne;
- informacje uzyskane z Wojskowych Służb informacyjnych.

Ocena stanu ochrony informacji niejawnych zawiera:

- zagrożenia dla bezpieczeństwa informacji niejawnych ze strony obcych służb specjalnych, przestępczości zorganizowanej i terroryzmu;
- organizację systemu ochrony informacji niejawnych, w tym działalność pionu ochrony, wydawanie aktów normatywnych, sprawowanie nadzoru, działalność organizacyjną i szkoleniową;
- funkcjonowanie systemu ochrony informacji niejawnych, w tym przestrzeganie przepisów o ochronie informacji, ochronę informacji w systemach i sieciach teleinformatycznych, ochronę informacji pochodzących z wymiany zagranicznej

Zbiorczą ocenę stanu ochrony informacji niejawnych w danym roku kalendarzowym opracowują te same osoby funkcyjne, które zobowiązane są do opracowania meldunku o wynikach kontroli rocznej a następnie przesyłają tą ocenę szefowi Wojskowych Służb Informacyjnych do 15 maja następnego roku kalendarzowego. Natomiast szef Wojskowych Służb Informacyjnych opracowuje zbiorczą ocenę stanu ochrony informacji niejawnych w resorcie obrony narodowej w danym roku kalendarzowym i przedstawia ją ministrowi obrony narodowej w terminie do 15 czerwca następnego roku kalendarzowego.

Każdorazowo z wynikami kontroli zapoznawany jest organ nadrzędny kontrolowanej jednostki organizacyjnej. Kierownik jednostki organizacyjnej jest zobowiązany w terminie 30 dni do usunięcia wszelkich stwierdzonych przez zespół kontrolny usterek i poinformowania o tym fakcie szefa Wojskowych Służb Informacyjnych. Wykonanie zaleceń pokontrolnych jest sprawdzane przez Wojskowe Służby Informacyjne.

Stan ochrony informacji niejawnych w resorcie obrony narodowej jest zróżnicowany w różnych jednostkach organizacyjnych. Niemniej jednak wszystkie skontrolowane dotychczas jednostki spełniają minimalne standardy we wszystkich aspektach bezpieczeństwa informacji niejawnych. Największe problemy występują w zakresie bezpieczeństwa teleinformatycznego oraz bezpieczeństwa fizycznego. Przetwarzaniu dokumentów w systemach i sieciach komputerowych nie towarzyszy bowiem wymagany poziom wiedzy o zagrożeniach jakie powodować może nie przestrzegania przepisów i procedur określonych w Szczególnych Wymaganiach

Bezpieczeństwa i Procedurach Bezpieczeństwa. Brakuje też tak zwanej kultury wykonawczej, która powinna towarzyszyć zarówno wykonawcom dokumentów niejawnych jak i osobom, do których są one kierowane.

W dziedzinie bezpieczeństwa fizycznego istnieje wiele niedociągnięć, które nie zawsze są spowodowane brakiem troski kierowników jednostek organizacyjnych i pionów ochrony. Bardzo istotną kwestią jest tutaj brak środków finansowych, które są niezbędne, aby osoby funkcyjne mogły sprostać niezwykle wysokim standardom bezpieczeństwa fizycznego i zainstalować w jednostkach organizacyjnych elektroniczne systemy zabezpieczeń czy kontroli dostępu. W wielu instytucjach centralnych systemy takie funkcjonują i niewiele się różnią od tych, które można spotkać w Kwaterze Głównej NATO czy dowództwach Sojuszu. Jednakże jest jeszcze wiele jednostek wojskowych, w których na drzwiach pomieszczeń służbowych dominuje kapsel wypełniony plasteliną, zaznaczony odciskiem referentki.

ROZDZIAŁ III

POLITYKA BEZPIECZEŃSTWA ORGANIZACJI TRAKTATU PÓŁNOCNOATLANTYCKIEGO

1. Główne dokumenty normatywne. Podstawowe zasady oraz minimalne standardy bezpieczeństwa.

Nie ulega wątpliwości, iż efektywna współpraca, prowadzenie konsultacji, wspólne ćwiczenia wojskowe, szkolenie czy sojusznicze planowanie w NATO wymagają wymiany informacji, w tym opatrzonych klauzulą tajności pomiędzy państwami sojuszniczymi. Niezależnie od tego, iż każda ze stron posiada swoje narodowe systemy ochrony informacji niejawnych konieczne jest prowadzenie wspólnej polityki w tej dziedzinie oraz stworzenie mechanizmów, zaakceptowanych przez wszystkie państwa członkowskie i zobowiązujących je do przestrzegania minimalnych, jednakowych dla wszystkich standardów bezpieczeństwa i ochrony informacji.

Podstawą prawną ochrony informacji niejawnych w Sojuszu jest Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzona w Brukseli, 6 marca 1997 roku (*ang. Security Agreement between the parties to the North Atlantic Treaty for the security of information*).[180] Umowa ma charakter otwarty dla każdego nowego członka NATO i nie zabrania zawierania przez jej Strony innych umów, przedmiotem których jest wymiana informacji niejawnych.

Stosownie do postanowień Umowy Strony zostały zobowiązane do:

---

[180] Większość krajów członkowskich NATO ratyfikowała Umowę. Polski Parlament uczynił to w dniu 27 maja 1999 roku a jednolita treść Umowy ogłoszona została w Dz. U. Nr 64 z 2000 roku, poz. 740. Obecnie jeszcze w ośmiu krajach NATO *(Belgia, Islandia, Włochy, Luksemburg, Norwegia, Portugalia, Hiszpania, Stany Zjednoczone)* trwają procesy ratyfikacyjne.

- ochrony i zabezpieczenia informacji niejawnych[181], niezależnie od tego czy zostały wytworzone w NATO[182], przekazane przez kraj członkowski NATO lub innemu krajowi członkowskiemu;
- utrzymywania klauzuli tajności otrzymanej informacji niejawnej;
- nie wykorzystywania informacji niejawnych do celów innych niż te, które służą Organizacji Traktatu Północnoatlantyckiego;
- nie udostępniania otrzymanej informacji państwom nie należącym do NATO, tzw. Stronie trzeciej;
- ustanowienia Krajowej Władzy Bezpieczeństwa, której celem będzie wprowadzenie w życie standardów bezpieczeństwa i ochrony informacji niejawnych, obowiązujących wszystkie państwa członkowskie;
- wprowadzenia systemu postępowań sprawdzających wobec obywateli swych krajów, którzy wymagają lub mogą wymagać dostępu do informacji niejawnych oznaczonych klauzulą CONFIDENTIAL i wyższą. Celem postępowania musi być określenie czy osoba, która wymaga dostępu do informacji niejawnych spełnia ustanowione prawem kryteria, czy zasługuje na zaufanie i jest lojalna. Postępowania takie muszą być przeprowadzone przed objęciem obowiązków bądź zatrudnieniem osoby sprawdzanej;
- współpracy, na wniosek Krajowej Władzy Bezpieczeństwa innego państwa NATO w prowadzeniu postępowań sprawdzających.

Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, choć jest oddzielnym aktem prawnym, w celach praktycznych została

---

[181] Przez informacje niejawne NATO należy rozumieć informacje lub materiały, odnośnie których zdecydowano, że wymagają ochrony przed niepowołanym ujawnieniem i które oznaczane są klauzulą tajności. Informacje takie, w postaci dokumentu mogą być zarejestrowane w jakiejkolwiek formie czy postaci fizycznej *(rękopisy, druki, karty i taśmy perforowane, mapy, wykresy, fotografie, obrazy, rysunki, ryciny, szkice, notatki i dokumenty robocze, kalki lub taśmy maszynowe, reprodukcje, każda forma rejestracji dźwięku, głosu - magnetyczna, elektroniczna, optyczna, video oraz przy użyciu sprzętu teleinformatycznego ze stałą lub usuwalną pamięcią).*

[182] W celu określenia podmiotu Umowy NATO zostało określone jako Organizacja Traktatu Północnoatlantyckiego oraz organy zarządzane na mocy albo Porozumienia o statusie Organizacji Traktatu Północnoatlantyckiego, Przedstawicieli Narodowych i Sztabu Międzynarodowego *(ang. Agreement on the status of the North Atlantic Treaty Organisation,, National Representatives and International Staff)*, podpisanego w Ottawie w dniu 20 września 1951 roku albo Protokołu o statusie Międzynarodowego Dowództwa Wojskowego *(ang. Protocol on the status of International Military Headquarters),,* które

włączona do głównego dokumentu normatywnego NATO w sferze ochrony informacji niejawnych – Bezpieczeństwo w Organizacji Traktatu Północnoatlantyckiego (*ang. Security within the North Atlantic Treaty Organisation*).[183] Dokument ten, w postaci Memorandum Rady Północnoatlantyckiej *(ang. Council Memorandum - C-M)* jest okresowo uaktualniany. Jego ostatnia wersja została przygotowana przez ekspertów Krajowych Władz Bezpieczeństwa krajów członkowskich i Biura Bezpieczeństwa NATO i opublikowana w 2002 roku.

Memorandum precyzuje generalne założenia ochrony informacji niejawnych, zawarte w Umowie i jest niejako „natowską biblią" w sferze bezpieczeństwa i ochrony informacji niejawnych. Określa podstawowe zasady oraz minimalne standardy bezpieczeństwa, obowiązujące wszystkie państwa członkowskie, w celu zapewnienia jednolitego poziomu ochrony informacji niejawnych, wymienianych pomiędzy Stronami Paktu. Oczywistym jest, że istnieje ścisły związek pomiędzy sojuszniczymi standardami bezpieczeństwa i narodowymi systemami ochrony informacji niejawnych. Oba obszary muszą wzajemnie się przenikać, rozwiązania muszą być kompatybilne, organy bezpieczeństwa, narodowe i sojusznicze muszą ściśle współdziałać. Teza ta wielokrotnie przewija się w zapisach Memorandum, które zobowiązuje kraje NATO oraz cywilne i wojskowe organy Paktu do przestrzegania podstawowych zasad i minimalnych standardów ochrony informacji niejawnych oraz ustanowienia procedur niezbędnych dla ich implementacji. W rozumieniu instrukcji minimalne standardy stosuje się wobec:

- informacji niejawnych NATO;
- informacji niejawnych kraju członkowskiego, przekazywanych NATO lub innemu krajowi natowskiemu w ramach realizacji programu, projektu bądź kontraktu NATO;
- informacji niejawnych przekazanych NATO a pochodzących z kraju, który nie jest członkiem Paktu;

---

ustanowiono na mocy przepisów Traktatu Północnoatlantyckiego, podpisanego w dniu 28 sierpnia 1952 roku, w Paryżu.

[183] Memorandum Rady Północnoatlantyckiej Nr C-M(2002)49.

- informacji niejawnych powierzonych organizacjom i osobom spoza NATO, na przykład zakładom przemysłowym czy uczelniom.

Memorandum określa w szczególności zasady i standardy ochrony informacji niejawnych w sferze bezpieczeństwa osobowego, bezpieczeństwa fizycznego, bezpieczeństwa informacji, bezpieczeństwa teleinformatycznego i bezpieczeństwa przemysłowego.[184] Ponadto określa obowiązki organów bezpieczeństwa NATO i obowiązki władz bezpieczeństwa krajów członkowskich.[185]

W rozumieniu Memorandum filarami solidnego bezpieczeństwa narodowego każdego państwa członkowskiego NATO są:

- właściwa organizacja systemu bezpieczeństwa, zapewniającego gromadzenie informacji dotyczących szpiegostwa, terroryzmu, działalności sabotażowej oraz dostęp do tego typu informacji w czasie procedur sprawdzających wobec osób wymagających dostępu do informacji niejawnych;
- ciągła współpraca centralnych organów administracji rządowej, mająca na celu przestrzeganie zasad ochrony informacji niejawnych, stosownie do polityki bezpieczeństwa ustanowionej w NATO.

Do podstawowych zasad, które muszą być stosowane przez państwa członkowskie i organy NATO należą:

- zapewnienie stosowania uzgodnionych minimalnych standardów w celu utrzymywania jednolitego poziomu ochrony informacji niejawnych, wymienianych pomiędzy organami NATO i państwami członkowskimi;
- zasada potrzeby wiedzy *(ang. Need to know)* musi być jedyną podstawą udostępniania informacji niejawnych osobom, które zostały przeszkolone na temat procedur bezpieczeństwa i posiadają poświadczenie bezpieczeństwa, uprawniające do dostępu do informacji niejawnych o poziomie CONFIDENTIAL i wyższym;

---

[184] Zasady i standardy bezpieczeństwa scharakteryzowane są w Rozdziale III.3.
[185] Organy bezpieczeństwa Sojuszu scharakteryzowane są w Rozdziale III.2.

- zarządzanie ryzykiem ujawnienia informacji niejawnych musi być obowiązkowe w cywilnych i wojskowych organach NATO oraz fakultatywne w krajach członkowskich;
- ochrona informacji niejawnych musi być zapewniona poprzez stosowanie środków bezpieczeństwa osobowego, fizycznego, bezpieczeństwa informacji i INFOSEC[186], którymi muszą być objęte wszystkie osoby posiadające dostęp do informacji niejawnych;
- wszystkie przypadki ujawnienia informacji niejawnych muszą być zgłaszane właściwym władzom bezpieczeństwa a w przesyłanych meldunkach musi znaleźć się ocena szkody dla NATO, jaką spowodowało ujawnienie informacji;
- informacja niejawna musi podlegać kontroli wykonawcy;
- informacje niejawne NATO mogą być udostępniane jedynie tym krajom, nie należącym do NATO, które podpisały Umowę Bezpieczeństwa z NATO lub dostarczyły do NATO tak zwane Zapewnienie Bezpieczeństwa, gwarantujące, iż przekazane im informacje niejawne NATO będą należycie chronione.[187]

W związku z tym, iż Memorandum określa jedynie generalne zasady ochrony informacji niejawnych towarzyszy mu szereg dokumentów, szczegółowo określających procedury bezpieczeństwa w poszczególnych sferach, tzw. dokumentów wspomagających *(ang. supporting directives)*. Należą do nich:

- Dyrektywa w sprawie bezpieczeństwa osobowego *(ang. Directive on Personnel Security)*;[188]
- Dyrektywa w sprawie bezpieczeństwa fizycznego *(ang. Directive on Physical Security)*;[189]
- Dyrektywa w sprawie bezpieczeństwa informacji *(ang. Directive on Security of Information)*;[190]

---

[186] INFOSEC *(ang. Information Security)* jest pojęciem określającym stosowanie środków bezpieczeństwa, umożliwiających ochronę informacji niejawnych przetwarzanych, przechowywanych lub przesyłanych w systemach łączności, systemach informatycznych i innych systemach elektronicznych przed utratą ich poufności i integralności.
[187] C-M(2002)49, str.2-3.
[188] Według oznaczeń natowskich – AC/35-D/2000.
[189] AC/35-D/2001

- Dyrektywa w sprawie bezpieczeństwa przemysłowego *(ang. Directive on Industrial Security)*;[191]
- Dyrektywa w sprawie bezpieczeństwa teleinformatycznego *(ang. Primary Directive on INFOSEC)*;[192]

Dyrektywa w sprawie bezpieczeństwa osobowego określa szczegółowo zasady prowadzenia postępowań sprawdzających i upoważniania osób do dostępu do informacji niejawnych. W szczególności precyzuje:

- konieczność określenia kto w państwie członkowskim NATO jest odpowiedzialny za wydawanie poświadczeń bezpieczeństwa osobowego *(ang. Personnel Security Clearance)*;
- potrzebę określenia, jakie stanowiska wymagają dostępu do informacji niejawnych;
- kryteria ubiegania się osób o wydanie poświadczeń bezpieczeństwa osobowego;
- wymogi prowadzenia postępowania sprawdzającego, przyznawania, ponownego wydawania i cofania poświadczenia bezpieczeństwa;
- obowiązki w zakresie prowadzenia ewidencji wydanych poświadczeń bezpieczeństwa;
- obowiązek przeszkolenia osób posiadających dostęp do informacji niejawnych;
- zasady dostępu do informacji niejawnych przez osoby nie posiadające poświadczenia bezpieczeństwa w sytuacjach wyjątkowych oraz jednorazowego dostępu w uzasadnionych przypadkach;
- zasady wydawania poświadczeń bezpieczeństwa dla kurierów, strażników, osób nie posiadających obywatelstwa kraju natowskiego.

Dyrektywa w sprawie bezpieczeństwa fizycznego precyzuje wymagania fizycznej ochrony informacji niejawnych a w szczególności odnosi się do:

---

[190] AC/35-D/2002

[191] AC/35-D/2003

[192] AC/35-D/2004. W związku z tym, że jest to dokument o klauzuli RESTRICTED, jego postanowienia nie będą omawiane w niniejszej pracy. Dokument ten został zatwierdzony przez Komitet Bezpieczeństwa NATO i jest uzupełniany przez szereg innych, szczegółowych dokumentów z dziedziny bezpieczeństwa teleinformatycznego. Podstawowe standardy bezpieczeństwa NATO w tej sferze będą omówione w dalszej części pracy w oparciu o dokument C-M(2002)49.

- środków fizycznego zabezpieczenia informacji niejawnych;
- minimalnych standardów przechowywania informacji niejawnych;
- ochrony przed technicznymi środkami uzyskiwania informacji;
- bezpieczeństwa fizycznego systemów łączności i systemów teleinformatycznych.

Dyrektywa w sprawie bezpieczeństwa informacji określa zasady ochrony dokumentów niejawnych w trakcie całego ich „życiowego cyklu", od wytworzenia do zniszczenia. Reguluje zwłaszcza wymogi w sprawach:

- klasyfikowania i oznaczania dokumentów;
- kontroli i przechowywania dokumentów;
- powielania, tłumaczenia i wykonywania wyciągów z dokumentów;
- rozpowszechniania i przesyłania informacji;
- potwierdzania odbioru i ewidencjonowania informacji;
- usuwania i niszczenia;
- postępowania w wypadku naruszenia zasad bezpieczeństwa i ujawnienia informacji;
- udostępniania informacji niejawnych NATO państwom nie natowskim i organizacjom międzynarodowym.

Dyrektywa w sprawie bezpieczeństwa przemysłowego ustanawia procedury związane z realizacją niejawnych kontraktów natowskich. Określa zwłaszcza:

- zasady negocjowania i zlecania niejawnych kontraktów NATO;
- wymogi bezpieczeństwa, które muszą być zachowane w trakcie realizacji kontraktów niejawnych;
- procedury udostępniania wykonawcy informacji niejawnych NATO w czasie realizacji kontraktu;
- procedury udostępniania podwykonawcom, konsorcjom i spółkom z kapitałem zagranicznym informacji niejawnych NATO w czasie realizacji kontraktu;
- zasady wydawania świadectwa bezpieczeństwa przemysłowego;
- zasady wydawania poświadczeń bezpieczeństwa osobowego dla pracowników firmy;

- wymogi dotyczące transportu informacji niejawnych w związku z realizacją kontraktu niejawnego;
- procedury dotyczące wizyt międzynarodowych w trakcie negocjowania i realizacji kontraktu.

Oprócz wymienionych powyżej dokumentów informacje niejawne mogą być chronione na podstawie oddzielnych umów międzynarodowych[193], lub oddzielnych dokumentów[194]. W związku ze szczególnym charakterem informacji kryptograficznych, w odniesieniu do takich informacji wymagane są szczególne środki bezpieczeństwa, które często wykraczają poza te ustanowione w podstawowych dokumentach takich jak Bezpieczeństwo w Organizacji Traktatu Północnoatlantyckiego.

Ponadto, w agendach NATO opracowano szereg innych zarządzeń i dyrektyw, szczegółowych instrukcji, wykładni, przewodników, które dostosowują generalne zapisy do specyfiki struktur działających w ściśle określonych sferach czy obszarach odpowiedzialności.

Interesujące jest to, iż w NATO ustanowiono również zasady i mechanizmy udostępniania informacji jawnych.[195] Wynika to z generalnego założenia, iż nawet dokumenty jawne, ale jednak wytworzone w Sojuszu nie mogą być ogólnodostępne ani przekazywane mass mediom.

---

[193] Informacje ATOMAL, stanowiące tajemnice związane z bronią atomową chronione są na podstawie Umowy między Stronami Traktatu Północnoatlantyckiego współpracy w dziedzinie informacji atomowych *(ang. Agreement between the Parties to the North Atlantic Treaty for Cooperation regarding Atomic Information)* – C-M(64)39.

[194] Informacje Stanów Zjednoczonych o szczególnym znaczeniu, wymieniane z NATO, chronione są zgodnie z zasadami określonymi w dokumencie „Zasady i procedury postępowania z dokumentami Stanów Zjednoczonych – Oddzielnych Planów Operacyjnych w NATO" *(ang. Special Procedures for the Handling of United States Single Integrated Operational Plan (US-SIOP) Information within NATO)* – C-M(71)27.

[195] Postępowanie z informacjami jawnymi *NATO (ang. The management of non-classified NATO information)*, C-M(2002)60.

2. Charakterystyka organów bezpieczeństwa Sojuszu i zakresów ich odpowiedzialności.

Do organów bezpieczeństwa Sojuszu należą zarówno krajowe władze bezpieczeństwa państw członkowskich jak i powołane w NATO organy bezpieczeństwa.

Każdy kraj członkowski jest zobowiązany do ustanowienia:

- Krajowej Władzy Bezpieczeństwa *(ang. National Security Authority);*
- Wyznaczonej Władzy Bezpieczeństwa *(ang, Designated Security Authority);*

Do obowiązków Krajowej Władzy Bezpieczeństwa należą między innymi:

- organizacja systemu ochrony informacji niejawnych NATO w strukturach narodowych, wojskowych i cywilnych, funkcjonujących w kraju oraz poza granicami państwa;
- zapewnienie prowadzenia okresowych kontroli ochrony informacji niejawnych NATO we wszystkich narodowych, cywilnych i wojskowych strukturach[196];
- zapewnienie prowadzenia postępowań sprawdzających wobec osób, które są upoważnione do dostępu do informacji niejawnych oznaczonych klauzulą CONFIDENTIAL i wyższą;
- zapewnienie opracowania planów uniemożliwiających dostęp do informacji niejawnych przez osoby nieupoważnione;
- autoryzacja organizacji centralnych kancelarii uprawnionych do przechowywania informacji o klauzuli COSMIC TOP SECRET.[197]

Do obowiązków Wyznaczonej Władzy Bezpieczeństwa należy ustanowienie narodowej polityki w zakresie bezpieczeństwa przemysłowego. W każdym państwie może być ustanowionych kilka bądź jedna Wyznaczona Władza Bezpieczeństwa. Jednak zawsze podlegają one Krajowej Władzy Bezpieczeństwa,

---

[196] W przypadku przechowywania informacji COSMIC TOP SECRET i ATOMAL inspekcje muszą być prowadzone co 18 miesięcy, chyba że w tym czasie inspekcja prowadzona była przez organ bezpieczeństwa NATO – Biuro Bezpieczeństwa.

[197] Utworzenie kancelarii przechowującej informacje niejawne o klauzuli COSMIC TOP SECRET musi być zgłoszone do Biura Bezpieczeństwa NATO.

sprawującej nadzór nad całokształtem spraw ochrony informacji niejawnych w danym państwie. Możliwym jest również wykonywanie zadań przypisanych Wyznaczonej Władzy Bezpieczeństwa przez Krajową Władzę Bezpieczeństwa.[198]

W NATO sprawami bezpieczeństwa i ochrony informacji niejawnych zajmują się:

- Komitet Bezpieczeństwa NATO *(ang. NATO Security Committee);*
- Biuro Bezpieczeństwa NATO *(ang. NATO Office of Security).*

Komitet Bezpieczeństwa NATO jest powoływany przez Radę Północnoatlantycką[199] i przed Radą rozlicza się ze swej działalności. W jego skład wchodzą przedstawiciele państw członkowskich, posiadający doświadczenie w sprawach bezpieczeństwa i ochrony informacji niejawnych w swych krajach. Zwykle są to szefowie bądź osoby sprawujące kierownicze funkcje w krajowych władzach bezpieczeństwa. Poza nimi w pracach Komitetu mogą brać udział przedstawiciele Komitetu Wojskowego NATO *(ang. NATO Military Committee)* oraz cywilnych i wojskowych organów Sojuszu, zwłaszcza wówczas, gdy omawiane są sprawy bezpośrednio dotyczące ich struktur. Z reguły Komitet spotyka się dwa razy do roku a do jego głównych zadań należą:

- rozpatrywanie wszelkich spraw związanych z bezpieczeństwem i ochroną informacji niejawnych NATO;
- rozpatrywanie spraw, związanych z bezpieczeństwem i ochroną informacji niejawnych, kierowanych przez Radę Północnoatlantycką, kraje członkowskie, Sekretarza Generalnego NATO, Komitet Wojskowy oraz szefów cywilnych i wojskowych organów Sojuszu;
- opracowywanie wytycznych, instrukcji i zaleceń w sferze bezpieczeństwa i przedstawianie ich do akceptacji Radzie Północnoatlantyckiej.

Biuro Bezpieczeństwa NATO jest organem działającym w strukturze Sztabu Międzynarodowego Kwatery Głównej NATO w Brukseli. Na jego czele stoi Dyrektor, sprawujący jednocześnie funkcję Przewodniczącego Komitetu

---

[198] Wykaz władz bezpieczeństwa powołanych w każdym kraju członkowskim NATO jest przekazywany, włącznie z adresami i kontaktami telefonicznymi do Biura Bezpieczeństwa NATO.

[199] Radę Północnoatlantycką stanowią ambasadorowie – stali przedstawiciele państw członkowskich przy Organizacji Traktatu Północnoatlantyckiego.

Bezpieczeństwa. Natomiast pracownicy Biura zapewniają obsługę i właściwą organizację pracy Komitetu. Personel Biura stanowią osoby posiadające doświadczenie w sprawach bezpieczeństwa zarówno w sferze wojskowej jak i cywilnej. Biuro utrzymuje ścisły kontakt z krajowymi władzami bezpieczeństwa państw członkowskich. Przykładem takiej współpracy może być powoływanie narodowych ekspertów, wykonujących konkretne zadania w strukturach Biura w określonym czasie.

Do głównych zadań Biura Bezpieczeństwa NATO należą między innymi:

- analiza wszelkich spraw, mających wpływ na bezpieczeństwo NATO oraz wprowadzanie zmian, wpływających na poprawę jego stanu;
- współpraca i koordynacja wszelkich spraw związanych z bezpieczeństwem i ochroną informacji NATO w państwach członkowskich
- zapewnienie implementacji decyzji w sprawach bezpieczeństwa, jakie przyjmowane są w NATO i obowiązują wszystkie państwa członkowskie oraz cywilne i wojskowe organy Sojuszu;
- informowanie Komitetu Bezpieczeństwa, Sekretarza Generalnego, oraz Przewodniczącego Komitetu Wojskowego o stanie bezpieczeństwa w NATO oraz wdrażaniu w życie decyzji Rady Północnoatlantyckiej;
- prowadzenie okresowych ocen ochrony informacji niejawnych NATO w krajach członkowskich, cywilnych i wojskowych organach Sojuszu oraz w dowództwach Paktu;
- prowadzenie dochodzeń, w porozumieniu z krajowymi władzami bezpieczeństwa oraz cywilnymi i wojskowymi organami Sojuszu, w sprawach ujawnienia informacji niejawnych NATO;
- przekazywanie krajowym władzom bezpieczeństwa wszelkich, informacji o ich obywatelach, które mają wpływ na rękojmię zachowania przez nich tajemnicy;
- opracowanie oraz wdrażanie w życie koncepcji ochrony Kwatery Głównej NATO w Brukseli;

- nadzór nad ochroną informacji ATOMAL stosownie do postanowień Umowy w tej sprawie.

Poza Komitetem Bezpieczeństwa i Biurem Bezpieczeństwa NATO za sprawy związane z ochroną informacji niejawnych odpowiadają szefowie wojskowych i cywilnych struktur Paktu. Są oni odpowiedzialni przed Radą Północnoatlantycką za bezpieczeństwo podległych im dowództw i obiektów, za ustanowienie struktur zajmujących się na bieżąco sprawami bezpieczeństwa oraz bezpośrednio za wdrażanie w życie instrukcji, programów i zaleceń, opracowanych przez Biuro Bezpieczeństwa i Komitet Bezpieczeństwa NATO oraz zaakceptowanych przez Radę Północnoatlantycką.

Tak zorganizowany system organów bezpieczeństwa w NATO jest czytelny i jasno rozgranicza ramy odpowiedzialności organów narodowych i wspólnych dla całego Paktu. Jednocześnie zapewnia konieczność stałej współpracy i wzajemnego informowania się o zjawiskach i wydarzeniach, które mogą negatywnie rzutować na bezpieczeństwo i ochronę informacji niejawnych.

3. Analiza wybranych aspektów bezpieczeństwa osobowego, fizycznego, informacji, przemysłowego i teleinformatycznego.

Bezpieczeństwo osobowe jest pojęciem używanym w NATO dla określenia zasad prowadzenia postępowań sprawdzających wobec osób, wymagających dostępu do informacji niejawnych. Każdy kraj natowski oraz każdy cywilny lub wojskowy organ NATO zobowiązane są do określenia, w swoich wewnętrznych strukturach, jakie stanowiska wymagają dostępu do informacji niejawnych. Osoby, które mają być wyznaczone na te stanowiska muszą być sprawdzone, objęte procedura postępowania sprawdzającego przed wydaniem stosownego poświadczenia. Celem tych procedur jest ocena czy osoba sprawdzana daje rękojmie zachowania tajemnicy. Do generalnych zasad w dziedzinie bezpieczeństwa osobowego należą:

- konieczność prowadzenia postępowań wobec osób wymagających dostępu do informacji o klauzuli CONFIDENTIAL lub wyższej,

- obowiązek przeszkolenia każdej osoby w zakresie ochrony powierzanych jej informacji przed upoważnieniem do dostępu do informacji niejawnych;
- potrzeba zapoznania z zakresem obowiązków na zajmowanym stanowisku służbowym oraz pisemnego potwierdzenia znajomości wymogów związanych z ochroną informacji niejawnych;
- obowiązek ciągłej oceny przez uprawnione władze bezpieczeństwa oraz przełożonych rękojmi zachowania tajemnicy przez osoby posiadające poświadczenie bezpieczeństwa.[200]

Za bezpieczeństwo osobowe odpowiedzialne są krajowe władze bezpieczeństwa, zobowiązane do:

- prowadzenia postępowań sprawdzających wobec osób ubiegających się o dostęp do informacji niejawnych, zarówno narodowych jak i natowskich, o klauzuli CONFIDENTIAL i wyższej oraz wydawania, odmawiania, przedłużania i cofania stosownych poświadczeń bezpieczeństwa;
- zagwarantowania, że postępowania sprawdzające prowadzone są za zgodą i wiedzą osoby sprawdzanej;
- współdziałania z innymi krajowymi władzami bezpieczeństwa w zakresie wymiany informacji o osobach oraz posiadanych przez nie poświadczeniach bezpieczeństwa.[201]

W toku postępowania sprawdzającego upoważnieni funkcjonariusze Krajowej Władzy Bezpieczeństwa muszą dokonać oceny lojalności osoby sprawdzanej. Dopuszczalne jest, o ile jest to zgodne z narodowym ustawodawstwem, sprawdzenie informacji dotyczących nie tylko osoby sprawdzanej, ale również małżonka, osoby wspólnie zamieszkującej lub członka bliskiej rodziny. Zwłaszcza istotne są dane czy osoba sprawdzana:

- popełniła przestępstwo szpiegostwa, sabotażu, terroryzmu, zdrady lub działalności wywrotowej;

---

[200] Załącznik „C" Bezpieczeństwo osobowe *(ang. Enclosure „C" Personnel Security)* do C-M(2002)49, str. 1.

[201] AC/35-D/2000, str. 3.

- współpracowała lub udzielała pomocy szpiegom, terrorystom, sabotażystom lub osobom, wobec których istnieją uzasadnione podejrzenia, iż pracują dla obcych służb specjalnych;
- była członkiem lub zwolennikiem organizacji, która przy pomocy działalności wywrotowej dąży do obalenia rządów krajów członkowskich;
- zataiła istotne dane, ważne dla bezpieczeństwa państwa lub świadomie skłamała wypełniając ankietę bezpieczeństwa lub w czasie rozmowy z prowadzącym postępowanie sprawdzające;
- była skazana za przestępstwo kryminalne, ma trudności finansowe lub majątek niewiadomego pochodzenia, jest uzależniona od alkoholu, ma skłonności do dewiacji seksualnych;
- może być podatna na szantaż, okazała się nielojalna, niewiarygodna, niedyskretna, naruszała przepisy bezpieczeństwa i zasady ochrony informacji niejawnych;
- cierpiała na zaburzenia psychiczne lub miała zaburzenia emocjonalne;
- może być podatna na presję wywierana przez krewnych, bliskich lub znajomych, którzy mogli ulec oddziaływaniu obcych służb specjalnych.

Weryfikacji wyszczególnionych danych dokonuje się poprzez analizę informacji o sprawdzanej osobie za okres ostatnich 5 lat albo od chwili ukończenia 18 lat do momentu rozpoczęcia procedury sprawdzającej. Wymogi te dotyczą postępowań przed uprawnieniem do dostępu do informacji o poziomie CONFIDENTIAL i SECRET, które muszą obejmować następujące czynności:

- wypełnienie ankiety bezpieczeństwa osobowego[202];
- sprawdzenie tożsamości, obywatelstwa, narodowości;
- sprawdzenie w kartotekach operacyjnych organów bezpieczeństwa, policji, w rejestrze skazanych, w rejestrach lokalnych agencji ds.

[202] Dokument C-M(2002)49 nie wprowadza wzoru ankiety bezpieczeństwa osobowego. W Załączniku Nr 16 znajduje się ankieta wykorzystywana przez Biuro Bezpieczeństwa NATO w trakcie postępowania sprawdzającego wobec osób zatrudnianych w cywilnych organach Paktu, pozostających w kompetencji Biura. Wzory dokumentów natowskich przytaczane są w oryginalnej wersji językowej.

przestrzegania prawa gdzie osoba sprawdzana była zatrudniona przez przynajmniej sześć miesięcy.

Postępowanie sprawdzające przed wydaniem poświadczenia bezpieczeństwa, uprawniającego do dostępu do informacji COSMIC TOP SECRET musi być oparte na sprawdzeniach, obejmujących okres przynajmniej 10 lat albo od chwili ukończenia 18 lat do momentu rozpoczęcia procedury sprawdzającej. Dodatkowo, poza czynnościami wyszczególnionymi powyżej wymagane jest ustalenie:

- statusu majątkowego, pod kątem możliwej podatności osoby sprawdzanej na szantaż, co może wynikać z trudności finansowych lub w celu oceny czy osoba sprawdzana posiada status materialny adekwatny do osiąganych dochodów;
- posiadanego wykształcenia, uczęszczania do szkół od 18 roku życia bądź w ciągu ostatnich 10 lat;
- miejsca zatrudnienia, zarówno aktualnego jak i w latach poprzednich;
- stosunku do służby wojskowej;

Obowiązkowym jest również przeprowadzenie rozmowy z osobą sprawdzaną. Zasada ta ma zastosowanie zwłaszcza wtedy, gdy uzyskiwane w toku sprawdzenia informacje świadczą na jej niekorzyść. Oprócz tego rozmowy muszą być przeprowadzone z osobami, które na tyle znają osobę sprawdzaną, że mogą przekazać informacje o niej i ocenić czy jest godną zaufania.

Krajowa Władza Bezpieczeństwa jest zobowiązana do przejawienia największej staranności w toku prowadzonego postępowania. Wszystkie informacje muszą być ocenione pod kątem generalnej oceny osoby sprawdzanej. Nawet niekorzystne informacje o osobie sprawdzanej lub członkach jej rodziny nie muszą automatycznie wykluczać przyznania jej poświadczenia bezpieczeństwa. W takim przypadku musi być dokonana ocena jak te informacje mogą wpłynąć na rękojmię zachowania tajemnicy oraz lojalność osoby sprawdzanej.

W rezultacie przeprowadzonego postępowania Krajowa Władza Bezpieczeństwa wydaje PERSONNEL SECURITY CLEARANCE

CERTIFICATE[203]. W przypadku zatrudnienia bądź desygnowania osoby posiadającej poświadczenie bezpieczeństwa do pracy lub służby w cywilnym lub wojskowym organie NATO, Krajowa Władza Bezpieczeństwa zobowiązana jest do dostarczenia wydanego poświadczenia do organu zatrudniającego ta osobę. Jest to bezwzględny warunek zatrudnienia w strukturze NATO. Jeśli w ciągu 12 miesięcy osoba ta nie podejmie pracy bądź nie rozpocznie służby w cywilnym lub wojskowym organie NATO lub przerwie pracę lub służbę na okres 12 miesięcy wymagane jest potwierdzenie przez właściwą Krajową Władze Bezpieczeństwa ważności posiadanego przez nią poświadczenia bezpieczeństwa.

Na potrzeby organizowanych w cywilnych i wojskowych organach NATO oraz w państwach członkowskich spotkań, seminariów i konferencji Krajowa Władza Bezpieczeństwa jest zobowiązana do wydania zaświadczenia *(ang. Certificate of Security Clearance)*, stwierdzającego, iż uczestnik posiada ważne poświadczenie bezpieczeństwa[204].

Wznowienie poświadczenia bezpieczeństwa następuje po 5 latach dla informacji COSMIC TOP SECRET i 10 latach dla informacji CONFIDENTIAL i SECRET w wyniku przeprowadzonego postępowania sprawdzającego, obejmującego okres od poprzednio prowadzonego sprawdzenia. Kolejne postępowanie przed wydaniem poświadczenia do poziomu CONFIDENTIAL i SECRET obejmować musi następujące czynności:

- wypełnienie kwestionariusza bezpieczeństwa osobowego lub uzupełniającej ankiety do poprzednio wypełnionego kwestionariusza;
- dla osób zatrudnionych bądź pełniących służbę w NATO – sprawdzenie rejestrów personalnych i bezpieczeństwa znajdujących się w tych organach oraz sprawdzenia, na wniosek macierzystej Krajowej Władzy Bezpieczeństwa w rejestrach kraju, w którym właściwy cywilny bądź wojskowy organ NATO się znajduje;

---

[203] Wzór NATO PERSONNEL SECURITY CLEARANCE CERTIFICATE, określony w AC/35-D/2000, znajduje się w Załączniku Nr 17.

[204] Wzór CERTIFICATE OF SECURITY CLEARANCE, określony w AC/35-D/2000, znajduje się w Załączniku Nr 18.

Kolejne postępowanie sprawdzające przed wydaniem poświadczenia bezpieczeństwa do poziomu COSMIC TOP SECRET poza procedurami wymienionymi powyżej może obejmować:

- przeprowadzenie rozmowy z dwiema osobami, które są w stanie bezstronnie ocenić przeszłość i lojalność osoby sprawdzanej;
- szczegółowe sprawdzenia w rejestrach kraju macierzystego, kraju w którym funkcjonuje cywilny lub wojskowy organ NATO oraz na wniosek Krajowej Władzy Bezpieczeństwa – w kraju, w którym przebywała osoba sprawdzana.

Wydanie poświadczenia bezpieczeństwa nie może być granicą, za którą kończy się zainteresowanie Krajowej Władzy Bezpieczeństwa osobą sprawdzaną. Każdy kraj członkowski zobowiązany jest do prowadzenia centralnej ewidencji wydanych poświadczeń bezpieczeństwa jak również musi ustanowić procedury, które pozwalają wycofać wydane poświadczenie, gdy ujawnione zostaną informacje świadczące o tym, że posiadacz poświadczenia nie daje gwarancji zachowania tajemnicy i stanowi tym samym zagrożenie dla bezpieczeństwa informacji.

W związku z tym, iż życie przynosi wiele niespodziewanych, nieprzewidywalnych sytuacji polityka bezpieczeństwa NATO upoważnia kraje członkowskie do ustanowienia procedur umożliwiających dostęp do informacji niejawnych osobom nie posiadającym poświadczenia bezpieczeństwa w sytuacjach:

- wstępnego wyznaczenia na stanowisko, wymagającego dostępu do informacji o poziomie wyższym niż posiadane poświadczenie bezpieczeństwa. Wyznaczenie na stanowisko może mieć miejsce pod warunkiem posiadania aktualnego poświadczenia o poziomie niższym oraz dokonania niezbędnych sprawdzeń, które nie są niekorzystne dla danej osoby. Wstępne zatrudnienie nie może przekraczać 6 miesięcy od terminu objęcia stanowiska. Właściwa Krajowa Władza Bezpieczeństwa może przedłużyć ten okres o kolejnych 6 miesięcy pod warunkiem, iż stosowne postępowanie sprawdzające zostało już wdrożone;
- jednorazowego dostępu do informacji wyższej niż posiadane poświadczenie bezpieczeństwa. Dostęp tego typu, związany z realizacją

zadań służbowych, musi być uzasadniony pisemnie przez przełożonego, zaewidencjonowany w prowadzonym przez właściwe władze bezpieczeństwa rejestrze i autoryzowany przez właściwą osobę funkcyjną[205]. Procedura ta nie może być stosowana powtórnie. Jeśli wymagany jest dostęp do informacji przez okres dłuższy niż 6 miesięcy obowiązkowym jest uzyskanie stosownego poświadczenia bezpieczeństwa osobowego;

- dostępu w sytuacjach wyjątkowych, takich jak wojna, nasilające się napięcie międzynarodowe, w czasie ćwiczeń połączonych z mobilizacją. Szefowie cywilnych lub wojskowych organów NATO mogą upoważnić do dostępu do informacji niejawnych osoby nie posiadające odpowiedniego poświadczenia, jeśli nie ma uzasadnionych wątpliwości, co do ich lojalności i wiarygodności. W odniesieniu do informacji COSMIC TOP SECRET dostęp tego typu należy ograniczyć do osób posiadających poświadczenie narodowe do poziomu ŚCIŚLE TAJNE lub TAJNE. Rejestr udzielonych upoważnień w tym trybie z opisem sytuacji, w jakich ich udzielono musi być prowadzony przez właściwe władze bezpieczeństwa,[206]

Bezpieczeństwo fizyczne – jest pojęciem, używanym w NATO dla określenia środków bezpieczeństwa, jakie są stosowane w celu fizycznej ochrony informacji niejawnych. Zgodnie z polityką bezpieczeństwa NATO wszystkie budynki, obiekty, biura i pomieszczenia, w których są przechowywane bądź przetwarzane informacje niejawne muszą być odpowiednio chronione. Przy doborze środków bezpieczeństwa fizycznego należy brać pod uwagę:

- klauzule tajności, ilość i formę przechowywanych dokumentów niejawnych;

---

[205] W NATO jest to osoba zajmująca stanowisko OF-6, które jest przewidziane dla oficera w stopniu „jednogwiazdkowego generała".

[206] AC/35-D/2000, str. 11-12.

- wymagania wobec personelu – posiadania adekwatnych do klauzuli tajności przechowywanych dokumentów, poświadczeń bezpieczeństwa oraz stosowanie zasady potrzeby wiedzy;
- ocenę zagrożeń ze strony obcych służb wywiadowczych, terroryzmu, działalności kryminalnej i antypaństwowej;
- sposób przechowywania informacji.

Środki bezpieczeństwa fizycznego powinny zapewniać uniemożliwienie wtargnięcia osoby nieuprawnionej w sposób skryty bądź z użyciem siły, zniechęcenie do podejmowanie działań przez nielojalny personel oraz jak najszybsze wykrywanie przypadków naruszenia zasad bezpieczeństwa w miejscu przechowywania informacji niejawnych. Aby osiągnąć zamierzony cel, planowanie zastosowania odpowiednich środków bezpieczeństwa fizycznego powinno mieć miejsce już na etapie projektowania obiektu i jego budowy. Generalną zasadą przy planowaniu zastosowania środków ochrony fizycznej jest zasada „ obrony w głąb"[207], polegająca na właściwym oznakowaniu oraz stosowaniu coraz bardziej skomplikowanych środków ochrony w miarę zmniejszania się odległości do najbardziej strzeżonej strefy, w której przechowywane są informacje o najwyższej klauzuli tajności.

Zgodnie z normami natowskimi informacje niejawne, o klauzuli CONFIDENTIAL i wyższej, muszą być przechowywane w strefach bezpieczeństwa. Rozróżniane są: strefa bezpieczeństwa klasy I, oznaczająca obszar, wejście do którego oznacza w praktyce dostęp do informacji niejawnych,[208] strefa bezpieczeństwa klasy II, oznaczająca obszar, w którym wewnętrzne środki ochrony uniemożliwiają bezpośredni dostęp do informacji niejawnych.[209] Zasadą jest, iż wokół stref bezpieczeństwa tworzy się strefy administracyjne, w których możliwe jest przechowywanie informacji o klauzuli RESTRICTED. Wymagają one oznaczenia granic, w ich obszarze możliwa jest kontrola osób i pojazdów.

---

[207] AC/35-D/2001, str. 2.

[208] Strefa I wymaga wyraźnie oznaczonych granic, przekraczanie których jest kontrolowane, systemu kontroli wejść umożliwiającego wejście osobom sprawdzonym, posiadającym stosowne zezwolenie. Wewnątrz musi znajdować się spis klauzul tajności i kategorii przechowywanych informacji niejawnych.

[209] Strefa II wymaga wyraźnie oznaczonych granic, przekraczanie których jest kontrolowane. Wejście do strefy mają jedynie osoby sprawdzone, posiadające stosowne zezwolenie. Inne osoby, w czasie przebywania w strefie, musza być eskortowane.

Do środków bezpieczeństwa fizycznego mogą należeć:

- ogrodzenie, chroniące granice obszaru;
- oświetlenie ochronne, umożliwiające prowadzenie skutecznej obserwacji tak przez strażników jak i przy użyciu środków technicznych;
- systemy wykrywania ruchu *(ang. Intrusion Detection System - IDS)*, instalowane na granicach obszaru. Mogą być one instalowane w sposób ukryty bądź też być widoczne dla osiągnięcia efektu odstraszania[210];
- kontrola osób wchodzących i wychodzących w odniesieniu do obszarów i pomieszczeń z możliwością prowadzenia wyrywkowych przeszukań;
- strażnicy, którzy przed zatrudnieniem muszą być odpowiednio sprawdzeni, jeśli jest to wymagane posiadać poświadczenie bezpieczeństwa, muszą być przeszkoleni, odpowiednio wyposażeni i nadzorowani;
- telewizja przemysłowa *(ang. Closed Circuit Television);*
- nadzór nad gośćmi, którzy mogą być eskortowani w czasie pobytu w obiekcie i którzy powinni nosić w widocznym miejscu przepustki identyfikujące;
- akceptacja przez Krajową Władzę Bezpieczeństwa wyposażenia (sejfy, drzwi, zamki, klasa i typ ścian) pomieszczeń, w których na otwartych regałach przechowywane są informacje niejawne.

Polityka bezpieczeństwa NATO określa minimalne standardy przechowywania informacji niejawnych. Zgodnie z nimi informacje COSMIC TOP SECRET wariantowo mogą być przechowywane:

- w I lub II strefie bezpieczeństwa, w zaaprobowanym przez Krajową Władzę Bezpieczeństwa sejfie. Jeden z poniższych warunków powinien być spełniony;
  - / pomieszczenie musi znajdować się pod stałą ochroną prowadzoną przez strażnika bądź przez służbę dyżurną,

---

[210] Zgodnie z zasadą „obrony w głąb", IDS można wykorzystywać w pomieszczeniach i budynkach. Stosowanie systemu powinno być połączone z zaplanowanymi działaniami grupy interwencyjnej, reagującej w możliwie krótkim czasie na wywołany alarm.

/ sejf musi być kontrolowany nie rzadziej, niż co dwie godziny bądź zainstalowany jest system telewizji przemysłowej,

- w pomieszczeniu specjalnie wzmocnionym, wyposażonym w system wykrywania ruchu, pod warunkiem użycia grupy interwencyjnej, zdolnej do przybycia w czasie nie dłuższym niż szacowany jako niezbędny do siłowego wejścia do tego pomieszczenia;
- w skarbcu, wyposażonym w system wykrywania ruchu, pod warunkiem użycia grupy interwencyjnej zdolnej do przybycia w czasie nie dłuższym niż szacowany jako niezbędny do siłowego wejścia do skarbca.

Informacje SECRET mogą być przechowywane według zasad określonych dla informacji o wyższej klauzuli bądź wariantowo:

- w zaaprobowanym przez Krajową Władzę Bezpieczeństwa sejfie bądź w skarbcu, bez dodatkowych elementów zabezpieczenia i kontroli;
- w pomieszczeniu specjalnie wzmocnionym, w którym dodatkowo stosuje się stałą ochronę, kontrolę pomieszczenia co cztery godziny lub system wykrywania ruchu pod warunkiem użycia grupy interwencyjnej w czasie nie dłuższym niż szacowany jako niezbędny do siłowego wejścia do pomieszczenia.

Informacje CONFIDENTIAL powinny być chronione tak jak dwie wyższe kategorie informacji, z tym iż nie jest wymagane stosowanie dodatkowych elementów kontroli. Informacje RESTRICTED powinny być przechowywane w zamykanym na klucz pojemniku.

Dyrektywa w sprawie bezpieczeństwa fizycznego określa, iż klucze do sejfów, szaf pancernych nie mogą być wynoszone poza budynek, w którym się znajdują i powinny być chronione tak samo jak informacje, do których umożliwiają dostęp. Klucze bieżącego użytku i klucze zapasowe powinny być przechowywane w oddzielnych pojemnikach a zapisy kombinacji do każdego z nich w oddzielnych kopertach. Istotnym jest, aby klucze zapasowe, przeznaczone do użycia na wypadek stanu zagrożenia były przechowywane w opieczętowanych, nieprzezroczystych kopertach przez odpowiednią instytucję, cywilny lub wojskowy organ NATO. Znajomość kombinacji szyfrowych sejfów musi być ograniczona do możliwie

najmniejszej liczby osób. Minimalnym wymogiem jest zmiana kombinacji szyfrowej:

- przy pierwszym wykorzystaniu;
- zawsze, kiedy ma miejsce zmiana personelu znającego kombinację;
- zawsze, kiedy zastąpiło ujawnienie lub istnieje podejrzenie ujawnienia kombinacji;
- nie rzadziej, niż co 12 miesięcy[211].

Istotną częścią regulacji w dziedzinie bezpieczeństwa fizycznego jest ochrona przed technicznymi środkami uzyskiwania informacji. Pomieszczenia lub miejsca, w których regularnie omawia się informacje niejawne o klauzuli NATO SECRET i wyższej oraz gdzie istnieje, potwierdzone przez właściwą władzę bezpieczeństwa, zagrożenie instalacji podsłuchu powinny być chronione przed podsłuchem pasywnym[212] i aktywnym.[213] Ochrona przed podsłuchem pasywnym wymaga skorzystania z doradztwa technicznego i może wymagać zastosowania w obszarach narażonych na podsłuch dźwiękoszczelnych ścian, drzwi, podłóg i sufitów. Natomiast ochrona przed podsłuchem aktywnym może wymagać technicznej lub fizycznej kontroli bezpieczeństwa konstrukcji pomieszczenia lub jego wyposażenia oraz armatury, sprzętu biurowego, środków łączności. Kontrole te mogą być prowadzone przez wyszkolony personel, za zgodą Krajowej Władzy Bezpieczeństwa.

Pomieszczenia wymagające szczególnej ochrony przed podsłuchem wymagają systematycznej kontroli również w czasie, gdy nie są w nich prowadzone żadne rozmowy. Każde wejście osób z zewnątrz, prace konserwacyjne czy nieuprawnione wtargnięcie musi być szczegółowo sprawdzone. W pomieszczeniach tych musi być prowadzony wykaz sprzętu i mebli, które znajdowały się i obecnie się w nim znajdują wraz z numerami seryjnymi i inwentarzowymi. Z reguły w pomieszczeniach tych nie powinno się instalować aparatów telefonicznych. Jednak tam gdzie ich instalacja jest nieunikniona muszą być zaopatrzone w urządzenia,

---

[211] AC/35-D/2001, str. 8

[212] Podsłuch pasywny rozumiany jest jako wyciek informacji niejawnych poprzez niezabezpieczone środki łączności, bezpośrednie podsłuchiwanie lub niezamierzoną emisję elektromagnetyczną.

[213] Podsłuch aktywny rozumiany jest jako wyciek informacji niejawnych NATO poprzez mikrofony przewodowe, bezprzewodowe lub inne, celowo zainstalowane urządzenia.

powodujące automatyczne wyłączenie, bądź powinny być fizycznie odłączane w czasie prowadzonych rozmów. Oczywiście wnoszenie telefonów komórkowych do pomieszczeń jest zabronione[214]. Eksploatacja sprzętu elektronicznego może nastąpić pod warunkiem jego sprawdzenia przez ekspertów w dziedzinie łączności, którzy muszą określić czy istnieje niebezpieczeństwo transmisji informacji poza obszar zabezpieczony przed technicznymi środkami uzyskiwania informacji.

Standardy w NATO szczegółowo określają wymogi bezpieczeństwa fizycznego w kancelariach oraz innych pomieszczeniach gdzie informacje niejawne przechowywane są bezpośrednio na regałach, wykresach, mapach. Dotyczą one w szczególności:

- konstrukcji – ściany, podłogi i sufit muszą być połączone ze sobą na stałe jako trwałe elementy;
- drzwi – muszą być wykonane z materiału o wysokiej wytrzymałości, zabezpieczone atestowanym zamkiem szyfrowym;
- otworów wentylacyjnych – otwory o powierzchni powyżej 620 centymetrów kwadratowych oraz przekroju większym niż 15 centymetrów muszą być zabezpieczone kratami, metalowymi żaluzjami lub urządzeniem do wykrywania ruchu;
- okien – muszą być pokryte materiałem nieprzezroczystym lub wyposażone w rolety. Okna na parterze muszą być zabezpieczone przed wyważeniem i zabezpieczone przez autonomiczny bądź zainstalowany w pomieszczeniu czujnik wykrywania ruchu.

Bezpieczeństwo informacji jest pojęciem stosowanym w NATO dla określenia zasad wytwarzania dokumentu klasyfikowanego, jego rejestrowania, przesyłania, kontrolowania, archiwizowania i niszczenia. Generalną zasadą jest, iż informacja niejawna wymaga ochrony w trakcie całego okresu swego istnienia. W tym celu ustanowiono w NATO następujące poziomy klasyfikowania informacji:

---

[214] W związku ze stosowaniem w wielu instytucjach i przedsiębiorstwach systemów umożliwiających natychmiastową blokadę telefonu komórkowego po wejściu do pomieszczenia wymóg ten może być ograniczony.

- COSMIC TOP SECRET (CTS) – jej ujawnienie może spowodować wyjątkowo poważną szkodę dla NATO;
- NATO SECRET (NS) – jej ujawnienie może spowodować poważną szkodę dla NATO;
- NATO CONFIDENTIAL NC) – jej ujawnienie może być szkodliwe dla NATO;
- NATO RESTRICTED (NR) – jej ujawnienie może być szkodliwe dla interesów lub dla skuteczności działań NATO.

Za nadanie klauzuli tajności, za wstępne określenie obiegu dokumentu niejawnego oraz za ewentualną możliwość zmiany klasyfikacji po określonym czasie lub zaistnieniu oczekiwanego zdarzenia odpowiada wykonawca. Bez jego zgody nie wolno zmieniać ani obniżać klauzuli tajności. Kraje natowskie oraz cywilne i wojskowe struktury Paktu są zobowiązane do wprowadzenia mechanizmów, gwarantujących poprawne oznaczanie dokumentów niejawnych. Wymogiem jest cykliczna weryfikacja klauzuli nadanej dokumentowi niejawnemu[215]. Innym standardem jest nadanie dokumentowi, który składa się z kilku części składowych takiej klauzuli, jak najwyższa klauzula dokumentu wchodzącego w jego skład. Często zdarza się też, że powstaje informacja zbiorcza składająca się z danych, pochodzących z różnych źródeł. Wówczas możliwym a nawet zalecanym jest nadawanie tego typu dokumentowi klauzuli wyższej niż wynikająca z klauzul dokumentów cząstkowych.

Klauzula informacji niejawnej może być zmieniona tylko przez wykonawcę lub za jego zgodą. Jeśli nie można ustalić autora dokumentu niejawnego zgodę taką wyraża następca prawny lub przełożony wyższego szczebla.

Każde państwo natowskie oraz cywilne i wojskowe organy Paktu są zobowiązane do stworzenia systemu kancelarii, których zadaniem jest otrzymywanie, przechowywanie, dystrybucja i niszczenie dokumentów niejawnych. Każdy kraj może utworzyć maksymalnie dwie główne kancelarie dla obsługi dokumentów COSMIC TOP SECRET, które spełniają również rolę głównego

[215] Informacja COSMIC TOP SECRET musi być weryfikowana co 5 lat o ile wykonawca nie określił, iż klauzula będzie automatycznie obniżona po 2 latach.

organu odbiorczo – wysyłkowego. Kancelarie te mogą również przechowywać informacje o niższych klauzulach. Oprócz kancelarii głównych w każdym państwie natowskim powinny funkcjonować kancelarie i punkty obsługi dokumentów odpowiadające za wewnętrzną dystrybucję informacji COSMIC TOP SECRET i NATO SECRET oraz za prowadzenie bazy danych o każdym, otrzymywanym dokumencie. Personel kancelarii narodowej może być również odpowiedzialny za obsługę informacji niejawnych NATO. Warunkiem jest posiadanie stosownego poświadczenia bezpieczeństwa i przeszkolenie w zakresie dostępu do informacji niejawnych NATO.

Jeśli w danej strukturze organizacyjnej *(ministerstwo, departament, dowództwo wojskowe)* funkcjonuje kancelaria COSMIC TOP SECRET obowiązkowym jest powołanie oficera do spraw nadzoru nad informacjami COSMIC TOP SECRET *(ang. COSMIC Control Officer - CCO)* oraz jeśli jest to konieczne jego zastępcy. CCO odpowiada w szczególności za[216]:

- fizyczną ochronę informacji COSMIC TOP SECRET w kancelarii głównej bądź wewnętrznej;
- prowadzenie aktualnej bazy danych o wszelkich dokumentach COSMIC TOP SECRET, znajdujących się w kancelarii i przekazanych do innych kancelarii;
- prowadzenie bieżącej bazy danych o wszystkich osobach, upoważnionych do dostępu, do przechowywanych w kancelarii, informacji niejawnych o klauzuli COSMIC TOP SECRET,;
- prowadzenie bazy danych wszystkich kancelarii i punktów obsługi, z którymi kancelaria wymienia informacje COSMIC TOP SECRET, w tym nazwisk innych oficerów do spraw nadzoru nad informacjami COSMIC TOP SECRET oraz wzorów ich podpisów;
- dystrybucję informacji niejawnych o klauzuli COSMIC TOP SECRET wyłącznie do upoważnionych adresatów;
- przesyłanie informacji COSMIC TOP SECRET;

[216] Zadania określone dla oficera do spraw nadzoru nad informacjami COSMIC TOP SECRET mogą być przypisane kierownikowi kancelarii COSMIC TOP SECRET.

- otrzymywanie potwierdzenia o przesłaniu lub przekazaniu informacji o klauzuli COSMIC TOP SECRET;
- zapewnienie, iż dokumenty o klauzuli COSMIC TOP SECRET są zwracane po ich wykorzystaniu do odpowiedniej kancelarii celem przechowywania lub zniszczenia;
- w przypadku kierowników głównych kancelarii COSMIC TOP SECRET, zawiadamianie Biura Bezpieczeństwa NATO o zmianach organizacyjnych, dotyczących kancelarii lub punktu obsługi dokumentów, za które jest odpowiedzialny.[217]

Zasady bezpieczeństwa informacji określają, iż kancelarie powinny prowadzić roczne kontrole dokumentów o klauzuli COSMIC TOP SECRET. Kontrola powinna wykazać, iż:

- dokument znajduje się w kancelarii i zawiera właściwą ilość stron;
- właściwie potwierdzono jego odbiór;
- istnieje informacja, że zmieniono jego klauzulę lub został zniszczony.[218].

Kancelarie i punkty obsługi powinny składać roczne raporty o wynikach przeprowadzonej inwentaryzacji do głównej kancelarii COSMIC TOP SECRET. Wyniki rocznych inwentaryzacji w głównych kancelariach COSMIC TOP SECRET są przesyłane przez właściwą Krajowa Władze Bezpieczeństwa do Biura Bezpieczeństwa NATO w terminie do 31 marca każdego roku.

W odniesieniu do dokumentów o klauzuli NATO SECRET minimalnymi wymogami są konieczność prowadzenia bieżącej bazy danych o przechowywanych dokumentach oraz prowadzenie okresowych, wyrywkowych kontroli kancelarii, komórek organizacyjnych i osób, którym udostępniane są informacje NATO SECRET.

Zgodnie z polityką bezpieczeństwa NATO nie wymaga się, aby dokumenty o klauzuli NATO CONFIDENTIAL i NATO RESTRICTED były rejestrowane. Jednakże odpowiednie środki bezpieczeństwa, uniemożliwiające dostęp do tych

---

[217] AC/35-D/2002, str. 4-5.
[218] Tamże, str. 5

informacji przez osoby nieuprawnione muszą być stosowane wszędzie tam, gdzie takie dokumenty są wytwarzane oraz przechowywane.

Dokumenty COSMIC TOP SECRET mogą być kopiowane jedynie w wyjątkowych sytuacjach, w celu realizacji konkretnego zadania, pod warunkiem zachowania szeregu wymogów dotyczących kontroli przez CCO, właściwej rejestracji i kontroli. Informacje NATO SECRET mogą być kopiowane przez adresatów z zachowaniem zasad ich oznaczania i rejestracji. Informacje NATO CONFIDENTIAL i NATO RESTRICTED mogą być kopiowane pod warunkiem, iż zachowane są zasady uniemożliwiające dostęp do nich przez osoby nieuprawnione.

Informacje niejawne NATO przenoszone w granicach obiektów powinny być ukryte w taki sposób, aby uniemożliwić wgląd w ich treść. Przesyłanie informacji poza te obiekty, na terenie kraju natowskiego może się odbywać z wykorzystaniem:

- wojskowej lub rządowej służby kurierskiej;
- państwowej służby pocztowej *(do klauzuli NATO SECRET włącznie);*
- autoryzowanej przez krajowe władze bezpieczeństwa komercyjnej firmy kurierskiej *(do klauzuli NATO SECRET);*
- transportu osobistego pod warunkiem zaewidencjonowania przesyłki w kancelarii, właściwego jej zapakowania oraz posiadania przez osobę przewożącą pisemnego upoważnienia. Jeżeli przewożony jest dokument o klauzuli NATO CONFIDENTIAL i wyższej wymagany jest certyfikat kuriera NATO *(ang. Courier Certificate).*[219]

Dokumenty niejawne o klauzuli NATO CONFIDENTIAL i wyższej, przesyłane pomiędzy instytucjami czy firmami, muszą być zapakowane w taki sposób, aby uniemożliwić wgląd w ich treść przez osoby postronne. Wewnętrzne opakowanie powinno być właściwie zabezpieczone, posiadać klauzulę tajności oraz pełny opis i adres odbiorcy informacji. Natomiast zewnętrzne opakowanie musi posiadać opis i adres odbiorcy, umożliwiać pokwitowanie odbioru przesyłki ale w żaden sposób nie powinno ujawniać, iż wewnątrz znajduje się dokument niejawny. Jeśli dokument jest przewożony przez kuriera, informacja o tym powinna

[219] Wzór certyfikatu kuriera NATO znajduje się w Załączniku Nr 19.

znajdować się na opakowaniu zewnętrznym. W odniesieniu do informacji o klauzuli RESTRICTED minimalnym wymogiem jest umieszczenie dokumentu, w co najmniej jednej, nie przezroczystej kopercie.

Przesyłanie informacji niejawnych COSMIC TOP SECRET do innych krajów odbywa się wyłącznie poprzez pocztę dyplomatyczną bądź kuriera wojskowego. Zabroniony jest transport osobisty. W odniesieniu do informacji SECRET i CONFIDENTIAL możliwym jest również przesyłanie informacji przesyłką poleconą bądź z użyciem transportu osobistego. Informacje o klauzuli RESTRICTED mogą być przesyłane przez pocztowe lub komercyjne firmy kurierskie. Kraje natowskie są zobowiązane do prowadzenia szczegółowej dokumentacji pozwalającej odtworzyć obieg informacji niejawnych. Szczególną uwagę powinno się zwracać na obieg informacji COSMIC TOP SECRET. Standardy natowskie ustanawiają obowiązek przechowywania karty zapoznania się z dokumentem o tej klauzuli przez 10 lat od daty jego zniszczenia.

Dokumenty niejawne, które utraciły swą aktualność bądź są zbędne powinny być sukcesywnie niszczone. Personel kancelarii, prowadzący stały nadzór nad przechowywanymi informacjami powinien nie czekając na szczegółowe instrukcje czy wytyczne na bieżąco decydować o niszczeniu dokumentów, które nie muszą być dłużej przechowywane. Niszczenie informacji COSMIC TOP SECRET odbywa się pod nadzorem CCO a informacji SECRET w obecności dwóch osób. Protokoły zniszczenia przechowywane są odpowiednio przez 10 i 5 lat od daty zniszczenia dokumentu. Nie jest koniecznym rejestrowanie faktów zniszczenia w odniesieniu do dokumentów niejawnych o klauzulach CONFIDENTIAL i RESTRICTED.

Istotną sferą bezpieczeństwa informacji jest metodyka postępowania na wypadek naruszenia zasad ochrony informacji niejawnych. Wszystkie nieprawidłowości w tej sferze muszą być natychmiast zgłaszane do Krajowej Władzy Bezpieczeństwa. Ich rozpatrywanie powinno być powierzane osobom, które nie mają żadnych powiązań z naruszającymi przepisy, posiadają doświadczenie w dziedzinie bezpieczeństwa informacji i prowadzenia dochodzeń a jeśli jest to konieczne posiadają przygotowanie kontrwywiadowcze. Głównym

celem dochodzenia jest ustalenie, czy została ujawniona informacja niejawna NATO. Jeśli w istocie doszło do ujawnienia informacji niejawnej a dostęp do niej miały osoby nieuprawnione, fakt ujawnienia informacji podlega zgłoszeniu do Biura Bezpieczeństwa NATO. Jeśli ujawnienie dotyczy informacji COSMIC TOP SECRET i SECRET, bądź istnieje podejrzenie, iż ujawnienie ma związek ze szpiegostwem lub informacje ujawnione zostały w środkach masowego przekazu, Krajowa Władza Bezpieczeństwa, cywilny lub wojskowy organ NATO muszą złożyć raport wstępny a w terminie 90 dni raport końcowy. Biuro Bezpieczeństwa NATO musi być poinformowane o wynikach dochodzenia, dotyczącego ujawnienia informacji CONFIDENTIAL, po jego zakończeniu. W zasadzie nie informuje się Biura Bezpieczeństwa NATO o ujawnieniu informacji o klauzuli RESTRICTED, chyba że ujawnienie ma związek z działalnością obcych służb specjalnych bądź informacja została ujawniona w środkach masowego przekazu. We wszystkich przypadkach, głównym celem raportów składanych do Biura Bezpieczeństwa jest oszacowanie szkody, jaka może być wyrządzona w związku z ujawnieniem informacji niejawnych NATO.

Informacje niejawne NATO, w uzasadnionych przypadkach mogą być udostępnione organizacjom międzynarodowym lub krajom nie natowskim. Podstawą udostępnienia informacji w tym trybie są prowadzone wspólnie działania lub projekty, które są zatwierdzone przez Radę Północnoatlantycką. Każdy wniosek musi być indywidualnie rozpatrzony i zatwierdzony[220] a udostępnienie musi zawsze odbywać się za zgodą wykonawcy.

Bezpieczeństwo przemysłowe jest pojęciem określającym zasady ochrony informacji klasyfikowanych NATO w trakcie negocjacji, zlecania oraz realizacji przez przedsiębiorców kontraktów niejawnych. Warunkiem realizacji kontraktu na rzecz NATO jest posiadanie FACILITY SECURITY CLEARANCE

---

[220] Informacje ATOMAL, niezależnie od klauzuli tajności nie mogą być udostępniane żadnej organizacji ani żadnemu krajowi, który nie jest strona Umowy między Stronami Traktatu Północnoatlantyckiego współpracy w dziedzinie informacji atomowych. W uzupełnieniu do wymienionej Umowy, w NATO opracowano Procedury Administracyjne *(ang. Administrative Arrangements),* regulujące zasady kontroli i przechowywania informacji tego typu, które musza być podpisane przez Strony Umowy – C-M(68)41.

CERTIFICATE[221], jeśli z jego realizacją wiąże się konieczność udostępnienia zarówno głównemu wykonawcy jak i podwykonawcy informacji niejawnych o klauzuli CONFIDENTIAL i wyższej[222]. Obowiązkiem agencji bądź biura prowadzących negocjacje z wykonawcą jest zapewnienie, aby uczestniczące w nich osoby posiadały wymagane poświadczenia bezpieczeństwa osobowego, właściwe do klauzuli tajności udostępnianych im informacji, oraz miały dostęp do informacji niejawnych w zakresie, jaki jest niezbędny do kontynuacji negocjacji. Po dokonaniu zlecenia głównego kontraktu, wykonawca może negocjować umowy z podwykonawcami, ci z kolei mogą podnajmować kolejne firmy. Generalną zasadą jest, iż wymogi, jakie obowiązują wykonawcę głównego mają zastosowanie do każdego kolejnego podwykonawcy. W sytuacji, gdy potencjalny podwykonawca ma siedzibę i jest zarejestrowany w państwie nie natowskim zgodę na zawarcie kontraktu z nim musi wyrazić agencja natowska, która negocjowała kontrakt z głównym wykonawcą.

Po podpisaniu kontraktu agencja natowska prowadząca negocjacje musi poinformować o nim Krajową Władzę Bezpieczeństwa bądź Wyznaczoną Władzę Bezpieczeństwa kraju, z którego pochodzi firma, mająca realizować kontrakt oraz zapewnić dostarczenie wykonawcy wraz z kontraktem Instrukcji Bezpieczeństwa Przemysłowego *(ang. Project Security Instruction)* lub Aneksu Bezpieczeństwa *(ang. Security Aspect Letter)*. Pierwszy z wymienionych dokumentów musi być opracowany do poważnych kontraktów. Jednak istotą obu dokumentów jest ustalenie jednolitych procedur bezpieczeństwa przemysłowego dla państw, organów NATO i bezpośrednich wykonawców, sprecyzowanie klauzuli tajności kontraktu oraz wymogów, jakie muszą być spełnione, aby przekazywane przedsiębiorcy informacje niejawne były należycie wykorzystywane i chronione. Oczywiście dominującą zasadą pozostaje zapewnienie zgody wykonawcy na udostępnienie informacji niejawnych.

Bezwzględnym warunkiem uczestnictwa w konkursie ofert, negocjacjach i późniejszej realizacji kontraktu jest wydanie FACILITY SECURITY

---

[221] Wzór FACILITY SECURITY CLEARANCE CERTIFICATE znajduje się w Załączniku Nr 20.

[222] Do kontraktów o klauzuli RESTRICTED nie wymaga się poświadczenia bezpieczeństwa przemysłowego, o ile nie wymagają tego narodowe przepisy ochrony informacji niejawnych państwa członkowskiego.

CLEARANCE CERTIFICATE przez Krajową Władzę Bezpieczeństwa kraju, w którym firma jest zarejestrowana i posiada osobowość prawną. Natomiast pracownicy firmy muszą otrzymać wymagane PERSONNEL SECURITY CLEARANCE CERTIFICATES i zostać przeszkoleni w zakresie procedur bezpieczeństwa obowiązujących w NATO. Odpowiedzialność za przeprowadzenie postępowań sprawdzających wobec osób spoczywa na Krajowej Władzy Bezpieczeństwa bądź Wyznaczonej Krajowej Władzy Bezpieczeństwa państwa, w którym jest zarejestrowany wykonawca kontraktu.

W czasie realizacji kontraktu niejawnego nieunikniony jest międzynarodowy transport przesyłek, wyposażenia i materiałów niejawnych NATO. W związku z tym muszą być zachowane zasady, gwarantujące bezpieczeństwo przewożonych przesyłek, włącznie z koniecznością posiadania przez firmy zapewniające transport FACILITY SECURITY CLEARANCE CERTIFICATE a przez osoby zajmujące się przesyłką PERSONNEL SECURITY CLEARANCE CERTIFICATES. W czasie organizacji przewozu muszą być zachowane zasady ochrony informacji określone w przepisach bezpieczeństwa informacji a zwłaszcza w Supporting Directive on Security of Information. Trasa transportu powinna przebiegać tylko przez kraje natowskie, jednak gdy jest to niemożliwe, zgodę na transport przez inne państwa muszą wyrazić władze bezpieczeństwa kraju wysyłającego przesyłkę.

Innym, nieuniknionym aspektem bezpieczeństwa przemysłowego jest organizacja wizyt międzynarodowych, składanych przez wojskowych i cywilnych przedstawicieli krajów NATO oraz wykonawców i podwykonawców kontraktów natowskich. Wizyty tego typu mogą mieć miejsce w instytucjach, w przedsiębiorstwie wykonawcy czy podwykonawcy państw członkowskich NATO oraz w cywilnym lub wojskowym organie Paktu. Muszą być one zatwierdzone przez Krajową Władzę Bezpieczeństwa lub Wyznaczoną Krajową Władzę Bezpieczeństwa a warunkami zatwierdzenia takiej wizyty są jej związek z konkretnym programem, projektem lub kontraktem oraz posiadanie poświadczeń bezpieczeństwa i potrzeby wiedzy przez składających wizytę. Z kolei przyjmujący wizytę muszą zapewnić udostępnienie odwiedzającym wyłącznie takich informacji niejawnych, które są związane z jej celem. Są też zobowiązani do sporządzania i

przechowywania wykazów osób odwiedzających, włącznie z danymi o instytucjach, jakie reprezentują.

Konsekwencją powyższych regulacji jest obowiązek występowania przez instytucje, wykonawców, podwykonawców, z wnioskiem o złożenie wizyty międzynarodowej *(ang. Request for Visit)*[223]. Wniosek taki jest kierowany do Krajowej bądź Wyznaczonej Władzy Bezpieczeństwa odwiedzanego kraju. Zawarte w nim dane muszą przede wszystkim potwierdzać posiadanie przez odwiedzających poświadczeń bezpieczeństwa osobowego. Podobna procedura obowiązuje w wypadku konieczności przeniesienia personelu, w ramach realizacji tego samego kontraktu niejawnego, z jednego przedsiębiorstwa do drugiego, znajdującego się na terenie innego państwa natowskiego. Jeśli jest to dopuszczalne przez przepisy narodowe wizyty związane z kontraktami CONFIDENTIAL i RESTRICTED mogą być uzgadniane na poziomie organów bezpieczeństwa składającego wizytę i odwiedzanego obiektu czy instytucji.[224]

Bezpieczeństwo teleinformatyczne jest pojęciem stosowanym w NATO dla określenia środków bezpieczeństwa, stosowanych do ochrony informacji niejawnych, przetwarzanych, przechowywanych lub przesyłanych w systemach, sieciach teleinformatycznych, systemach łączności i innych systemach elektronicznych przed utratą jej poufności, integralności lub dostępności, przypadkowo lub w sposób zamierzony a także w celu zapobieżenia utraty integralności i dostępności samych systemów. Dla określenia bezpieczeństwa teleinformatycznego używane jest powszechnie pojęcie INFOSEC. Zgodnie z natowskimi standardami INFOSEC obejmuje środki bezpieczeństwa transmisji komputerowej, emisji i bezpieczeństwa kryptograficznego oraz wykrywanie, dokumentowanie oraz przeciwdziałanie zagrożeniom dla informacji niejawnych przetwarzanych w systemach teleinformatycznych i dla samych systemów. Bezpieczeństwo teleinformatyczne nie może być pojęciem oderwanym od innych aspektów bezpieczeństwa, takich jak fizycznego, osobowego czy informacji.

---

[223] Wzór Request for visit znajduje się w Załączniku Nr 21.

[224] Może to być oficer bezpieczeństwa *(ang. Security Officer)*, który jest odpowiednikiem pełnomocnika ochrony jednostki organizacyjnej.

Zgodnie z polityką bezpieczeństwa NATO dopiero połączenie tych czterech aspektów bezpieczeństwa informacji niejawnych i wzajemne przestrzeganie ustanowionych norm w każdej ze sfer pozwoli utworzyć tak zwane bezpieczne środowisko i będzie gwarancją zachowania poufności i integralności informacji przetwarzanych w tym środowisku z wykorzystaniem systemów i sieci teleinformatycznych.

Zgodnie z normami natowskimi celami bezpieczeństwa teleinformatycznego są:

- zapewnienie poufności informacji niejawnych NATO poprzez kontrolowanie ujawniania i dostępu do nich oraz sprzętu, na przykład kryptograficznego przy pomocy którego są przetwarzane;
- zapewnienie integralności informacji niejawnych NATO oraz sprzętu przy pomocy którego są przetwarzane;
- zapewnienie dostępności informacji niejawnych NATO oraz sprzętu przy pomocy którego są przetwarzane.[225]

Integralność i dostępność informacji niejawnych NATO oraz sprzętu powinna być chroniona przy użyciu jak najmniejszych środków. Dodatkowe środki muszą być podejmowane wówczas, gdy istnieje zwiększone zagrożenie dla informacji bądź zidentyfikowane są słabe strony funkcjonującego systemu.

Wszystkie systemy przetwarzające informacje niejawne muszą podlegać procesowi akredytacji, zwykle prowadzonemu przez właściwe Krajowe Władze Bezpieczeństwa. Osoby upoważnione do dostępu do informacji niejawnych, przetwarzanych w systemach i sieciach teleinformatycznych muszą posiadać PERSONNEL SECURITY CLEARANCE CERTIFICATES i być świadome swej odpowiedzialności nie tylko za poufność, dostępność i integralność tych informacji, ale też za bezpieczeństwo sprzętu, wchodzącego w skład danego systemu. Wymóg posiadania poświadczenia bezpieczeństwa dotyczy też osób, które, odpowiadając za dostępność i integralność sprzętu nie posiadają bezpośredniego dostępu do informacji niejawnych. Obszary, w których ulokowane są systemy i sieci teleinformatyczne muszą spełniać wymogi bezpieczeństwa fizycznego i

[225] C-M(2002)49, Załącznik F *(ang. Enclosure F)*, str 1.

gwarantować, iż cele bezpieczeństwa teleinformatycznego zostaną osiągnięte. Wszystkie niejawne komputerowe nośniki informacji *(dyski stałe i wymienne)* muszą być właściwie oznakowane, przechowywane i chronione w taki sam sposób, jak chronione są dokumenty o najwyższej klauzuli tajności, znajdujące się na tych nośnikach. Krajowe władze bezpieczeństwa zobowiązane są do określenia procedur, zgodnie z którymi mogą być kasowane informacje niejawne przechowywane na komputerowych nośnikach informacji.

W stosunku do systemów przetwarzających informacje niejawne NATO muszą być stosowane środki bezpieczeństwa zapewniające:

- niezawodną identyfikację osób upoważnionych do dostępu do informacji niejawnych;
- kontrolę ujawnienia informacji niejawnych i dostępu do nich;
- weryfikację integralności i pochodzenia informacja niejawnych;
- zachowanie integralności i dostępności informacji niejawnych;
- kontrolę połączeń systemów przetwarzających informacje niejawne;
- określenie i zachowanie stopnia tajności, ocenę i weryfikację funkcjonowania systemu;
- nadzór nad pracą użytkownika i funkcjonowaniem systemu.

Środki te mają służyć odstraszaniu, zapobieganiu, wykrywaniu oraz likwidowaniu skutków naruszenia tajności, integralności i dostępności informacji niejawnych NATO oraz systemów, w których są przetwarzane. Dotyczy to nie tylko ich bezproblemowego funkcjonowania, ale również sytuacji, gdy istnieje zagrożenie ich bezpieczeństwa.

Bardzo ważną sferą jest elektromagnetyczna transmisja informacji niejawnych NATO, podczas której muszą być stosowane specjalne środki, zapewniające ochronę przesyłanych danych. Cywilne i wojskowe organy NATO odpowiadają za określenie wymogów, jakie muszą być zachowane w czasie transmisji informacji w celu ich zabezpieczenia przed wykryciem czy przechwyceniem. Jeśli przesyłane są informacje o klauzuli NATO SECRET i wyższej transmisja musi odbywać się z przy zastosowaniu metod i sprzętu kryptograficznego. Organem NATO, uprawnionym do zatwierdzenia sprzętu,

używanego do takiej transmisji jest Komitet Wojskowy NATO.W odniesieniu do informacji o klauzuli CONFIDENTIAL i RESTRICTED dopuszczalna jest również akceptacja metody szyfrowania lub sprzętu kryptograficznego przez kraj członkowski. Nie dotyczy to jednak sytuacji, gdy metoda bądź sprzęt są finansowane ze środków NATO. Organem zatwierdzającym pozostaje w tym przypadku Komitet Wojskowy.

W wyjątkowych okolicznościach informacje niejawne do klauzuli SECRET mogą być przesyłane otwartym tekstem, bez szyfrowania. W rozumieniu polityki bezpieczeństwa NATO może to mieć miejsce w okresie zbliżającego się kryzysu, konfliktu lub wojny lub w sytuacji, gdy dostarczenie informacji na czas ma wyjątkowe znaczenie i dokonano oceny, iż informacja nie może być wykorzystana w czasie, uniemożliwiającym wykonanie prowadzonej operacji.

Normy bezpieczeństwa teleinformatycznego stanowią, iż sprzęt kryptograficzny czy metody szyfrowania muszą podlegać w NATO szczególnej ochronie. Każdy kraj członkowski jest zobowiązany do ustanowienia przepisów i organów, które zajmują się dystrybucją i ochroną informacji kryptograficznych. Muszą też istnieć specjalne procedury regulujące zarówno dzielenie się informacjami z dziedziny kryptografii, jak również wybór, produkcję i zaopatrzenie w sprzęt kryptograficzny.

Najwyższym organem NATO, odpowiadającym za sprawy bezpieczeństwa teleinformatycznego, w tym opracowywanie dokumentów normatywnych i przestrzeganie ustanowionych norm jest Komitet Konsultacji, Dowodzenia i Kontroli *(ang. NATO Consultation, Command and Control (C3) Board),* który ściśle współpracuje z Biurem Bezpieczeństwa NATO. Każdy kraj członkowski jest zobowiązany do ustanowienia:

- Krajowej Władzy Bezpieczeństwa Łączności *(ang. National Communications Security Authority)*, odpowiedzialnej za właściwy wybór, i funkcjonowanie systemów i sprzętu kryptograficznego oraz utrzymywanie kontaktu z organami bezpieczeństwa kryptograficznego NATO;

- Krajowej Władzy Dystrybucji *(ang. National Distribution Authority)*, uprawnionej do otrzymywania, przechowywania i dystrybucji wewnątrz swego kraju materiałów kryptograficznych NATO.

ROZDZIAŁ IV

OCENA ZGODNOŚCI POLSKICH ROZWIĄZAŃ W DZIEDZINIE BEZPIECZEŃSTWA I OCHRONY INFORMACJI NIEJAWNYCH W SFERZE WOJSKOWEJ ZE STANDARDAMI NATO

1. Prowadzenie postępowań sprawdzających przed wydaniem poświadczenia bezpieczeństwa osobowego.

Przyznać należy, iż podstawowe zasady i minimalne standardy, dotyczące prowadzenia postępowań sprawdzających wobec osób przed wydaniem PERSONNEL SECURITY CLEARANCE CERTIFICATE, określone w dokumentach normatywnych Sojuszu znajdują odzwierciedlenie w Ustawie o ochronie informacji niejawnych i dokumentach niższego rzędu, regulujących prowadzenie takich postępowań. Inaczej być nie może, ponieważ przy opracowywaniu polskich przepisów, w czasie trwania procesu akcesyjnego, dokumenty natowskie były materiałem wyjściowym, który posłużył do przygotowania narodowych przepisów w tym zakresie. Poza tym odbywało się szereg konsultacji z ekspertami Sojuszu, zwłaszcza Biura Bezpieczeństwa NATO oraz krajowymi władzami bezpieczeństwa państw członkowskich, których celem było opracowanie rozwiązań, spójnych z polityką bezpieczeństwa Paktu.

Jednakże jest kilka sfer, w których polskie rozwiązania różnią się nieco od sojuszniczych, bądź poświęcają mniej uwagi na zagadnienia, które w przepisach natowskich są bardziej uwypuklone.

Nie jest celowym powtarzanie tego, co jest wspólne, natomiast istotna jest analiza na ile małe różnice i niuanse, które nie przeczą rozwiązaniom przyjętym w Sojuszu powodują, iż nasze rodzime służby ochrony państwa oraz pełnomocnicy ochrony jednostek organizacyjnych są bardzo zajęci i czasami zajmują się sprawami, które z punktu widzenia polityki bezpieczeństwa NATO są raczej drugorzędne.

Do najważniejszych różnic w sferze bezpieczeństwa osobowego pomiędzy rozwiązaniami oferowanymi w dokumentach normatywnych NATO a polskimi normatywami należą:

Klauzula tajności, od jakiej wymagane jest poświadczenie bezpieczeństwa.

Według norm natowskich PERSONNEL SECURITY CLEARANCE CERTIFICATE wymagany jest w przypadku konieczności dostępu do informacji o poziomie CONFIDENTIAL. W wypadku konieczności dostępu do informacji o poziomie RESTRICTED nie prowadzi się postępowania sprawdzającego a jedynie przeszkolenie osoby, która wymaga dostępu do tego typu informacji. Przeszkolenie dotyczy obowiązujących przepisów w zakresie ochrony informacji niejawnych.

Zgodnie z polskimi przepisami osoba, która wymaga dostępu do informacji ZASTRZEŻONYCH podlega postępowaniu sprawdzającemu, które kończy się wydaniem bądź odmową wydania poświadczenia bezpieczeństwa osobowego. Wydaje się, iż polskie rozwiązania nakazujące sprawdzanie osób przed upoważnieniem ich do dostępu do informacji ZASTRZEŻONYCH są nieco restrykcyjne i chyba już wymagają zmiany. Odstąpienie od obowiązku prowadzenia postępowań sprawdzających przed upoważnieniem do dostępu do informacji o klauzuli ZASTRZEŻONE zbliżyłoby również wymogi prawa do realiów systemu ochrony informacji niejawnych bowiem ilość poświadczeń do poziomu RESTRICTED, wydanych w Siłach Zbrojnych RP jest znikoma w porównaniu do wyższych klauzul tajności.

Poświadczanie znajomości przepisów o ochronie informacji niejawnych.

Regulacje natowskie określają, iż każda osoba, której wydano poświadczenie bezpieczeństwa i przeszkolono ją, lub którą jedynie przeszkolono w wypadku informacji niejawnych o poziomie RESTRICTED, powinna potwierdzić pisemnie, że zna swoje obowiązki w sferze ochrony informacji niejawnych i wie jakie konsekwencje, zgodnie z obowiązującym prawem, grożą jej w wypadku świadomego lub nieświadomego spowodowania, iż powierzone jej informacje niejawne dostaną się w niepowołane ręce. Rejestr takich oświadczeń powinien być

prowadzony przez krajowe władze bezpieczeństwa państwa natowskiego lub cywilnego bądź wojskowego organu NATO.

W Polsce przepisy prawa nie stanowią, iż wymagane jest oddzielne oświadczenie tego typu. W konsekwencji nie ma żadnych rejestrów takich oświadczeń. Domniemanie, iż zatrudniana osoba zna przepisy o ochronie informacji niejawnych wynika z potwierdzenia znajomości zakresu odpowiedzialności na zajmowanym stanowisku, w którym zazwyczaj zawarte są obowiązki w zakresie ochrony powierzanych informacji niejawnych. Znajomość zakresu odpowiedzialności na zajmowanym stanowisku powinna być potwierdzana przez osobę zatrudnioną w każdej instytucji cywilnej czy wojskowej.

Zakres postępowania sprawdzającego.

W przepisach natowskich duży nacisk jest położony na ustalenie czy osoba objęta postępowaniem sprawdzającym mogła mieć jakiekolwiek związki z działalnością szpiegowską, organizacjami sabotażowymi, terrorystycznymi, wywrotowymi i czy w związku z tym może być podatna na szantaż czy wywieranie presji. Oprócz tego istotne jest ustalenie stanu majątkowego i możliwej podatności na wywieranie presji w związku z ewentualnymi trudnościami finansowymi. Obie te sfery dotyczą nie tylko osoby sprawdzanej ale również współmałżonka, osoby z którą osoba sprawdzana mieszka oraz członków najbliższej rodziny.

Zgodnie z polskimi normami, w toku postępowania ustala się również ewentualne zagrożenia tego typu zarówno w stosunku do osoby sprawdzanej jak i jej rodziny. Jednakże nie jest to obligatoryjne a dane dotyczące rodziny sprawdza się w szerszym zakresie, kiedy istnieją uzasadnione podejrzenia co do wiarygodności sprawdzanej osoby bądź prawdziwości przekazanych przez nią w ankiecie bezpieczeństwa informacji tak o sobie jak i o członkach rodziny.

Sprawdzenia w czasie postępowania sprawdzającego.

Normą w NATO jest sprawdzanie informacji, przekazanych przez osobę objętą pierwszym postępowaniem sprawdzającym w kwestionariuszu bezpieczeństwa za ostatnie 5 lat lub od ukończenia 18 lat *(w przypadku*

postępowania do poziomu CONFIDENTIAL i SECRET) oraz 10 lat lub od ukończenia 18 lat *(w przypadku postępowania do poziomu COSMIC TOP SECRET)*. Dodatkowo, prowadzone w toku postępowania do poziomu COSMIC TOP SECRET rozmowy powinny obejmować okres ostatnich 7 lat lub od ukończenia 18 lat. W odniesieniu do wykształcenia osoba sprawdzana powinna podać dane od 18 roku życia.

Normy przewidziane w polskich przepisach przewidują konieczność podania informacji za ostatnich 10 lat niezależnie od rodzaju postępowania sprawdzającego *(dane o zatrudnieniu, adresy zamieszkiwania, etc.)* natomiast dane dotyczące kontaktów służbowych lub prywatnych osoby sprawdzanej i członków jej rodziny z obywatelami innych państw muszą obejmować okres ostatnich 20 lat. Dane o wykształceniu dotyczą wszystkich szkół ukończonych przez osobę sprawdzaną. Nie ma natomiast w polskich rozwiązaniach żadnego ograniczenia co do okresu, jaki może być przedmiotem rozmowy z osobą sprawdzaną.

Innym niuansem postępowania sprawdzającego, jest natowskie zalecenie dokonywania sprawdzeń w kartotekach, gdzie osoba sprawdzana była zatrudniona lub zamieszkiwała przez przynajmniej sześć miesięcy. W Polsce sprawdzenia opierają się jedynie na rejestrach centralnych.

Rezultat postępowania sprawdzającego.

Normy natowskie przewidują, iż postępowanie sprawdzające może się zakończyć wydaniem, odmową wydania PERSONNEL SECURITY CLEARANCE CERTIFICATE bądź cofnięciem posiadanego dokumentu, w wypadku ujawnienia informacji, mających negatywny wpływa na rękojmię zachowania tajemnicy.

Polskie standardy przewidują jedynie dwie możliwości zakończenia postępowania przed wydaniem poświadczenia bezpieczeństwa osobowego, mianowicie jego wydanie lub odmowę wydania.

Okres ważności poświadczenia bezpieczeństwa.

Standardy natowskie przewidują konieczność prowadzenia kolejnych postępowań sprawdzających po upływie 10 lat dla poziomu CONFIDENTIAL i

SECRET oraz 5 lat dla poziomu COSMIC TOP SECRET od daty wydania poprzedniego PERSONNEL SECURITY CLEARANCE CERTIFICATE.

Ustawa o ochronie informacji niejawnych stanowi, iż postępowania sprawdzające powtarza się co 10 lat w wypadku dostępu do informacji ZASTRZEŻONE i POUFNE, co 5 lat w wypadku TAJNE i co 3 lata w wypadku ŚCIŚLE TAJNE. Normy te, stosunkowo restrykcyjne w odniesieniu do dostępu do informacji TAJNE i ŚCIŚLE TAJNE, powodują konieczność częstszego niż w wielu krajach NATO wznawiania postępowania przed wydaniem kolejnego poświadczenia. W rezultacie wpływa to na znaczne zwiększenie ilości prowadzonych przez służby ochrony państwa i pełnomocników ochrony postępowań oraz ilości wydanych poświadczeń. W stosunku do osoby, której wydano poświadczenie bezpieczeństwa do poziomu ŚCIŚLE TAJNE i która nadal wymaga takiego uprawnienia, Wojskowe Służby Informacyjne są zobowiązane do wznowienia postępowania już po upływie dwóch i pół roku od momentu wystawienia poświadczenia. Jest to spowodowane wymogiem norm prawnych stanowiących, iż wniosek o przeprowadzenie kolejnego postępowania musi być nadesłany do służb ochrony państwa na minimum 6 miesięcy przed upływem terminu ważności posiadanego poświadczenia. Polskie rozwiązania powodują, iż zwłaszcza w odniesieniu do Sił Zbrojnych RP, które są nośnikiem największej ilości informacji o najwyższych klauzulach tajności niezbędne jest prowadzenie olbrzymiej ilości postępowań przed wydaniem poświadczenia do poziomu TAJNE i ŚCIŚLE TAJNE. Wydaje się, że wymogi polskie powinny być złagodzone i dostosowane do proponowanych przez politykę bezpieczeństwa NATO.

Wznowienie posiadanego poświadczenia bezpieczeństwa osobowego.

Normy bezpieczeństwa osobowego NATO stanowią, iż kolejne postępowanie sprawdzające, po upływie terminu ważności wydanego PERSONNEL SECURITY CLEARANCE CERTIFICATE obejmuje okres od poprzednio dokonanego sprawdzenia. Kolejne postępowanie powinno obejmować ponowne wypełnienie kwestionariusza. Dopuszczalne jest też wypełnienie uzupełniającej pierwszy kwestionariusz ankiety.

Zgodnie z polskimi przepisami, konieczne jest przeprowadzenie pełnego postępowania sprawdzającego i analiza danych, przekazanych przez osobę sprawdzaną w takiej samej ankiecie bezpieczeństwa osobowego. Różnica polega jedynie na tym, iż przy ponownym sprawdzeniu, nie wszystkie punkty w ankiecie muszą być wypełnione.

Upoważnianie do dostępu do informacji niejawnych osób o podwójnym obywatelstwie.

Generalną zasadą w NATO jest zakaz udostępniania informacji niejawnych osobie będącej obywatelem państwa nie natowskiego. Jednakże, polityka bezpieczeństwa stosunkowo szczegółowo określa zasady upoważniania do dostępu do informacji niejawnych osoby posiadające podwójne obywatelstwo. Nie ma specjalnych ograniczeń w wypadku, gdy postępowaniem sprawdzającym objęta jest osoba posiadająca obywatelstwo dwóch państw natowskich bowiem polityka bezpieczeństwa NATO zobowiązuje krajowe władze bezpieczeństwa państw członkowskich do ścisłej współpracy, w tym do wymiany informacji o swoich obywatelach. W sytuacji, gdy osoba, która wymaga dostępu do informacji natowskich i posiada podwójne obywatelstwo, w tym jedno państwa nie natowskiego krajowe władze bezpieczeństwa są zobowiązane do przejawienia szczególnej wnikliwości. Nie przeczy to generalnej zasadzie, iż jeśli Krajowa Władza Bezpieczeństwa jest pewna, że osoba sprawdzana gwarantuje lojalność wobec państwa natowskiego nie ma podstaw do tego, aby odmówić jej wydania poświadczenia bezpieczeństwa. Innym niuansem bezpieczeństwa osobowego jest pełnienie służby wojskowej w armiach państw członkowskich przez obywateli państw nie natowskich.[226] Żołnierze ci, określani jako asymilowani żołnierze sił zbrojnych podlegają ogólnym procedurom, obowiązującym w państwach członkowskich. Innym ciekawym rozwiązaniem, ustanowionym przez politykę bezpieczeństwa NATO jest możliwość akceptacji przez Krajową Władzę Bezpieczeństwa państwa NATO dostępu do informacji niejawnych, do poziomu

[226] Dotyczy to takich kategorii obywateli Wielkiej Brytanii, USA i Kanady jak „obywatele Królestwa" *(ang. Nationals of a Kingdom)*, obywatele Państwa *(ang. Citizens of a State)*, przybyli do Kanady imigranci *(ang. Landed immigrants in Canada)*.

SECRET *(z włączeniem informacji atomowych i specjalnych kategorii)* obywatelom niektórych państw nie natowskich, którzy są zatrudnieni przez rząd bądź przedsiębiorcę kraju NATO[227]. Dostęp do informacji może być zapewniony jedynie w czasie trwania kontraktu lub wykonywania konkretnego zadania bądź operacji.

Polskie rozwiązania przewidują, iż dostępu do informacji niejawnych, stanowiących tajemnicę państwową nie mogą mieć obywatele nie posiadający obywatelstwa polskiego[228]. Jednakże Ustawa o ochronie informacji niejawnych nie określa prawa do dostępu do informacji niejawnych w wypadku posiadania podwójnego obywatelstwa, z których jedno jest na przykład państwa nie natowskiego. Nie określa też zasad udostępniania informacji, stanowiących tajemnicę służbową. W każdym szczególnym przypadku i wątpliwości w tym zakresie niezbędna jest analiza i ocena prawna.

Zatrudnianie osób wymagających dostępu do informacji niejawnych na okres wstępny.

Zgodnie z przepisami NATO możliwe jest udostępnianie informacji niejawnych i zatrudnianie osób, które nie posiadają PERSONNEL SECURITY CLEARANCE CERTIFICATE do wymaganej klauzuli tajności. Zatrudnienie może nastąpić pod następującymi warunkami: posiadanie PERSONNEL SECURITY CLEARANCE CERTIFICATE, upoważniającego do dostępu do informacji o niższej klauzuli niż wymagane, wystąpienie z wnioskiem o przeprowadzenie postępowania w celu przyznania wymaganego certyfikatu, brak informacji świadczących, że dana osoba naruszyła przepisy o ochronie informacji niejawnych oraz akceptacja przez Krajową Władzę Bezpieczeństwa zatrudnienia danej osoby. Praca w tych warunkach nie powinna trwać dłużej niż 6 miesięcy a za aprobatą Krajowej Władzy Bezpieczeństwa zezwolenie może być przedłużone pod warunkiem, że rozpoczęło się postępowanie sprawdzające.

---

[227] Na obecnej liście, zaaprobowanej przez Komitet Bezpieczeństwa NATO znajdują się: Australia, Austria, Finlandia, Irlandia, Nowa Zelandia, Szwecja, Szwajcaria. Lista ta, w razie potrzeby może być uaktualniana.

[228] Ograniczenie to nie dotyczy obywateli innego państwa, wymagających dostępu do informacji niejawnych w związku z realizacją kontraktów niejawnych.

Polskie normy nie przewidują takich sytuacji. Posiadanie poświadczenia nie jest bezwzględnym warunkiem zatrudnienia na stanowisku, wymagającym dostępu do informacji niejawnych. Jednakże obowiązkiem kierownika jednostki organizacyjnej jest takie zorganizowanie warunków pracy, aby do czasu uzyskania poświadczenia bezpieczeństwa zatrudniona osoba nie miała dostępu do informacji niejawnych.

Jednorazowy dostęp do informacji niejawnych.

Jeżeli dostęp do informacji niejawnych, zgodnie z zasadami upoważniania do jednorazowego dostępu jest wymagany po raz kolejny bądź na okres dłuższy niż 6 miesięcy wymagane jest bezwzględnie właściwe poświadczenie bezpieczeństwa. Wszelkie upoważnienia do dostępu do informacji niejawnych w tym trybie muszą być rejestrowane.

Polskie przepisy nie regulują tak szczegółowo tych zasad a uprawnione osoby upoważniają do zapoznawania się z informacjami niejawnymi, wyłącznie na zasadzie jednorazowego dostępu.

2. Stosowanie fizycznych środków ochrony informacji niejawnych.

Zasady fizycznej ochrony informacji niejawnych ustanowione przez politykę bezpieczeństwa NATO, w większości znajdują odzwierciedlenie w naszych, narodowych regulacjach.

Do różnic, które można też określić niuansami, w sferze bezpieczeństwa fizycznego pomiędzy rozwiązaniami oferowanymi w dokumentach normatywnych NATO a naszymi rodzimymi przepisami należą:

Stosowanie technicznych środków ochrony fizycznej.

W przepisach Sojuszu zalecane jest stosowanie technicznych środków ochrony fizycznej, takich jak telewizja przemysłowa czy systemy wykrywania ruchu. W praktyce, zalecenia te znajdują wyraz w stosowaniu coraz bardziej skomplikowanych urządzeń, które zastępują pracę strażnika czy wartownika.

Asumpt do wprowadzania coraz nowszych rozwiązań w tej dziedzinie dały też tragiczne wydarzenia, związane z terrorystycznym zamachem na Stany Zjednoczone, we wrześniu 2001 roku. Obecnie, w cywilnych i wojskowych strukturach Paktu wszechobecne są systemy monitoringu, wykrywacze metalu, elektroniczne przepustki, elektronicznie kodowany dostęp do urządzeń, na których przetwarzane są informacje niejawne.

Polskie regulacje nie zobowiązują bezwarunkowo do stosowania skomplikowanych urządzeń technicznych. Jednakże zalecają ich wprowadzanie, bowiem systemy te są doskonalsze od ludzkich oczu, zapewniają ciągły nadzór nad najbardziej chronionymi obiektami czy pomieszczeniami i reakcję ochrony lub wartowników w krótkim czasie na wtargnięcie do obiektu osób niepożądanych a także wpływają pozytywnie na pracę osób odpowiedzialnych bezpośrednio za ochronę informacji niejawnych w jednostce organizacyjnej. W połączeniu z pracą ochrony i patrolowaniem dają niemal całkowitą pewność, iż informacje niejawne są należycie chronione. Zdawać sobie należy sprawę z tego, iż wprowadzenie technicznych środków ochrony fizycznej jest bardzo kosztowne. Tylko największe firmy są w stanie wyposażyć swoje obiekty w kosztujące miliony złotych urządzenia. Trudniej jest o nie w jednostkach organizacyjnych sfery budżetowej, w tym w obiektach ministerstwa obrony narodowej. Jednakże przyszłość bezpieczeństwa fizycznego to skomplikowana technika zastępująca pracę pionu ochrony.

Kontrola kluczy i kombinacji zamków.

Minimalne wymogi bezpieczeństwa fizycznego określają, iż klucze, kombinacje oraz koperty z zapisem kombinacji do obiektów i pomieszczeń, w których przechowywane są informacje niejawne muszą być chronione w taki sam sposób jak informacje niejawne. Kombinacje szyfrowe muszą być obligatoryjnie zmieniane w odstępach czasowych, nie przekraczających 12 miesięcy.

Polskie normy, w jednostkach organizacyjnych resortu obrony narodowej nie ustanawiają obowiązku ochrony kluczy i kombinacji szyfrowych na takim samym

poziomie jak chronione są informacje, do których umożliwiają dostęp. Jednakże skracają okres zmiany kombinacji szyfrowych do 6 miesięcy.

Wymagania w zakresie bezpieczeństwa fizycznego obiektów.

Polityka bezpieczeństwa NATO definiuje obowiązek określania wymagań w zakresie bezpieczeństwa fizycznego obiektów, w których mają być przechowywane informacje niejawne na etapie ich budowy.

Jest to generalny zapis, który zmaterializował się w polskich, szczegółowych przepisach, stanowiących, iż służby ochrony państwa są zobowiązane do opiniowania budowy obiektów już w fazie projektowania, kiedy opracowywane są tzw. plany organizacyjno – użytkowe. Jest to interesujące rozwiązanie, które pozwala na wyrażenie opinii Krajowej Władzy Bezpieczeństwa na początkowym etapie przygotowywania się jednostki organizacyjnej do otrzymywania, przetwarzania i przechowywania informacji niejawnych. Dzięki niemu jednostka organizacyjna czy przedsiębiorca znając obowiązujące wymogi unika ponoszenia kosztów w przyszłości gdyby w procesie na przykład certyfikacji pomieszczeń, systemów lub sieci teleinformatycznych okazało się, iż wybudowane obiekty nie spełniają wymogów, określonych przez Krajową Władzę Bezpieczeństwa.

3. Wytwarzanie, obieg i niszczenie dokumentów niejawnych.

W zasadzie standardy polityki bezpieczeństwa NATO w odniesieniu do zasad wytwarzania dokumentu klasyfikowanego, jego rejestrowania, przesyłania, kontrolowania, archiwizowania i niszczenia znajdują odzwierciedlenie w naszych, narodowych regulacjach. Do różnic w tym zakresie należą:

Klauzule tajności dokumentów niejawnych.

Zalecanym standardem natowskim są cztery poziomy klauzul tajności. Podział taki został wprowadzony również w Polsce. Są jednak państwa, które nie ustanowiły w swych narodowych rozwiązaniach klauzuli RESTRICTED. Należą do nich na przykład Stany Zjednoczone. Oczywiście jest to suwerenna decyzja

każdego państwa członkowskiego i władz bezpieczeństwa tego kraju. Problem rodzi się dopiero wówczas, gdy istnieje potrzeba przekazanie temu krajowi konkretnej informacji oznaczonej klauzulą RESTRICTED. Przepisy natowskie nie precyzują, jakie procedury powinny obowiązywać w takiej sytuacji. Biuro Bezpieczeństwa NATO zaleca w tego typu przypadkach traktowanie informacji RESTRICTED zgodnie z zasadami, jakie są ustanowione dla informacji o poziomie wyższym a więc CONFIDENTIAL.

Określenie, jakim informacjom należy nadawać konkretną klauzulę tajności.

Normy bezpieczeństwa informacji, określając jakie klauzule tajności obowiązują w NATO, nie wprowadzają wykazów rodzajów informacji, którym powinna być przypisana konkretna klauzula tajności. Stosowana jest generalna zasada odpowiedzialności wykonawcy za nadaną dokumentowi klauzulę tajności.

W polskich przepisach zasada ta jest również dominującą. Jednak w odniesieniu do informacji, stanowiących tajemnicę państwową ustawodawca zdecydował o umieszczeniu w Załączniku do Ustawy o ochronie informacji niejawnych wykazu, ułatwiającego wykonawcy nadanie właściwej klauzuli tajności. Przyznać trzeba, że wykaz taki jest bardzo pomocny.

Przechowywanie i okresowa weryfikacja informacji niejawnych.

Zgodnie z polityką bezpieczeństwa NATO, minimalnym i w zasadzie jedynym wymogiem w zakresie zasadności utrzymywania klauzuli COSMIC TOP SECRET, przyznanej konkretnemu dokumentowi jest konieczność weryfikacji tej klauzuli nie rzadziej, niż co 5 o ile wykonawca nie określił, iż będzie ona automatycznie obniżona po 2 latach.

Polskie przepisy są w tym względzie bardzo szczegółowe i stosunkowo rygorystyczne, stanowiąc, iż informacje stanowiące tajemnicę państwową podlegają ochronie przez okres 50 lat od daty ich wytworzenia a niektóre nawet bez względu na upływ czasu. Dopiero po upływie 20 lat Rada Ministrów może określić, w drodze rozporządzenia, które spośród informacji niejawnych oznaczonych klauzulą

TAJNE przestały stanowić tajemnicę państwową. Równie szczegółowo ustawa określa czasokres przechowywania informacji stanowiących tajemnicę służbową.

Zasady przechowywania informacji niejawnych.

Interpretując standardy natowskie można przyjąć, iż kancelarie ustanawia się tam, gdzie istnieje konieczność przechowywania informacji niejawnych o klauzulach COSMIC TOP SECRET i SECRET. Zasady wytwarzania dokumentu klasyfikowanego, jego rejestrowania, przesyłania, kontrolowania, archiwizowania i niszczenia odnoszą się bowiem do informacji o tych klauzulach. Szczegółowe rozwiązania w zakresie rejestrowania dokumentów o niższych klauzulach pozostawia się w gestii krajowych władz bezpieczeństwa państw członkowskich. W praktyce funkcjonowania cywilnych i wojskowych organów NATO oznacza to, iż dokumenty CONFIDENTIAL i RESTRICTED nie podlegają rejestracji. Osoby wytwarzające tego typu dokumenty jak również ci, którzy je otrzymują są odpowiedzialne za właściwą ich ochronę i uniemożliwienie przekazania informacji niejawnych osobom nieuprawnionym *(nie mającym stosownego PERSONNEL SECURITY CLEARANCE CERTIFICATE bądź potrzeby wiedzy).* Dokumenty o klauzuli RESTRICTED są przechowywane na przykład w zamykanym na klucz biurku, szufladzie lub szafce.

Rozwiązania polskie stanowią, iż kancelarie tajne tworzy się w jednostkach organizacyjnych, w których występują dokumenty zawierające informacje niejawne o klauzuli POUFNE lub stanowiące tajemnicę państwową. W rezultacie, w polskim systemie kancelaryjnym rejestruje się ogromną ilość dokumentów a ponieważ czas ich przechowywania jest również dłuższy często nasze rodzime kancelarie są przepełnione a ich personel bardzo zajęty.

Okresowe kontrole dokumentów niejawnych.

Polityka bezpieczeństwa NATO określa, iż przynajmniej raz do roku musi się odbywać kontrola dokumentów niejawnych o klauzuli COSMIC TOP SECRET, polegająca na spisie z natury posiadanych przez kancelarie dokumentów. Jest to

jedyny minimalny wymóg, w dodatku odnoszący się tylko do dokumentów o najwyższej klauzuli tajności.

Nasze przepisy wprowadzają w tym zakresie system kontroli, zapewniający cykliczny nadzór nad wszystkimi informacjami klasyfikowanymi, niezależnie od klauzuli tajności. Obligatoryjne są kontrole roczne, prowadzone w każdej jednostce organizacyjnej, oprócz nich odbywają się również półroczne, bieżące i wyrywkowe.

Zasady niszczenia dokumentów niejawnych.

Regulacje bezpieczeństwa informacji stanowią, iż powinien istnieć system nadzoru i oceny pozwalający na niszczenie nieaktualnych bądź niepotrzebnych dokumentów niejawnych. Protokoły zniszczeń dokumentów COSMIC TOP SECRET powinny być przechowywane przez 10 lat a NATO SECRET przez 5 lat. Nie jest wymagane przechowywanie takich protokołów w odniesieniu do dokumentów o niższych klauzulach tajności.

Polskie normy, obowiązujące w Siłach Zbrojnych ustanawiają szczegółowe regulacje w tym zakresie włącznie z tym, ile osób powinno uczestniczyć w komisyjnym niszczeniu dokumentów niejawnych. Niszczenie dokumentów odbywa się w trakcie rocznej kontroli stanu ochrony informacji niejawnych bądź dokonywane jest przez personel kancelarii i wykonawcę. Protokoły zniszczenia wszystkich dokumentów niejawnych podlegają archiwizacji.

4. Prowadzenie postępowań sprawdzających przed wydaniem świadectwa bezpieczeństwa przemysłowego.

Klauzula tajności kontraktu niejawnego.

Zgodnie z polityką bezpieczeństwa NATO, FACILITY SECURITY CLEARANCE CERTIFICATE jest wymagany, jeśli z realizacją kontraktu wiąże się konieczność udostępnienia firmie informacji niejawnych o klauzuli CONFIDENTIAL i wyższej. Przepisy natowskie dopuszczają też możliwość obniżenia tej granicy do poziomu RESTRICTED, jeśli tak stanowią przepisy narodowe.

W polskich rozwiązaniach, jeśli realizacja prac czy umowy na rzecz obronności łączy się z dostępem do informacji niejawnych, stanowiących tajemnicę państwową obowiązkowo wykonawca musi posiadać świadectwo bezpieczeństwa przemysłowego. Regulacje te nie mają zastosowania przy realizacji kontraktów natowskich, a więc realizowanych z funduszu inwestycyjnego Sojuszu oraz umów na rzecz innych państw lub organizacji międzynarodowych, w których obowiązują przepisy analogiczne do ustanowionych przez NATO.

Wykonawca i podwykonawca kontraktu niejawnego.

Zasady bezpieczeństwa przemysłowego NATO dużo uwagi poświęcają mechanizmom realizacji kontraktów niejawnych. Przewidują możliwość zawierania kontraktu z wykonawcą głównym, który może zlecać jego realizację w całości bądź częściowo podwykonawcom, którzy są z kolei upoważnieni do zawierania umów z innymi firmami. Wszystkie zaangażowane w realizację umów firmy obowiązują jednak te same wymogi odnośnie posiadania FACILITY SECURITY CLEARANCE CERTIFICATE. Prawdopodobnie zapisy te są konsekwencją realizacji kontraktów niejawnych przez spółki z kapitałem zagranicznym, międzynarodowe konsorcja, zrzeszające zarówno firmy z krajów natowskich jak i przez przedsiębiorców, zarejestrowanych w państwach nie należących do Sojuszu.

Pierwotna wersja Ustawy o ochronie informacji niejawnych w ogóle nie definiowała pojęcia podwykonawcy, co sprawiało szereg trudności interpretacyjnych. Dopiero w jej znowelizowanej postaci, w 2001 roku, pojawił się enigmatyczny zapis dopuszczający potrzebę zawarcia umowy z podwykonawcą przez przedsiębiorcę bądź jednostkę naukowo-badawczą realizujących kontrakt, związany z dostępem do informacji niejawnych, stanowiących tajemnicę państwową.

Świadectwo bezpieczeństwa przemysłowego.

Warunkiem uczestnictwa w konkursie ofert, negocjacjach i późniejszej realizacji kontraktu o klauzuli CONFIDENTIAL i wyższej jest wydanie FACILITY SECURITY CLEARANCE CERTIFICATE przez Krajową Władzę

Bezpieczeństwa kraju, w którym firma jest zarejestrowana i posiada osobowość prawną. Dodatkowo pracownicy firmy muszą otrzymać wymagane PERSONNEL SECURITY CLEARANCE CERTIFICATES i zostać przeszkoleni w zakresie procedur bezpieczeństwa obowiązujących w NATO. Są to generalne standardy, ustanowione przez politykę bezpieczeństwa NATO. Jednakże, w odniesieniu do kontraktów o klauzuli RESTRICTED, realizowanych w państwach, które wymagają posiadania świadectwa bezpieczeństwa przemysłowego, dopuszczalne jest przystąpienie przez przedsiębiorcę do konkursu ofert nawet wówczas gdy nie posiada on FACILITY SECURITY CLEARANCE CERTIFICATE, bowiem w kraju, w którym jest zarejestrowany nie jest to wymagane. Warunkiem, w tej szczególnej sytuacji jest poinformowanie ewentualnego, przyszłego wykonawcy o obowiązkach w zakresie ochrony informacji niejawnych i potwierdzenie ich znajomości.

Nasze przepisy narodowe nie wprowadzają regulacji tego typu, chociaż będą musiały je uwzględniać przy realizacji kontraktów o klauzuli RESTRICTED przez polskich przedsiębiorców w innych krajach natowskich.

Czas ważności świadectwa bezpieczeństwa przemysłowego.

Zgodnie z zasadami polityki bezpieczeństwa NATO, FACILITY SECURITY CLEARANCE CERTIFICATE jest wydawany przez krajowe władze bezpieczeństwa państw natowskich na określony czas. Wewnętrzną sprawą każdego państwa natowskiego jest jak długi jest to okres.

Natomiast w Polsce świadectwo bezpieczeństwa przemysłowego wydawane jest do konkretnej umowy, związanej z dostępem do informacji niejawnych lub konkretnego zadania na rzecz obronności i bezpieczeństwa państwa. W praktyce często się zdarza, iż ten sam przedsiębiorca ubiega się, w tym samym czasie bądź w krótkich odstępach czasu o kilka świadectw bezpieczeństwa przemysłowego, przekazując w kwestionariuszu bezpieczeństwa przemysłowego niemal te same dane dotyczące zwłaszcza zdolności przedsiębiorstwa do należytej ochrony informacji niejawnych. Dodatkowo, ponosi koszty związane z przeprowadzeniem

postępowania i wydaniem świadectwa bezpieczeństwa przemysłowego. Wydaje się, iż rozwiązania natowskie w tym zakresie są bardziej praktyczne.

5. Ochrona informacji niejawnych w systemach i sieciach teleinformatycznych.

W NATO problematykę bezpieczeństwa teleinformatycznego reguluje szereg dokumentów w formie wytycznych, instrukcji i szczegółowych przewodników. Wiele z tych dokumentów oznaczonych jest klauzulą tajności. Przyczyną takiego stanu rzeczy jest fakt, iż w lokalnych i rozległych sieciach teleinformatycznych przetwarzana i przekazywana jest olbrzymia ilość informacji niejawnych, często są one szyfrowane przy przesyłaniu na znaczne odległości. Wiedza na temat ich funkcjonowania i zasad utrzymania jest również informacją niejawną. Ponadto, w Sojuszu bezpieczeństwo teleinformatyczne jest pojęciem bardzo szerokim, zawierającym elementy bezpieczeństwa fizycznego, osobowego czy bezpieczeństwa informacji.

Należy podkreślić, iż w polskich przepisach, nie wszystkie natowskie standardy bezpieczeństwa teleinformatycznego znajdują swoje odzwierciedlenie. Wiele z dokumentów obowiązujących w NATO jest sukcesywnie implementowanych do polskich rozwiązań wraz z postępującym rozwojem technik komputerowych i zaopatrywaniem Sił Zbrojnych RP w odpowiedni sprzęt. Do różnic pomiędzy polskimi standardami i natowską polityką bezpieczeństwa należą:

Jakość stosowanych komputerów.

W cywilnych i wojskowych organach Sojuszu powszechnie stosowane są komputery klasy TEMPEST, pozwalające na wytwarzanie i przesyłanie informacji do poziomu NATO SECRET. Umożliwia to natychmiastową transmisję niejawnych danych do różnych punktów dowodzenia i ośrodków decyzyjnych. W praktyce wygląda to tak, iż najpierw dokument niejawny przesyłany jest elektronicznie, aby osoby funkcyjne mogły podejmować natychmiastowe działania a dopiero potem

dostarczany jest w formie pisemnej *(ang. hard copy)* celem dokumentowania prowadzonych działań.

W naszych rodzimych rozwiązaniach taki system funkcjonowania, w związku z małą ilością odpowiednich komputerów, ograniczających emisję ujawniającą jeszcze raczkuje. Powszechnie stosowane są specjalne kabiny[229], w których umieszczane są komputery, dostępne na rynku. Wytwarzanie dokumentów niejawnych z wykorzystaniem wolnostojących stanowisk komputerowych jest w Siłach Zbrojnych RP zabronione.

Lista preferowanego sprzętu i oprogramowania.

O znaczeniu bezpieczeństwa teleinformatycznego świadczą, opracowywane i cyklicznie uaktualniane w NATO, listy sprzętu teleinformatycznego i oprogramowania komputerowego, które zostały sprawdzone i ocenione jako bezpieczne. Jednocześnie są zalecane do użytku w cywilnych i wojskowych organach NATO oraz państwach członkowskich.

Do tej pory nie ma listy tego typu w Siłach Zbrojnych RP. Jednakże wraz z postępującym procesem certyfikacji, prowadzonej przez Jednostkę Certyfikującą Wyroby w WSI należy się liczyć w przyszłości z zasadnością opracowania listy bezpiecznych lub rekomendowanych produktów komputerowych na potrzeby resortu obrony narodowej.

Eksploatacja systemów i sieci komputerowych.

Do przesyłania informacji niejawnych w NATO stosowane są rozległe, niejawne systemy sieciowe, umożliwiające bezpieczne przesyłanie informacji na olbrzymie odległości, do dowództw strategicznych czy regionalnych.[230]

Możliwości techniczne sprawiają, iż w naszej armii, na razie stosowane są pojedyncze systemy teleinformatyczne w jednostkach wojskowych czy dowództwach oraz małe sieci lokalne. Niewątpliwie będzie następował postęp w tej

---

[229] Chodzi tutaj o Bezpieczne Stanowiska Komputerowe, ograniczające emisję ujawniającą komputerów.

[230] Dowództwami strategicznymi w NATO są Dowództwo NATO w Europie *(ang. Allied Command Europe),* stacjonujące w Belgii i Dowództwo NATO w strefie atlantyckiej *(ang. Allied Command Atlantic),* stacjonujące w USA. Podlegają im dowództwa regionalne, w Europie stacjonujące w Holandii i we Włoszech a w strefie atlantyckiej w Wielkiej Brytanii, USA i Portugalii.

dziedzinie, choćby w celach zapewnienia przepływu informacji pomiędzy strukturami wojskowymi NATO a naszymi jednostkami wojskowymi, wyznaczonymi do wspólnych działań operacyjnych.

Akredytacja systemów i sieci teleinformatycznych.

W NATO każdy system lub sieć teleinformatyczna, przeznaczone do przetwarzania informacji niejawnych, niezależnie od ich klauzuli podlegają akredytacji.

Podobnie jest w naszym kraju, gdzie podstawą akredytacji są opracowane dla systemu lub sieci teleinformatycznej szczególne wymagania bezpieczeństwa. Niewielką różnicą jest możliwość tymczasowej akredytacji w przypadku systemów natowskich, podczas gdy nasze narodowe przepisy nie przewidują takiej możliwości. Pełna akredytacja systemu przez Krajową Władzę Bezpieczeństwa jest bezwzględnym warunkiem przetwarzania informacji niejawnych, stanowiących tajemnicę państwową. W przypadku tajemnicy służbowej, w Polsce podobnie jak w NATO rozpoczęcie eksploatacji systemu następuje na podstawie oceny szczególnych wymagań bezpieczeństwa.

Odpowiedzialność za bezpieczeństwo systemów i sieci teleinformatycznych.

Stosownie do narodowych regulacji za bezpieczeństwo informacji przetwarzanych w sieciach systemach teleinformatycznych oraz za bezpieczeństwo tych systemów odpowiadają kierownik jednostki organizacyjnej, administrator systemu lub sieci teleinformatycznej oraz inspektor bezpieczeństwa teleinformatycznego. Według obecnego stanu wymienione osoby funkcyjne gwarantują właściwy nadzór w tej dziedzinie.

Wraz z rozbudową sieci i systemów należy się będzie liczyć z koniecznością wyznaczania dodatkowych osób funkcyjnych, które odpowiadają za bezpieczeństwo teleinformatyczne w NATO. Należeć będą do nich oficerowie bezpieczeństwa do spraw TEMPEST, Transmisji Informacji *(jeśli zachodzi konieczność transmisji informacji na odległość)*, Bezpieczeństwa Sprzętu Kryptograficznego *(jeśli przewidywane jest wykorzystywanie środków*

kryptograficznych), Bezpieczeństwa Zdalnego Terminala *(w przypadku rozległych sieci ze zdalnymi terminalami)*. Funkcje tego typu pełnią w zależności od potrzeb oficerowie, odpowiadający za bezpieczeństwo teleinformatyczne w strukturach natowskich.

UWAGI KOŃCOWE

System ochrony informacji niejawnych w Polsce, w tym w Siłach Zbrojnych RP ma solidne podstawy prawne i jest kompatybilny zarówno w sferze normatywnej jak i organizacyjnej ze standardami, ustanowionymi przez politykę bezpieczeństwa NATO. Inaczej być nie może, ponieważ członkostwo w największym pakcie polityczno – militarnym współczesnego świata zobowiązuje do przestrzegania norm, wymogów i zasad, obowiązujących wszystkie państwa – Strony Traktatu Północnoatlantyckiego.

Jednakże, Polska jest nadal obok Węgier i Czech państwem o najkrótszym stażu w NATO. Zrozumiałym jest więc, iż porównanie poziomu ochrony informacji niejawnych w naszym kraju do tych, które są ustanowione w państwach i armiach funkcjonujących w Pakcie od wielu lat wypada często na naszą niekorzyść. Nawet, jeśli możemy mówić o zgodności dokumentów normatywnych, obowiązujących w naszym kraju i w innych państwach NATO to jeszcze przez wiele lat będziemy musieli się uczyć tak zwanej kultury wykonawczej lub jak to jest określane w NATO kultury bezpieczeństwa *(ang. Security Culture)*. Pojęcie to jest używane dla określenia wewnętrznej dyscypliny, świadomości każdego wykonawcy dokumentu niejawnego i każdej osoby, która w swej działalności ma do czynienia z narodowymi i sojuszniczymi informacjami niejawnymi jak należy z nimi postępować. Zgodnie z interpretacją natowskiej polityki bezpieczeństwa właściwe postępowanie z dokumentami, oznaczonymi klauzulą tajności i ciągłe uwzględnianie możliwych zagrożeń dla ich poufności musi stać się wewnętrznym nawykiem każdej, upoważnionej do wytwarzania i posiadania takich dokumentów osoby.

Innym problemem, rzutującym na efektywność i sprawność naszego systemu ochrony informacji niejawnych są możliwości budżetowe i techniczne. Stosowanie nowoczesnych systemów zastępujących ludzkie zmysły jest bardzo kosztowne. W ostatecznym rozrachunku wydatki poniesione na ochronę informacji niejawnych

zwracają się w dwójnasób. Jednak desygnowanie dużych środków na zaawansowane technologie i systemy monitoringu, w krótkim czasie, zwłaszcza w jednostkach organizacyjnych sfery budżetowej, jest bardzo trudne.

Polska i jej Siły Zbrojne są na dobrej drodze do jasno sprecyzowanego celu – ustanowienia standardów bezpieczeństwa informacji niejawnych na poziomie gwarantującym ich pełną ochronę. Jednak szczegółowa analiza naszych narodowych przepisów i norm ustanowionych przez politykę bezpieczeństwa NATO pozwala na stwierdzenie, iż zbliżenie narodowych do sojuszniczych rozwiązań mogłoby być szybsze, bez szkody dla poziomu ochrony informacji niejawnych. Uzasadnionym byłoby dokonanie korekt przepisów o ochronie informacji niejawnych jak również wprowadzenie nowych regulacji, aby system mógł działać sprawniej. Ponadto niektóre rozwiązania są bardzo restrykcyjne i mogą być w NATO oceniane jako nieco anachroniczne. Często polskie normy zmuszają do prowadzenia postępowań i wprowadzenia mechanizmów, które w Sojuszu nie są w ogóle wymagane.

Uwzględniając dotychczasowe doświadczenia, ocenę funkcjonowania i kierunki ewolucji systemu ochrony informacji niejawnych w Polsce, w tym w Siłach Zbrojnych w ciągu ostatnich czterech lat, celowym jest rozpatrzenie zasadności wprowadzenia wyszczególnionych poniżej, zarówno generalnych regulacji jak i szczegółowych zmian w Ustawie o ochronie informacji niejawnych. Zmiany te oczywiście wpłynęłyby bezpośrednio na regulacje zawarte w aktach wykonawczych, w tym w odniesieniu do sfery obronności i Sił Zbrojnych RP w stosownych zarządzeniach i decyzjach ministra obrony narodowej oraz w dokumentach wydanych przez szefa Wojskowych Służb Informacyjnych. Proponowane zmiany powinny obejmować:

- Rozszerzenie podmiotów, wobec których mają zastosowanie przepisy analizowanej ustawy o jednostki organizacyjne, podległe ministrowi obrony narodowej i przez niego nadzorowane. Obecnie, ustawa ogranicza się do Sił Zbrojnych RP i ich jednostek organizacyjnych. Uzasadnionym byłoby jasne sprecyzowanie, iż przepisy o ochronie informacji niejawnych stosuje się też wobec innych jednostek organizacyjnych,

takich jak spółki skarbu państwa, dla których minister obrony narodowej jest organem założycielskim. Zlikwidowałoby to trudności interpretacyjne służb ochrony państwa, która z nich jest właściwą do prowadzenia, określonych w ustawie postępowań wobec tych spółek i ich pracowników oraz pewną lukę, w której pozostają firmy naszego przemysłu obronnego.

- Zobowiązanie służb ochrony państwa do prowadzenia kontroli niezależnie od poziomu przechowywanych w jednostce organizacyjnej dokumentów niejawnych. Obecnie Agencja Bezpieczeństwa Wewnętrznego i Wojskowe Służby Informacyjne są uprawnione do kontroli stanu zabezpieczenia informacji niejawnych, stanowiących tajemnice państwową. Służby ochrony państwa powinny mieć również obowiązek kontroli stanu zabezpieczenia informacji niejawnych, stanowiących tajemnicę służbową, co z jednej strony zmusiłoby kierowników jednostek organizacyjnych do dbałości o system ochrony informacji w podległych strukturach jednostki organizacyjnej a z drugiej pozwoliłoby służbie ochrony państwa na pełną ocenę stanu zabezpieczenia informacji niejawnych, w pozostających w ich kompetencjach jednostkach organizacyjnych.
- Uprawnienie służb ochrony państwa do kontroli prawidłowości prowadzonych przez pełnomocników zwykłych postępowań sprawdzających, przed wydaniem poświadczenia bezpieczeństwa osobowego. Obecnie służby ochrony państwa, właściwe do kontroli ochrony informacji niejawnych oraz kontroli przestrzegania przepisów w tym zakresie, nie mają jasno sprecyzowanego prawa do kontroli akt postępowania sprawdzającego. Zapis ustawowy o uprawnieniu do prowadzenia kontroli jest nieco ogólny i różnie interpretowany. W związku z tym należałoby rozpatrzyć możliwość wprowadzenia regulacji, uprawniającej służby ochrony państwa do prowadzenia takich kontroli. Sprawdzenie wszystkich aspektów ochrony informacji niejawnych, w tym działalności pełnomocnika, bez skontrolowania teczki postępowania

sprawdzającego nie daje bowiem pełnego obrazu jego funkcjonowania w jednostce organizacyjnej.

- Uprawnienie bądź zobowiązanie kierownika jednostki organizacyjnej do opracowywania wykazu rodzajów informacji niejawnych, stanowiących tajemnicę służbową. Ustawa ustanawia klauzule tajności wytwarzanych dokumentów niejawnych i określa w załączniku, jakie rodzaje informacji należy zaliczyć do stanowiących tajemnicę państwową i przyznać im klauzulę TAJNE bądź ŚCIŚLE TAJNE. Nie ma natomiast, poza ogólnym określeniem definicji informacji o klauzuli POUFNE i ZASTRZEŻONE wyszczególnienia, jaka konkretnie informacja jest POUFNĄ a jaka może być już zaklasyfikowana jako ZASTRZEŻONA. Oczywiście opracowanie takiej listy i umieszczenie jej w dokumencie o randze ustawy jest zbyteczne a nawet trudne do realizacji. Jednakże w celu ułatwienia wykonawcom konkretnej jednostki organizacyjnej, realizującej zadania w konkretnej dziedzinie, celowym byłoby nadanie kierownikowi tej jednostki uprawnień bądź obowiązku opracowania na wewnętrzne potrzeby swych pracowników wykazu rodzajów informacji, stanowiących tajemnicę służbową.
- Wprowadzenie obowiązku szkolenia osób, wobec których nie prowadzi się postępowania sprawdzającego. Ustawa zwalnia z obowiązku prowadzenia postępowania sprawdzającego wobec osób sprawujących najwyższe funkcje państwowe takie jak Prezydent RP czy członkowie Rady Ministrów. Pomimo tego, że są to osoby, sprawujące najwyższe urzędy w państwie powinny być jednak przeszkolone przez Agencję Bezpieczeństwa Wewnętrznego w zakresie przepisów o ochronie informacji niejawnych bądź zadeklarować znajomość takich przepisów. Celowym byłoby również rozszerzenie grona osób, wobec których nie jest wymagane prowadzenie postępowania sprawdzającego o pracowników wymiaru sprawiedliwości a zwłaszcza sędziów i prokuratorów. Powinni oni jedynie podlegać obowiązkowi przeszkolenia w sferze ochrony informacji niejawnych. Byłoby to zgodne z zasadami

funkcjonowania demokratycznego państwa, w którym organy władzy sądowniczej są niezależne a sędziowie orzekając niezawiśli.

- Wprowadzenie alternatywnych sposobów zakończenia postępowania sprawdzającego. Zasadą ustawową jest, że postępowanie sprawdzające wobec osób kończy się wydaniem poświadczenia bezpieczeństwa lub odmową jego wydania. Nie są natomiast uregulowane prawnie sytuacje, w których kontynuowanie postępowania jest niewskazane. Dotyczy to śmierci osoby sprawdzanej, rezygnacji z ubiegania się o wyznaczenie na stanowisko, związane z dostępem do informacji niejawnych bądź rezygnacji kierownika jednostki organizacyjnej z planów zatrudnienia osoby, wobec której postępowanie zostało już wszczęte. W takich przypadkach dopuszczalna jest interpretacja służb ochrony państwa, wskazująca na ustanie przyczyn prawnych, dla których postępowanie sprawdzające zostało wszczęte. Biorąc pod uwagę realną możliwość odwoływania się osób sprawdzanych od tego typu decyzji, uzasadnionym jest wprowadzenie normy prawnej, takiej jak zaprzestanie prowadzenia postępowania, odstąpienie od jego prowadzenia bądź jego umorzenie.
- Weryfikacja sprawdzanych osób pod kątem naruszenia przez nie przepisów o ochronie informacji niejawnych. Zakres prowadzonych sprawdzeń przed wydaniem poświadczenia bezpieczeństwa osobowego jest stosunkowo szeroki. Odnosi się między innymi do ustalenia czy osoba sprawdzana popełniła przestępstwo, zwłaszcza ścigane z oskarżenia publicznego. Kwestia odpowiedzialności dyscyplinarnej nie jest przedmiotem weryfikacji. Jednakże celowym byłoby sprawdzenie czy osoba poddana procedurze postępowania sprawdzającego naruszyła w przeszłości zasady ochrony informacji niejawnych i poniosła za to określone w przepisach konsekwencje dyscyplinarne. Wiedza na ten temat jest niezwykle istotna w świetle obowiązku określenia czy osoba sprawdzana daje rękojmię zachowania tajemnicy. Dlatego też celowym byłoby uzupełnienie ankiety bezpieczeństwa osobowego o pytania

dotyczące naruszenia w przeszłości przepisów o ochronie informacji niejawnych oraz poniesienia za to dyscyplinarnych konsekwencji.

- Zawieszenie postępowania sprawdzającego. Służby ochrony państwa bądź pełnomocnicy ochrony są zobligowani do sfinalizowania prowadzonych postępowań sprawdzających w ustawowo określonych terminach. Częstokroć jest to niewykonalne nie tylko z uwagi na opóźnienia w realizacji przez inne instytucje państwowe wymaganych sprawdzeń wobec osób objętych postępowaniem, lecz również z uwagi na inne, obiektywne przyczyny. Należą do nich choroba czy dłuższa nieobecność osoby sprawdzanej, co w przypadku kadry zawodowej, uczestniczącej w kursach lub szkoleniach poligonowych jest często spotykane. Inną sytuacją, która może się zdarzyć jest naruszenie prawa i popełnienie przestępstwa umyślnego przez osobę sprawdzaną. Popełnienie tego typu przestępstwa dyskwalifikuje osobę sprawdzaną i uniemożliwia wydanie jej poświadczenia bezpieczeństwa. Cóż ma uczynić prowadzący postępowanie funkcjonariusz służby ochrony państwa lub pełnomocnik ochrony, który wie, iż wobec osoby sprawdzanej toczy się postępowanie karne za przestępstwo umyślne, ścigane z oskarżenia publicznego. Logicznym wydaje się, iż postępowanie mogłoby być przerwane czy zawieszone do czasu orzeczenia wyroku. Dałoby to możliwość właściwej oceny osoby sprawdzanej i usprawiedliwiało nie dochowanie terminów ustawowych, dotyczących czasu, w którym powinno nastąpić sfinalizowanie postępowania sprawdzającego.
- Uprawnienie służb ochrony państwa do prowadzenia zwykłych postępowań sprawdzających. Stosownie do generalnej regulacji służby ochrony państwa prowadzą postępowania sprawdzające wobec osób przed wydaniem poświadczenia bezpieczeństwa osobowego, upoważniającego do dostępu do informacji niejawnych, stanowiących tajemnicę państwową. Co prawda nowelizacja z 2001 roku wprowadziła możliwość prowadzenia zwykłych postępowań sprawdzających wobec

pełnomocników ochrony jednak delegacja ta powinna być rozszerzona i precyzować prawo służb ochrony państwa do prowadzenia postępowania zwykłego wobec pełnomocników ochrony u przedsiębiorców, w jednostkach naukowych i badawczo rozwojowych wówczas, gdy ubiegają się one o realizację kontraktu natowskiego. W takiej sytuacji bowiem świadectwo bezpieczeństwa przemysłowego jest wymagane zgodnie z regulacjami polityki bezpieczeństwa NATO. Innym przykładem jest realizacja zadań na rzecz obronności, które nie wymagają świadectwa bezpieczeństwa przemysłowego, jednak osoby, wykonujące tego typu zadania bądź prace muszą posiadać wydane przez pełnomocnika poświadczenia bezpieczeństwa osobowego. Nieodparcie nasuwa się pytanie, kto w wyszczególnionych wyżej przypadkach przeprowadzi zwykłe postępowanie sprawdzające wobec pełnomocnika i wyda mu poświadczenie do poziomu POUFNE. Jedynym logicznym rozwiązaniem jest sprecyzowanie takich uprawnień dla służb ochrony państwa.

- Upoważnienie pełnomocnika ochrony do wglądu do uprzednio opracowanych akt postępowania sprawdzającego w przypadku prowadzenia ponownej procedury sprawdzającej. Akta postępowań sprawdzających mogą być udostępniane, po zakończeniu postępowania przez pełnomocnika, osobie sprawdzanej, na żądanie sądu i prokuratora w celu ścigania karnego, szefom służb ochrony państwa oraz innym osobom funkcyjnym, które są uprawnione do rozpatrywania odwołania osoby sprawdzanej a także osobie upoważnionej do obsady stanowiska lub służbom ochrony państwa dla celów postępowania sprawdzającego. Delegacja ta wyklucza pełnomocnika ochrony z grona osób, które mają prawo wglądu do akt przeprowadzonego postępowania. Jednakże pełnomocnik ochrony w trakcie prowadzenia kolejnego postępowania powinien mieć prawo wglądu do akt dotyczących osoby, którą sprawdza, na przykład w celu porównania danych, jakie zostały zamieszczone we wcześniej wypełnianej ankiecie bezpieczeństwa osobowego.

- Przedłużenie czasu ważności poświadczeń bezpieczeństwa osobowego. Dotychczasowe regulacje stanowią, iż postępowanie sprawdzające powtarza się:
  / w odniesieniu klauzuli ZASTRZEŻONE i POUFNE - co 10 lat;
  / w odniesieniu do klauzuli TAJNE - co 5 lat;
  / w odniesieniu do klauzuli ŚCIŚLE TAJNE - co 3 lata.

  Biorąc pod uwagę olbrzymią ilość postępowań sprawdzających, prowadzonych zwłaszcza przez służby ochrony państwa, w tym WSI w Siłach Zbrojnych RP, oraz uwzględniając standardy natowskie, stanowiące, że postępowania do poziomu CONFIDENTIAL i SECRET powtarza się co 10 lat a COSMIC TOP SECRET po 5 latach, uzasadnionym jest ustawowe przedłużenie terminów ważności wydanych poświadczeń bezpieczeństwa. Postępowanie przed wydaniem poświadczenia do poziomu ŚCIŚLE TAJNE mogłoby być powtarzane co 5-6 lat a do poziomu TAJNE co 6-8 lat.
- Przedłużenie zalecanego czasu na sfinalizowanie postępowania sprawdzającego. Ustawa stanowi, iż postępowania sprawdzające wobec osób powinny być sfinalizowane;
  / w ciągu miesiąca od daty pisemnego polecenia przeprowadzenia postępowania zwykłego,
  / w ciągu 2 miesięcy od daty złożenia wniosku o przeprowadzenie poszerzonego postępowania sprawdzającego,
  / w ciągu 3 miesięcy od daty złożenia wniosku o przeprowadzenie postępowania specjalnego.

  Terminy te są stosunkowo krótkie i choć ustawa jedynie zaleca ich przestrzeganie to w praktyce dochowanie tych terminów jest bardzo trudne. Biorąc pod uwagę możliwość przedłużenia okresu ważności wydanego poświadczenia bezpieczeństwa osobowego, celowym byłoby przedłużenie okresu, w którym postępowanie powinno być sfinalizowane. Przykładowo, postępowanie zwykłe mogłoby być sfinalizowane w ciągu

2-3 miesięcy, poszerzone w ciągu 4 miesięcy a specjalne w ciągu 5 miesięcy.

- Zobowiązanie negatywnie zweryfikowanej osoby do zwrotu posiadanego poświadczenia bezpieczeństwa. Obecnie brakuje regulacji, określających tryb postępowania w przypadku ujawnienia nowych informacji, wskazujących, że osoba posiadająca poświadczenie bezpieczeństwa nie daje rękojmi zachowania tajemnicy. Pomimo tego, że ustawodawca określił, iż w takich przypadkach służba ochrony państwa bądź pełnomocnik ochrony mogą z urzędu przeprowadzić kolejne postępowanie, jednakże nie sprecyzował, co się dzieje z aktualnie posiadanym poświadczeniem bezpieczeństwa. Jako dokument jawny każdy może się nim dalej posługiwać. Całkowicie uzasadnionym byłoby ustanowienie mechanizmu zmuszającego osobę, której w wyniku kolejnego niejako weryfikującego nowe informacje postępowania, odmówiono wydania poświadczenia bezpieczeństwa, do zwrotu uprzednio wydanego poświadczenia.
- Umożliwienie uznawania certyfikatu dla sieci, systemu teleinformatycznego i urządzenia wydanych przez inną służbę ochrony państwa oraz krajowe władze bezpieczeństwa państw natowskich. Regulacje dotyczące certyfikacji systemów i sieci teleinformatycznych są stosunkowo szczegółowe i odnoszą się do wszystkich aspektów tego procesu. Nierozwiązaną jednak pozostaje sprawa wzajemnego uznawania przez służby ochrony państwa wydanych przez nie certyfikatów. To samo dotyczy certyfikatów, wydanych przez inne krajowe władze bezpieczeństwa państw NATO na urządzenia i narzędzia kryptograficzne, służące do ochrony informacji niejawnych. Ich zastosowanie w Siłach Zbrojnych, zgodnie z dotychczasową praktyką może nastąpić na zasadzie bezwarunkowego uznania przez Jednostkę Certyfikująca WSI wydanego przez inną służbę ochrony państwa certyfikatu bądź jego uznania, po przeanalizowaniu wyników badań, które były podstawą wydania certyfikatu. Czasem wydaje się to zbyteczną nadgorliwością, zwłaszcza

wobec certyfikatów wydanych przez inne państwa natowskie, które przecież w procesie certyfikacji wykorzystują bardziej zaawansowane od naszych rodzimych technologie. Wydaje się, iż celowym byłoby ustanowienie mechanizmu, pozwalającego służbom ochrony państwa na automatyczne, wzajemne uznawanie wydanych certyfikatów.

- Określenie w ustawie możliwości zawierania przez przedsiębiorcę, jednostkę naukowo – badawczą, ubiegających się o realizację umowy, związana z dostępem do informacji niejawnych, stanowiących tajemnicę państwową umów z podwykonawcami. Ustawodawca dosyć enigmatycznie odnosi się do tego problemu, zobowiązując jedynie przedsiębiorcę do uzupełnienia kwestionariusza bezpieczeństwa przemysłowego w sytuacji, gdy pojawia się konieczność zawarcia umowy z podwykonawcą. Należałoby zdefiniować pojęcie podwykonawcy jak również zobowiązać go do przestrzegania przepisów o ochronie informacji niejawnych na takim samym poziomie, do jakiego jest zobowiązany wykonawca umowy. Prawnego uregulowania wymaga również sytuacja, w której realizacją umowy zajmuje się konsorcjum składające się z kilku firm, z których tylko jedna posiada świadectwo bezpieczeństwa przemysłowego, uprawniające do realizacji umowy.
- Odstąpienie od ustawowej zasady jednorazowego wydawania świadectwa bezpieczeństwa przemysłowego do konkretnej umowy lub zadania realizowanego na rzecz obronności i bezpieczeństwa państwa, związanego z dostępem do informacji niejawnych, stanowiących tajemnicę państwową. Praktyką większości państw natowskich jest, iż FACILITY SECURITY CLEARANCE CERTIFICATE wydawany jest na określony czas. W naszych, krajowych warunkach można rozpatrywać różne okresy, na jakie mogłoby być wydawane świadectwo bezpieczeństwa przemysłowego. Być może uzasadnionym byłoby powiązanie czasu ważności świadectwa z okresem ważności poświadczeń bezpieczeństwa, wydanych osobom, zaangażowanym w realizację kontraktu. Inną możliwością jest ograniczenie terminu ważności

świadectwa ostatecznym terminem realizacji umowy, terminem okresu gwarancyjnego na wykonaną pracę bądź okresem obsługi czy serwisowania.

- Upoważnienie służb ochrony państwa do wydawania świadectwa przemysłowego do umów lub zadań, związanych z dostępem do informacji, stanowiących tajemnicę służbową. Uregulowania wymagają zwłaszcza zasady prowadzenia postępowań przed wydaniem świadectwa bezpieczeństwa przemysłowego do kontraktów natowskich. Zgodnie z polityką bezpieczeństwa NATO świadectwa są wymagane od poziomu CONFIDENTIAL.
- Pełne zwolnienie jednostek budżetowych z opłat za wydawanie certyfikatów dla systemów i sieci teleinformatycznych. Obecnie jednostki budżetowe są zwolnione z opłat za przeprowadzenie czynności poprzedzających wydanie certyfikatu, płacą jednak za sam certyfikat. W praktyce służba ochrony państwa jest zobowiązana do pobrania opłaty od jednostki organizacyjnej, na przykład pozostającej w jej strukturze. Rozwiązanie takie jest raczej nielogiczne i jest niczym innym jak przepływem środków finansowych pomiędzy różnymi podziałkami tego samego budżetu.

Większość ewentualnych zmian dotyczy bezpośrednio postępowań sprawdzających wobec osób. Ich wprowadzenie w Ustawie o ochronie informacji niejawnych wpłynęłoby na konieczność zmian w aktach niższego rzędu, w tym w decyzjach ministra obrony narodowej. Niektóre z nich zostały już zmodyfikowane. Pozostałe należałoby uaktualnić nie tylko w powiązaniu z ewentualną nowelizacją Ustawy o ochronie informacji niejawnych, ale również z obecnie opracowywaną Ustawą o Wojskowych Służbach Informacyjnych, które są głównym elementem systemu ochrony informacji niejawnych w Siłach Zbrojnych RP.

Nowelizacja aktów normatywnych powinna przynieść szereg pozytywnych skutków. Po pierwsze zbliży nasze rozwiązania do standardów natowskich a po drugie zmniejszy obciążenie służb ochrony państwa i pełnomocników ochrony

zwłaszcza w zakresie prowadzenia postępowań sprawdzających przed wydaniem poświadczenia bezpieczeństwa osobowego.

Abstrahując od możliwości dokonania zmian w przepisach trzeba przyznać, iż system ochrony informacji niejawnych w Siłach Zbrojnych RP, budowany w przededniu wstąpienia Polski do NATO i modyfikowany od 1999 roku działa sprawnie i zapewnia właściwą ochronę informacji niejawnych przed zagrożeniami, jakie stwarza współczesny świat.

Czteroletnie doświadczenia dowiodły, iż większość natowskich regulacji została dostosowana do specyfiki Sił Zbrojnych RP. Jednakże troską służb ochrony państwa i kierowników jednostek organizacyjnych powinno być dostosowywanie obowiązujących przepisów do nowych zagrożeń dla bezpieczeństwa informacji niejawnych. System ten musi być elastyczny, wprowadzający nowe mechanizmy i zdolny do przeciwstawienia się nowym jakościowo zagrożeniom ze strony na przykład terroryzmu czy przestępczości zorganizowanej. Dotyczy to zarówno sfery regulacji prawnych jak i właściwych reakcji na zagrożenia osób uprawnionych do dostępu do informacji niejawnych.

Docelowe stworzenie takiego systemu wynika z narodowych interesów Rzeczypospolitej Polskiej i stanowi o sojuszniczej wiarygodności Polski i naszych Sił Zbrojnych na arenie międzynarodowej a zwłaszcza w Organizacji Traktatu Północnoatlantyckiego.

BIBLIOGRAFIA

I. Akty prawne o randze ustawy.

1. Ustawa z dnia 21 listopada 1967 roku o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, Dz. U. z 1967 roku, Nr 44, poz. 220 z późniejszymi zmianami.
2. Ustawa z dnia 14 grudnia 1982 roku o ochronie tajemnicy państwowej i służbowej, Dz. U. z 1983 roku, Nr 40, poz. 271 z późniejszymi zmianami.
3. Ustawa z dnia 28 września 1991 roku o kontroli skarbowej, Dz. U. z 1991 roku, Nr 100, poz. 442 z późniejszymi zmianami.
4. Ustawa z dnia 3 kwietnia 1993 roku o badaniach i certyfikacji, Dz. U. z 1993 roku, Nr 55, poz. 250 z późniejszymi zmianami.
5. Ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli, Dz.U. z 1995 r., Nr 13, poz. 59 z późniejszymi zmianami.
6. Ustawa z dnia 11 maja 1995 roku o Naczelnym Sądzie Administracyjnym, Dz. U. z 1995 roku, Nr 74, poz. 368 z późniejszymi zmianami.
7. Ustawa z dnia 14 grudnia 1995 roku o urzędzie Ministra Obrony Narodowej, Dz. U. z 1996 roku, Nr 10, poz. 56 z późniejszymi zmianami.
8. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku, Dz. U. z 1997 roku, Nr 78 poz. 483 z późniejszymi zmianami.
9. Ustawa z dnia 6 czerwca 1997 roku Kodeks Karny, Dz. U. z 1997 roku, Nr 88, poz. 553 z późniejszymi zmianami.
10. Ustawa z dnia 6 czerwca 1997r. Kodeks Postępowania Karnego, Dz. U. z 1997 roku, Nr 89, poz. 555 z późniejszymi zmianami.
11. Ustawa z dnia 25 czerwca 1997 r. o świadku koronnym, Dz. U. z 1997 roku, Nr 114, poz. 738 z późniejszymi zmianami.
12. Ustawa z dnia 29 stycznia 1997 roku o ochronie danych osobowych, Dz. U. z 1997 roku, Nr 133, poz. 883 z późniejszymi zmianami.

13. Ustawa z dnia 29 sierpnia 1997 roku – Ordynacja podatkowa, Dz. U. z 1997 roku, Nr 137, poz. 926 z późniejszymi zmianami.
14. Ustawa z dnia 29 sierpnia 1997 roku - Prawo bankowe, Dz. U. z 1997 roku, Nr 140, poz. 939 z późniejszymi zmianami.
15. Ustawa z dnia 18 grudnia 1998 roku o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, Dz. U. z 1998 roku, Nr 155, poz. 1016 z późniejszymi zmianami.
16. Ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych, Dz. U. z 1999 roku, Nr 11, poz. 95 z późniejszymi zmianami.
17. Ustawa z dnia 21 stycznia 2000 roku o zmianie niektórych ustaw związanych z funkcjonowaniem administracji publicznej, Dz. U. z 2000 roku, Nr 12, poz. 136.
18. Ustawa z dnia 24 maja 2000 roku o Krajowym Rejestrze Karnym, Dz. U. z 2000 roku, Nr 50, poz. 580 z późniejszymi zmianami.
19. Ustawa z dnia 27 kwietnia 2001 roku o zmianie ustawy o podatku od towarów i usług oraz o podatku akcyzowym, ustawy o zamówieniach publicznych oraz ustawy o ochronie informacji niejawnych, Dz. U. z 2001 roku, Nr 56, poz. 580.
20. Ustawa z dnia 14 czerwca 1960 roku, Kodeks Postępowania Administracyjnego, Dz. U. z 2000 roku, Nr 98, poz. 1071.
21. Ustawa z dnia 15 lipca 1987 roku o Rzeczniku Praw Obywatelskich, Dz. U. z 2001 roku, Nr 14, poz. 147.
22. Ustawa z dnia 16 marca 2001 roku o Biurze Ochrony Rządu, Dz. U. z 2001 roku, Nr 27, poz. 298.
23. Ustawa z dnia 30 czerwca 2000 roku Prawo własności przemysłowej, Dz. U. z 2001 roku, Nr 49, poz. 508.
24. Ustawa z dnia 6 lipca 2001 roku o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych, Dz. U. z 2001 roku, Nr 110, poz.1189.
25. Ustawa z dnia 21 grudnia 2001 roku o zmianie ustawy o organizacji i trybie pracy Rady Ministrów oraz o zakresie działania ministrów, ustawy o

działach administracji rządowej oraz o zmianie niektórych ustaw, Dz. U. z 2001 roku, Nr 154, poz. 1800.

26. Ustawa z dnia 24 sierpnia 2001 roku o Żandarmerii Wojskowej i wojskowych organach porządkowych, Dz. U. z 2001 roku, Nr 123, poz. 1353.
27. Ustawa z dnia 20 czerwca 1985 roku o Prokuraturze, Dz. U. z 2002 roku, Nr 21, poz. 206.
28. Ustawa z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz. U. z 2002 roku, Nr 74, poz. 676.
29. Ustawa z dnia 7 czerwca 2002 roku o zniesieniu Generalnego Inspektora Celnego, o zmianie ustawy o kontroli skarbowej oraz o zmianie niektórych, innych ustaw, Dz. U. z 2002 roku, Nr 89, poz. 804.
30. Ustawa z dnia 30 sierpnia 2002 roku – Prawo o postępowaniu przed sądami administracyjnymi, Dz. U. z 2002 roku, Nr 153, poz. 1270.

II. Wykonawcze akty normatywne.

1. Rozporządzenie Ministra Sprawiedliwości z dnia 1 grudnia 1998 r. w sprawie sposobu przechowywania protokołów zeznań obejmujących okoliczności, na które rozciąga się obowiązek zachowania tajemnicy państwowej, służbowej albo związanej z wykonywaniem zawodu lub funkcji, Dz. U. z 1998 roku, Nr 148, poz. 975.
2. Rozporządzenie Rady Ministrów z dnia 9 lutego 1999 r. w sprawie stanowisk i rodzajów prac zleconych w organach administracji rządowej, których wykonywanie może łączyć się z dostępem do informacji niejawnych, stanowiących tajemnicę państwową, Dz. U. z 1999 roku, Nr 18, poz. 155.
3. Rozporządzenie Rady Ministrów z dnia 9 lutego 1999 r. w sprawie organizacji kancelarii tajnych, Dz. U. z 1999 roku, Nr 18, poz. 156 z późniejszymi zmianami.

4. Rozporządzenie Rady Ministrów z dnia 9 lutego 1999 r. w sprawie wzorów: kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, odmowy wydania świadectwa bezpieczeństwa przemysłowego, Dz. U. z 1999 roku, Nr 18, poz. 157.
5. Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie szczegółowego zakresu, warunków i trybu współdziałania organów, służb i innych państwowych jednostek organizacyjnych ze służbami ochrony państwa w toku prowadzonych postępowań sprawdzających, Dz. U. z 1999 roku, Nr 18, poz. 159.
6. Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie szczegółowego trybu prowadzenia przez służby ochrony państwa kontroli w zakresie ochrony informacji niejawnych stanowiących tajemnicę państwową, Dz. U. z 1999 roku, Nr 18, poz. 160.
7. Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie sposobu i trybu udostępniania danych z ewidencji, Dz. U. z 1999 roku, Nr 18, poz. 161 z późniejszymi zmianami.
8. Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych, Dz. U. z 1999 roku, Nr 18, poz. 162.
9. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 23 lutego 1999 r. w sprawie wzoru poświadczenia bezpieczeństwa oraz wzoru odmowy wydania poświadczenia bezpieczeństwa, Dz. U. z 1999 roku, Nr 18, poz. 165 z późniejszymi zmianami.
10. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 23 lutego 1999 r. w sprawie wzoru zaświadczenia, stwierdzającego odbycie przeszkolenia w zakresie ochrony informacji niejawnych, Dz. U. z 1999 roku, Nr 18, poz. 166.
11. Rozporządzenie Ministrów Spraw Wewnętrznych i Administracji oraz Obrony Narodowej z dnia 26 lutego 1999 r. w sprawie sposobu oznaczania materiałów, w tym klauzulami tajności oraz sposobu umieszczania klauzul

na tych materiałach, Dz. U. z 1999 roku, Nr 18, poz. 167 z późniejszymi zmianami.

12. Rozporządzenie Ministrów Spraw Wewnętrznych i Administracji oraz Obrony Narodowej z dnia 26 lutego 1999 r. w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów, Dz. U. z 1999 roku, Nr 18, poz. 168.
13. Rozporządzenie Prezesa Rady Ministrów z dnia 13 lipca 2001 r. w sprawie wysokości opłat za przeprowadzenie postępowania sprawdzającego przez służbę ochrony państwa oraz za wydanie świadectwa bezpieczeństwa przemysłowego, Dz. U. z 2001 roku, Nr 74, poz. 788.
14. Rozporządzenie Prezesa Rady Ministrów z dnia 16 lipca 2001 r. w sprawie wysokości opłat za przeprowadzenie przez służbę ochrony państwa czynności warunkujących wydanie certyfikatu dla systemu lub sieci teleinformatycznej, urządzenia lub narzędzia kryptograficznego oraz za wydanie tych certyfikatów, Dz. U. z 2001 roku, Nr 77, poz. 820.
15 Rozporządzenie Ministra Obrony Narodowej z dnia 26 września 2001 roku w sprawie wyrobów, które nie mogą być nabywane bez certyfikatu, Dz. U. z 2001 roku, Nr 113, poz. 1213.
16. Zarządzenie Nr 49/MON ministra obrony narodowej z dnia 7 sierpnia 2002 roku w sprawie szczególnych zasad organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych, Dziennik Urzędowy ministra obrony narodowej Nr 15 z 30 sierpnia 2002, poz. 149.
17. Decyzja Nr 191/MON Ministra Obrony Narodowej z dnia 12 października 1999 roku w sprawie działalności kontrolnej w resorcie Obrony Narodowej, Dziennik Rozkazów MON z 1999 roku, poz. 89.
18. Decyzja Nr 29/MON ministra obrony narodowej z dnia 8 marca 2000 r. w sprawie szczególnych zasad i trybu przeprowadzania postępowań sprawdzających, dokumentowania i archiwizacji materiałów dotyczących postępowań, Dziennik Rozkazów MON z 2000 roku, poz., 74.

19. Decyzja Nr 30/MON ministra obrony narodowej z dnia 8 marca 2000 roku w sprawie powołania pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów i sieci teleinformatycznych oraz utworzenia pionów ochrony w jednostkach organizacyjnych resortu obrony narodowej, Dziennik Rozkazów MON z 2000 roku, poz., 75 z późniejszymi zmianami.
20. Decyzja Nr 31/MON ministra obrony narodowej z dnia 8 marca 2000 roku w sprawie zasad opracowywania planów ochrony jednostek organizacyjnych resortu obrony narodowej, Dziennik Rozkazów MON z 2000 roku, poz., 76.
21. Decyzja Nr 181/MON ministra obrony narodowej z dnia 6 października 2000 roku w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej, Dziennik Rozkazów MON z 2000 roku, poz., 111.
22. Decyzja Nr 182/MON ministra obrony narodowej z dnia 8 marca 2000 roku w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej, Dziennik Rozkazów MON z 2000 roku, poz., 112 z późniejszymi zmianami.
23. Decyzja Nr. 100/MON ministra obrony narodowej z dnia 6 czerwca 2000 roku w sprawie Jednostki Certyfikującej, właściwej w Ministerstwie Obrony Narodowej do certyfikacji wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych, Dziennik Rozkazów MON z 2000 roku, poz., 55.
24. Decyzja Nr 16/MON ministra obrony narodowej z dnia 25 stycznia 2001 roku w sprawie szkolenia w zakresie ochrony informacji niejawnych, Dziennik Urzędowy ministra obrony narodowej Nr 1 z 15 lutego 2001 roku, poz. 9.
25. Decyzja Nr 29/MON ministra obrony narodowej z dnia 22 lutego 2001 roku w sprawie trybu certyfikacji i kontroli kancelarii zagranicznych, kancelarii środków i materiałów kryptograficznych, punktów obsługi dokumentów zagranicznych, stacji łączności kryptograficznej oraz pomieszczeń wydzielonych (terminali) teleinformatycznych w jednostkach

organizacyjnych resortu obrony narodowej, Dziennik Urzędowy ministra obrony narodowej Nr 3 z 20 marca 2001 roku, poz. 32.

26. Przepisy o ochronie tajemnicy w Siłach Zbrojnych, Sygn. Sztab Gen. 1251/86,
27. Zarządzenie szefa Wojskowych Służb Informacyjnych nr 12 z dnia 9 czerwca 1999 roku.

III. Dokumenty normatywne NATO

1. Umowa między Stronami Traktatu Północnoatlantyckiego współpracy w dziedzinie informacji atomowych *(ang. Agreement between the Parties to the North Atlantic Treaty for Cooperation regarding Atomic Information)* – C-M(64)39.
2. Procedury Administracyjne *(ang. Administrative Arrangements),* regulujące zasady kontroli i przechowywania informacji atomowych tego typu, które musza być podpisane przez Strony Umowy – C-M(68)41.
3. Bezpieczeństwo w Organizacji Traktatu Północnoatlantyckiego (*ang. Security within the North Atlantic Treaty Organisation*), Memorandum Rady Północnoatlantyckiej Nr C-M(2002)49.
4. „Zasady i procedury postępowania z dokumentami Stanów Zjednoczonych – Oddzielnych Planów Operacyjnych w NATO" *(ang. Special Procedures for the Handling of United States Single Integrated Operational Plan (US-SIOP) Information within NATO)* – C-M(71)27.
5. Dyrektywa w sprawie bezpieczeństwa osobowego *(ang. Directive on Personnel Security),* AC/35-D/2000.
6. Dyrektywa w sprawie bezpieczeństwa fizycznego *(ang. Directive on Physical Security),* AC/35/2001.
7. Dyrektywa w sprawie bezpieczeństwa informacji *(ang. Directive on Security of Information)* AC/35-D/2002.
8. Dyrektywa w sprawie bezpieczeństwa przemysłowego *(ang. Directive on Industrial Security),* AC/35-D/2003.

9. Postępowanie z informacjami jawnymi *NATO (ang. The management of non-classified NATO information)*, C-M(2002)60.

IV. Inne

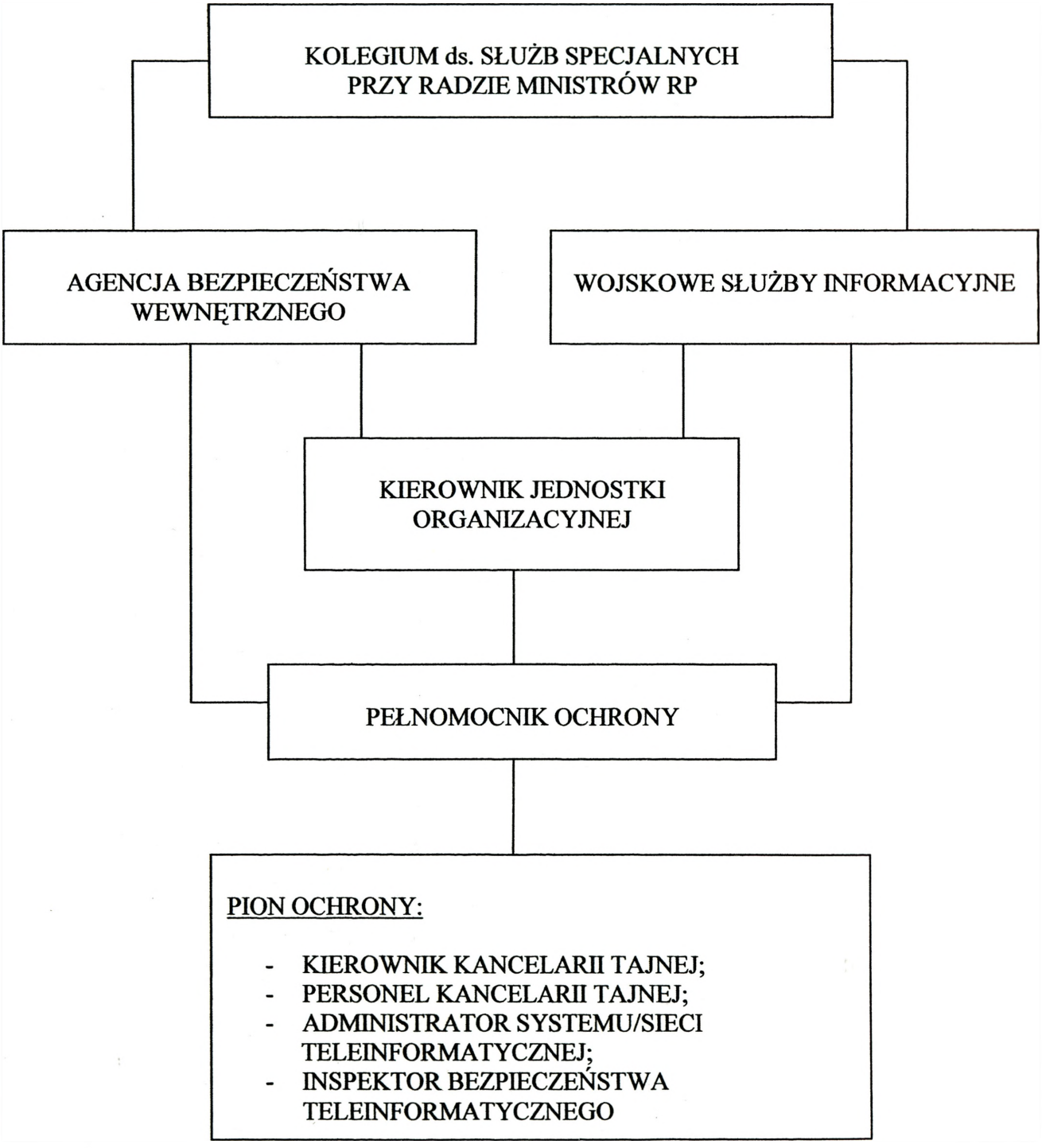
1. Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, sporządzona w Rzymie 4 listopada 1950 roku, Dz. U. z 1993 roku, Nr 61, poz. 284 z późniejszymi zmianami.
2. Wyrok Trybunału Konstytucyjnego z dnia 10 maja 2000 roku, sygn. Akt K 21/99, Dz. U. z 2000 roku, Nr 39, poz. 462.
3. Popularna Encyklopedia Powszechna, Wyd. Pinnex, Kraków 1998, tom 19 i 21.
4. Jakubus B., Ryszkowski M. – Ochrona informacji niejawnych, Wyd. Projekt, Warszawa 2001.
5. NATO Vademecum, Wyd. Bellona, Warszawa 1995r.
6. NATO po Pradze *(ang. NATO after Prague),* Biuro Prasy i Informacji NATO, Bruksela, 2002.
7. Sprawozdanie z działalności KOIN w 1999 roku, Kancelaria Prezesa Rady Ministrów, Warszawa, styczeń 2000r.
8. Informacja o działalności KOIN w 2000 roku, Kancelaria Prezesa Rady Ministrów, Warszawa, luty 2001.
9. Trybuna, nr 235 (3528) z 8 października 2001 roku.

ZAŁĄCZNIKI

1. System ochrony informacji niejawnych w Polsce.
2. System ochrony informacji niejawnych w Siłach Zbrojnych RP.
3. Struktura Biura Ochrony Informacji Niejawnych Ministerstwa Obrony Narodowej.
4. Struktura Oddziału Ochrony Informacji Niejawnych Dowództwa Okręgu Wojskowego.
5. Certyfikat bezpieczeństwa.
6. Ankieta bezpieczeństwa osobowego.
7. Poświadczenie bezpieczeństwa.
8. Odmowa wydania poświadczenia bezpieczeństwa.
9. Kwestionariusz bezpieczeństwa przemysłowego.
10. Świadectwo bezpieczeństwa przemysłowego.
11. Odmowa wydania świadectwa bezpieczeństwa przemysłowego.
12. Wysokość opłat, pobieranych przez Wojskowe Służby Informacyjne za czynności realizowane w ramach postępowania sprawdzającego przed wydaniem świadectwa bezpieczeństwa przemysłowego.
13. Certyfikat dla systemu/sieci teleinformatycznej.
14. Wysokość opłat, pobieranych przez Wojskowe Służby Informacyjne za czynności warunkujące wydanie certyfikatu dla systemu lub sieci teleinformatycznej, urządzenia lub narzędzia kryptograficznego oraz za wydanie tych certyfikatów.
15. Zaświadczenie stwierdzające odbycie przeszkolenia w zakresie ochrony informacji niejawnych.
16. Personal particulars forms.
17. NATO personnel security clearance certificate.
18. Certificate of security clearance.
19. Courier certificate.
20. Facility security clearance certificate.
21. Request for visit.

Załącznik Nr 1

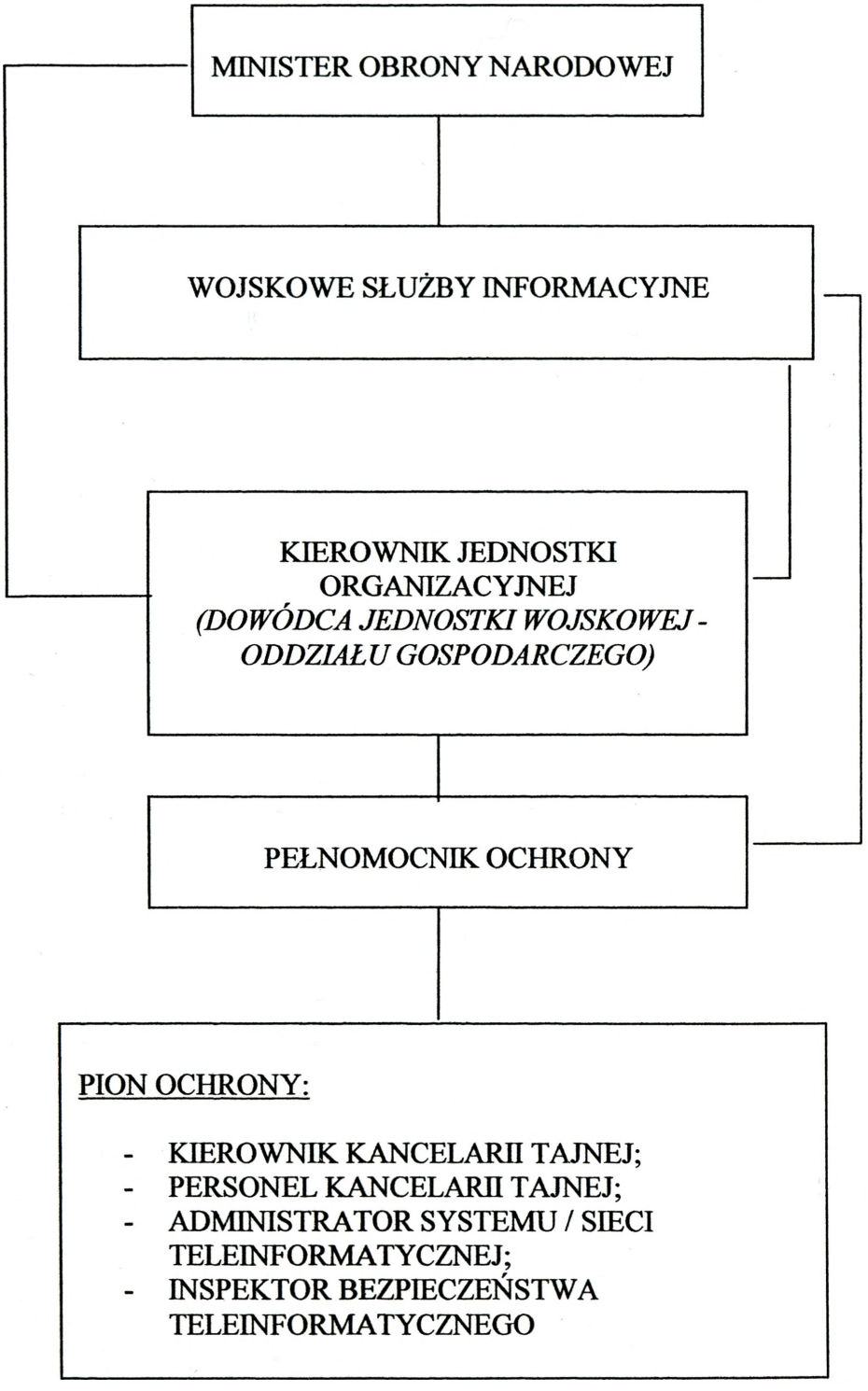
SYSTEM OCHRONY INFORMACJI NIEJAWNYCH W POLSCE[231]



[231] Źródło – opracowanie własne

Załącznik Nr 2

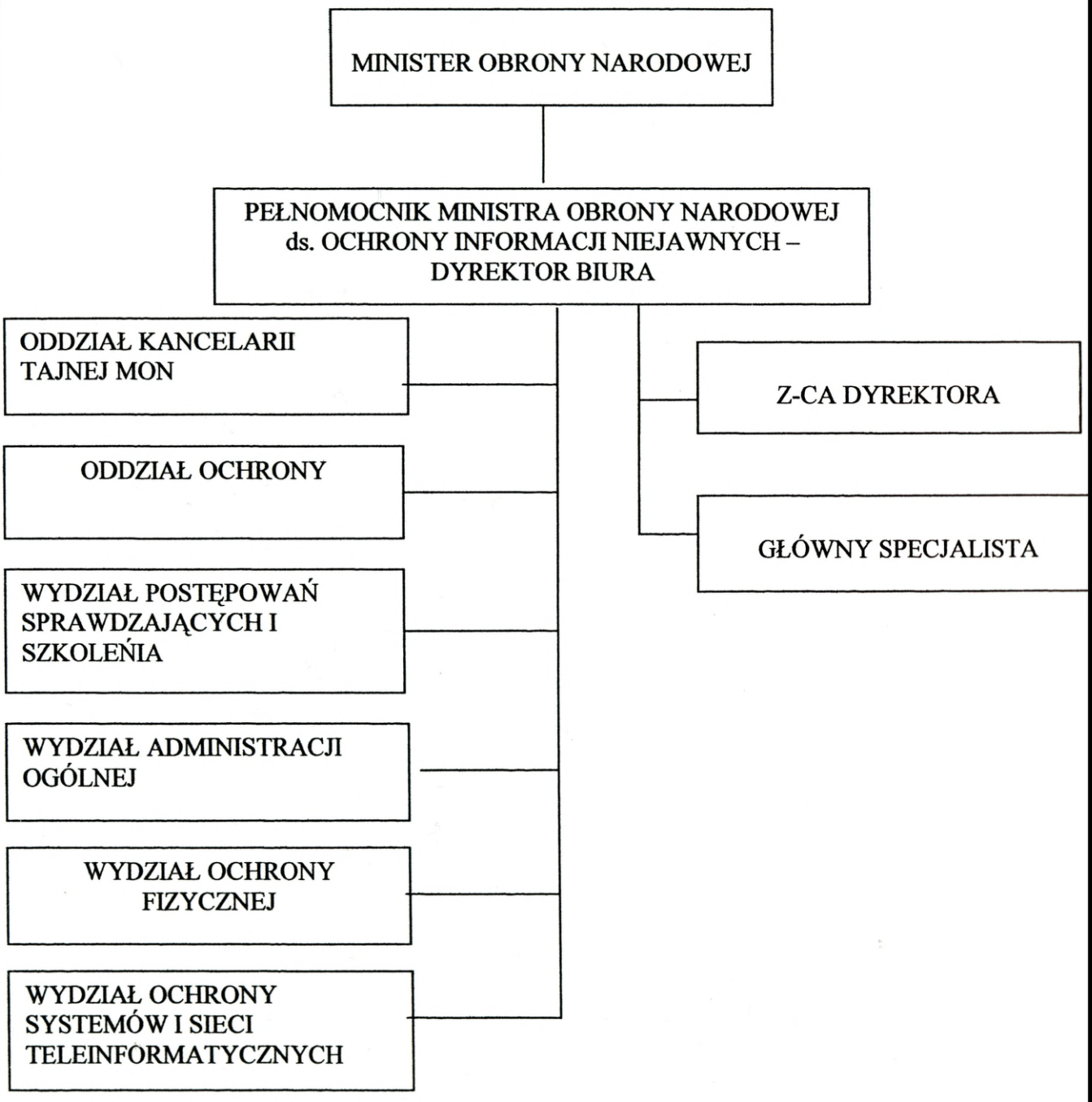
SYSTEM OCHRONY INFORMACJI NIEJAWNYCH W SIŁACH ZBROJNYCH RP[232]



[232] Źródło – opracowanie własne

Załącznik Nr 3

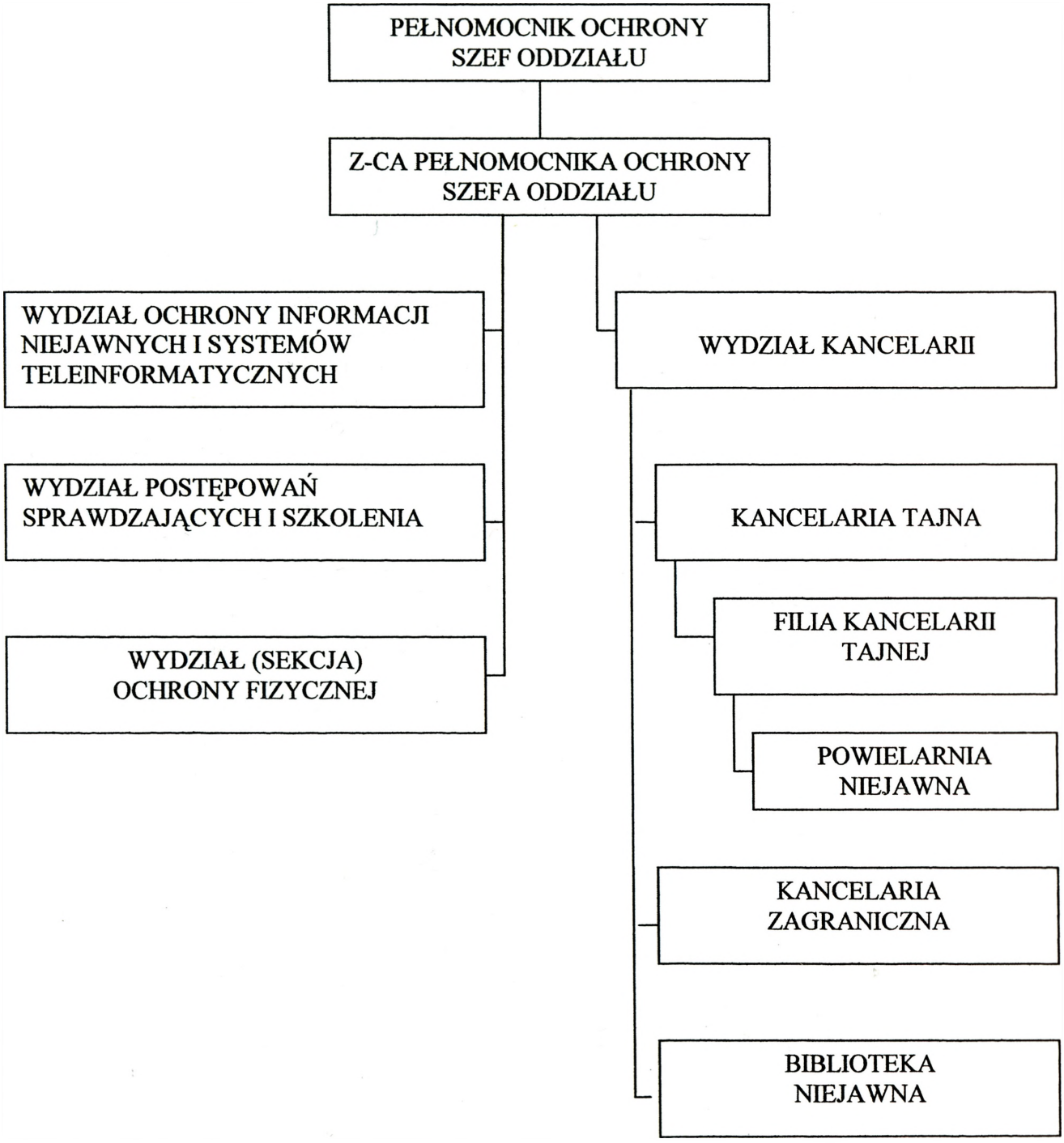
STRUKTURA BIURA OCHRONY INFORMACJI NIEJAWNYCH MINISTERSTWA OBRONY NARODOWEJ[233]



[233] Struktura została ustanowiona na mocy Decyzji Nr 30/MON.

Załącznik Nr 4

STRUKTURA ODDZIAŁU OCHRONY INFORMACJI NIEJAWNYCH DOWÓDZTWA OKREGU WOJSKOWEGO.[234]



[234] Struktura została ustanowiona na mocy Decyzji Nr 30/MON.

Załącznik Nr 5

CERTYFIKAT BEZPIECZEŃSTWA

dla pomieszczenia .....
w
.....

Zaświadcza się, że Stała Komisja, działając na podstawie § 1 decyzji Nr 29/MON Ministra Obrony Narodowej z dnia 22 lutego 2001 r. w sprawie trybu certyfikacji i kontroli kancelarii zagranicznych, kancelarii środków i materiałów kryptograficznych, punktów obsługi dokumentów zagranicznych, stacji łączności kryptograficznej oraz pomieszczeń wydzielonych (terminali) teleinformatycznych w jednostkach organizacyjnych resortu Obrony Narodowej, w dniach ..... przeprowadziła kontrolę pomieszczenia w .....

Komisja stwierdziła, ze kontrolowane pomieszczenie jest zorganizowane w sposób zapewniający wymagany poziom bezpieczeństwa i ochrony informacji niejawnych, do klauzuli .....* włącznie.

Certyfikat ważny jest do: .....

Data .....
.....

m.p.

(imię i nazwisko, stopień, stanowisko służbowe, podpis)

*podać właściwą klauzulę np.: TAJNE

Załącznik Nr 6

ANKIETA BEZPIECZEŃSTWA OSOBOWEGO

Szanowna Pani,

Szanowny Panie,

Rząd Rzeczypospolitej Polskiej, kierując się troską o bezpieczeństwo narodowe i mając powinność jego ochrony, przedstawia tę ankietę w przekonaniu, iż zostanie ona wypełniona zgodnie z Pana /Pani/ najlepszą wiedzą i wolą. Dziękując za współpracę podkreślamy, że celem tej ankiety jest wyłącznie ochrona bezpieczeństwa narodowego przed zagrożeniami ze strony obcych służb specjalnych, ugrupowań terrorystycznych lub grup przestępczych. Prosimy uważnie przeczytać poniższą instrukcję, a w razie wątpliwości zwrócić się do pełnomocnika ochrony w Pana /Pani/ jednostce organizacyjnej lub do właściwej służby ochrony państwa o pomoc w wypełnieniu ankiety.

Instrukcja

1. Przed wypełnieniem ankiety proszę się z nią dokładnie zapoznać.

2. Proszę wypełniać ankietę pismem drukowanym, a w razie możliwości pismem maszynowym.

3. Jeśli ankieta zawiera zbyt mało miejsca na wpisanie danych, proszę je podać na osobnej karcie formatu A-4, którą należy dołączyć do ankiety.

4. W razie braku wiedzy umożliwiającej podanie danych, proszę wpisać sformułowanie: "nie wiem".

5. Jeżeli treść któregoś z punktów lub podpunktów ankiety nie dotyczy Pana /Pani/ osoby, proszę wpisywać sformułowanie: "nie dotyczy".

6. Jeśli dane w kolejnych punktach ankiety są identyczne z danymi podanymi w poprzednich punktach, można w kolejnych punktach wpisywać sformułowanie: "jak w pkt ... lit. ...".

7. Jeżeli któryś z członków rodziny, o których mowa w pkt 2-9 ankiety, zmarł, proszę ograniczać wypełnianie takiego fragmentu ankiety wyłącznie do podania jego imienia, nazwiska, daty i miejsca urodzenia oraz sformułowania: "nie żyje".

8. Niniejszą ankietę wypełnia się w podanym niżej zakresie, w związku z upoważnieniem Pana /Pani/ do dostępu do informacji niejawnych.

9. Osoby objęte postępowaniem sprawdzającym w związku z dostępem do informacji niejawnych oznaczonych klauzulą "zastrzeżone" wypełniają następujące punkty: 1, 2a-c, 3a-c, 12, 13, 22, 28a.

10. Osoby objęte postępowaniem sprawdzającym w związku z dostępem do informacji niejawnych oznaczonych klauzulą "poufne" wypełniają wyłącznie następujące punkty: 1-7, 9, 12, 13, 15-19, 22-28, 30, 32 i 33.

11. Osoby objęte postępowaniem sprawdzającym w związku z dostępem do informacji niejawnych oznaczonych klauzulą "tajne" nie wypełniają pkt 31.

12. Osoby objęte postępowaniem sprawdzającym w związku z dostępem do informacji niejawnych oznaczonych klauzulą "ściśle tajne" wypełniają wszystkie punkty ankiety.

13. Przy ponownym postępowaniu sprawdzającym przeprowadzanym po upływie 10 lat w stosunku do osoby, która otrzymała poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych oznaczonych klauzulą "poufne" - osobę tę prosi się o wypełnienie pkt: 10, 17, 22-25, 28 i 29 z odniesieniem się wyłącznie do okresu począwszy od daty wypełnienia poprzedniej ankiety do dnia wypełnienia następnej ankiety. Jeżeli dane odnoszące się do wyżej wymienionych punktów nie uległy zmianie, należy przy nich wpisać sformułowanie: "bez zmian".

14. Przy ponownym postępowaniu sprawdzającym, przeprowadzanym po upływie trzech lat w stosunku do osoby, która otrzymała poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych oznaczonych klauzulą "ściśle tajne", a po upływie pięciu lat w stosunku do osoby, która otrzymała poświadczenie bezpieczeństwa upoważniające do dostępu do informacji oznaczonych klauzulą "tajne" - osoby te nie wypełniają punktów: 1j oraz 1k.

15. Przy kolejnym postępowaniu sprawdzającym przeprowadzanym po upływie okresów, o których mowa wyżej, proszę wypełnić punkty: 10, 17, 22-25, 28 i 29, odnosząc się wyłącznie do okresu począwszy od daty wypełnienia poprzedniej ankiety do dnia wypełnienia następnej ankiety. Jeżeli dane odnoszące się do wyżej wymienionych punktów nie uległy zmianie, należy przy nich wpisać sformułowanie: "bez zmian".

.....
(pieczęć instytucji występującej o sprawdzenie osoby upoważnionej do dostępu do informacji niejawnych)

.....

Poufne
(po wypełnieniu)
Egz. nr .....

miejsce
na fotografię
4 x 3,5 cm

ANKIETA
BEZPIECZEŃSTWA OSOBOWEGO

Niniejsza ankieta bezpieczeństwa osobowego wykorzystana będzie zgodnie z ustawą na użytek postępowania sprawdzającego w związku z upoważnieniem Pana(-i) do dostępu do informacji niejawnych oznaczonych klauzulą (proszę zakreślić właściwe pole):

„Zastrzeżone" ☐

„Poufne" ☐

„Tajne" ☐

„Ściśle tajne" ☐

1. Osoba podlegająca sprawdzeniu:

a. Nazwisko .....

b. Nazwiska poprzednie (również nazwisko rodowe) .....

c. Imiona .....

d. Imiona poprzednie (w razie ich zmiany) .....

e. Data urodzenia ..... miejsce urodzenia .....

f. Posiadane obywatelstwo(a) .....

g. Posiadane uprzednio obywatelstwa .....

h. W przypadku zmiany obywatelstwa proszę podać:

– na jakie imiona i nazwisko wydano akt o zmianie lub utracie obcego obywatelstwa albo akt uzyskania posiadanego obecnie obywatelstwa .....

– data wydania .....

– numer i nazwa dokumentu .....

– wydany przez .....

i. Dowód osobisty: seria i numer .....

wydany przez .....

data wydania .....

j. Nr PESEL .....

k. Numer Identyfikacji Podatkowej (NIP) .....

l. Posiadany stopień wojskowy .....

ł. Seria i numer książeczki wojskowej .....

– wydana przez .....

– data wydania .....

m. Aktualne miejsce zamieszkania (zameldowanie na pobyt stały)

.....
(państwo, miasto, ulica, nr domu, nr mieszkania,

.....
kod pocztowy, nr telefonu domowego)

n. Aktualny adres pobytu czasowego (jeżeli inny niż w pkt 1 lit. m)

.....
(państwo, miasto, ulica, nr domu, nr mieszkania,

.....
kod pocztowy, nr telefonu domowego)

o. Paszport: seria i nr .....

wydany przez .....

termin ważności: .....

p. Aktualne miejsce(a) pracy, służby:

1. .....
(nazwa oraz nr REGON pracodawcy)

.....
(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego, nr faxu)

.....

.....
(zajmowane stanowisko lub charakter wykonywanych prac) (wysokość miesięcznych poborów/dochodów netto)

2. .....
(nazwa pracodawcy)

.....
(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego, nr faxu)

.....

.....
(zajmowane stanowisko) (wysokość miesięcznych poborów/dochodów netto)

r. Dodatkowe źródła utrzymania/zarobkowania
(Dotyczy również dochodów otrzymywanych bez świadczenia pracy, np. renty zagranicznej, dywidendy od posiadanych papierów wartościowych, odsetek od lokat bankowych, zysków z obrotu akcjami na giełdzie, udziałów w funduszach powierniczych, dochodów z wynajmu nieruchomości, wygranych w grach losowych o wysokości przekraczającej trzykrotne średnie wynagrodzenie w Polsce, honorariów za publikacje, działalność dydaktyczną, dochodów z realizacji umów zleconych itp.)

1. .....
(nazwa pracodawcy)

.....
(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego, nr faxu)

.....

.....
(zajmowane stanowisko lub charakter wykonywanych prac) (wysokość miesięcznych poborów/dochodów netto)

2. .....
(nazwa pracodawcy)

.....
(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego, nr faxu)

.....

.....
(zajmowane stanowisko) (wysokość miesięcznych poborów/dochodów netto)

3. Inne dochody. .....
(źródło/wysokość)

.....

2. Ojciec osoby sprawdzanej:

a) Imię i nazwisko .....

b) Miejsce urodzenia ..... data urodzenia .....

c) Obywatelstwo (a) .....

d) Aktualne miejsce(a) pracy:

.....
(nazwa pracodawcy)

.....
(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego, nr faxu)

.....

.....
(zajmowane stanowisko)

e) Aktualne miejsce zameldowania (stałe i czasowe)

.....
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy, nr telefonu domowego)

.....

.....

f) Aktualny adres zamieszkania .....
(jeżeli jest inny niż ww.) (państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy,

.....
(nr telefonu domowego)

.....

3. Matka osoby sprawdzanej:

a) Imię i nazwisko .....

b) Miejsce urodzenia ..... data urodzenia .....

c) Obywatelstwo (a) .....

d) Aktualne miejsce(a) pracy:

.....
(nazwa pracodawcy)

.....
(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego, nr faxu)

.....

.....
(zajmowane stanowisko)

e) Aktualne miejsce zameldowania (stałe i czasowe)

.....
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy, nr telefonu domowego)

.....

.....

f) Aktualny adres zamieszkania .....
(jeżeli jest inny niż ww.) (państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy,

.....
(nr telefonu domowego)
.....

4. Rodzeństwo osoby sprawdzanej:

1) a) Imię i nazwisko .....

b) Miejsce urodzenia ..... data urodzenia .....

c) Obywatelstwo (a) .....

d) Aktualne miejsce(a) pracy:

.....
(nazwa pracodawcy)

.....
(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego, nr faxu)

.....

.....
(zajmowane stanowisko)

e) Aktualne miejsce zameldowania (stałe i czasowe)

.....
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy, nr telefonu domowego)

.....

.....

f) Aktualny adres zamieszkania .....
(jeżeli jest inny niż ww.) (państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy,

.....
(nr telefonu domowego)
.....

2) a) Imię i nazwisko .....

b) Miejsce urodzenia ..... data urodzenia .....

c) Obywatelstwo (a) .....

d) Aktualne miejsce(a) pracy:

.....
(nazwa pracodawcy)

.....
(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego, nr faxu)

.....

.....
(zajmowane stanowisko)

e) Aktualne miejsce zameldowania (stałe i czasowe)

.....
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy, nr telefonu domowego)

.....

.....

f) Aktualny adres zamieszkania .....
(jeżeli jest inny niż ww.) (państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy,

.....
(nr telefonu domowego)
.....

3) a) Imię i nazwisko .....

b) Miejsce urodzenia ..... data urodzenia .....

c) Obywatelstwo (a) .....

d) Aktualne miejsce(a) pracy:

.....
(nazwa pracodawcy)

.....
(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego, nr faxu)

.....

.....
(zajmowane stanowisko)

e) Aktualne miejsce zameldowania (stałe i czasowe)

.....
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy, nr telefonu domowego)

.....

.....

f) Aktualny adres zamieszkania .....
(jeżeli jest inny niż ww.) (państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy,

.....
(nr telefonu domowego)
.....

5. Małżonek(ka) osoby sprawdzanej:

dot. także
konkubenta/konkubiny
lub osoby o takim
charakterze pozostającej we wspólnym
gospodarstwie
domowym z osobą
wymienioną w pkt 1

Imię i nazwisko (także nazwisko rodowe): .....
Miejsce urodzenia ..... data urodzenia .....

Posiadane obywatelstwo(a) .....

Aktualne miejsce pracy:

(a) .....
(nazwa oraz nr REGON pracodawcy)

.....
(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego)

. . . . . .

. . . . . .

(zajmowane stanowisko)

(b) . . . . . .

(nazwa oraz nr REGON pracodawcy)

. . . . . .

(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego)

. . . . . .

. . . . . .

(zajmowane stanowisko)

Aktualne miejsce zameldowania (stałe i czasowe)
(jeżeli inne niż w pkt 1 lit. m lub n)

. . . . . .

(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy, nr telefonu domowego)

. . . . . .

. . . . . .

Aktualny adres zamieszkania . . . . . (jeżeli jest inny niż ww.)

(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy,

. . . . . .

(nr telefonu domowego)

. . . . . .

Data i miejscowość zawarcia małżeństwa . . . . . .

Dowód osobisty: seria i numer . . . . . .

wydany przez . . . . . .

data wydania . . . . . .

6. Ojciec:
osoby wymienionej
w pkt 5
Imię i nazwisko: . . . . . .

Miejsce urodzenia . . . . . data urodzenia . . . . . .

Posiadane obywatelstwo(a) . . . . . .

Aktualne miejsce(a) pracy:

. . . . . .

(nazwa oraz nr REGON pracodawcy)

. . . . . .

(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego)

. . . . . .

. . . . . .

(zajmowane stanowisko)

Aktualne miejsce zameldowania (stałe i czasowe)

. . . . . .
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy, nr telefonu domowego)

. . . . . .
. . . . . .

Aktualny adres zamieszkania . . . . . (jeżeli jest inny niż ww.)
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy,

. . . . . .
(nr telefonu domowego)
. . . . . .

7. Matka:
osoby wymienionej
w pkt 5Imię i nazwisko: . . . . . .
Miejsce urodzenia . . . . . data urodzenia . . . . . .

Posiadane obywatelstwo(a) . . . . . .

Aktualne miejsce(a) pracy:

. . . . . .
(nazwa oraz nr REGON pracodawcy)

. . . . . .
(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego)

. . . . . .

. . . . . .
(zajmowane stanowisko)

Aktualne miejsce zameldowania (stałe i czasowe)

. . . . . .
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy, nr telefonu domowego)

. . . . . .

. . . . . .

Aktualny adres zamieszkania . . . . . (jeżeli jest inny niż ww.)
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy,

. . . . . .
(nr telefonu domowego)
. . . . . .

8. Rodzeństwo:
osoby wymienionej
w pkt 5
(a) Imię i nazwisko: . . . . . .
Data i miejsce urodzenia . . . . . .

Obywatelstwo(a) . . . . . .

Aktualne miejsce(a) pracy:

. . . . . .
(nazwa pracodawcy)

. . . . . .
(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego)

. . . . . .

. . . . . .

(zajmowane stanowisko)

Aktualne miejsce zameldowania (stałe i czasowe)

. . . . . .

(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy, nr telefonu domowego)

. . . . . .

. . . . . .

Aktualny adres zamieszkania . . . . . (jeżeli jest inny niż ww.)

(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy,

. . . . . .

(nr telefonu domowego)

. . . . . .

(b) Imię i nazwisko: . . . . . .

Data i miejsce urodzenia . . . . . .

Obywatelstwo(a) . . . . . .

Aktualne miejsce(a) pracy:

. . . . . .

(nazwa pracodawcy)

. . . . . .

(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego)

. . . . . .

. . . . . .

(zajmowane stanowisko)

Aktualne miejsce zameldowania (stałe i czasowe)

. . . . . .

(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy, nr telefonu domowego)

. . . . . .

. . . . . .

Aktualny adres zamieszkania . . . . . (jeżeli jest inny niż ww.)

(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy,

. . . . . .

(nr telefonu domowego)

. . . . . .

(c) Imię i nazwisko: . . . . . .

Data i miejsce urodzenia . . . . . .

Obywatelstwo(a) . . . . . .

Aktualne miejsce(a) pracy:

. . . . . .

(nazwa pracodawcy)

. . . . . .
(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego)

. . . . . .
(zajmowane stanowisko)

Aktualne miejsce zameldowania (stałe i czasowe)

. . . . . .
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy, nr telefonu domowego)

. . . . . .

. . . . . .

Aktualny adres zamieszkania . . . . . (jeżeli jest inny niż ww.)
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy,

. . . . . .
(nr telefonu domowego)
. . . . . .

9. Dzieci:
osoby wymienionej
w pkt 5
(a) Data i miejsce urodzenia . . . . . .

Nazwisko . . . . . .

Imię (imiona) . . . . . .

Aktualne miejsce zameldowania (stałe i czasowe)
(jeżeli jest inne niż w pkt 1 lit. m lub n bądź pkt 5)

. . . . . .
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy, nr telefonu domowego)

. . . . . .

. . . . . .

Aktualny adres zamieszkania . . . . . (jeżeli jest inny niż ww.)
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy,

. . . . . .

Aktualne miejsce(a) pracy:

. . . . . .
(nazwa pracodawcy)

. . . . . .
(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego)

. . . . . .

. . . . . .
(zajmowane stanowisko)

(b) Data i miejsce urodzenia . . . . . .

Nazwisko . . . . . .

Imię (imiona) . . . . . .

Aktualne miejsce zameldowania (stałe i czasowe)
(jeżeli jest inne niż w pkt 1 lit. m lub n bądź pkt 5)

. . . . . .
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy, nr telefonu domowego)

. . . . . .

. . . . . .

Aktualny adres zamieszkania . . . . . (jeżeli jest inny niż ww.)
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy,

. . . . . .

Aktualne miejsce(a) pracy:

. . . . . .
(nazwa pracodawcy)

. . . . . .
(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego)

. . . . . .

. . . . . .
(zajmowane stanowisko)

(c) Data i miejsce urodzenia . . . . . .

Nazwisko . . . . . .

Imię (imiona) . . . . . .

Aktualne miejsce zameldowania (stałe i czasowe)
(jeżeli jest inne niż w pkt 1 lit. m lub n bądź pkt 5)

. . . . . .
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy, nr telefonu domowego)

. . . . . .

. . . . . .

Aktualny adres zamieszkania . . . . . (jeżeli jest inny niż ww.)
(państwo, miasto, ulica, nr domu, nr mieszkania, kod pocztowy,

. . . . . .

Aktualne miejsce(a) pracy:

. . . . . .
(nazwa pracodawcy)

. . . . . .
(adres: państwo, miasto, ulica, nr domu, kod pocztowy, nr telefonu służbowego)

. . . . . .

. . . . . .
(zajmowane stanowisko)

10. Wprzypadku gdy członkowie rodziny, o których mowa w punktach 2 – 9, mieszkają stale za granicą lub przebywali poza nią dłużej niż 3 miesiące, proszę podać następujące dane:

Okres zamieszkiwania lub pobytu		Nazwisko i imię	Państwo dokładny adres	Powód pobytu
od	do			

11. Czy w latach 1944 – 1990 był pracownikiem lub tajnym współpracownikiem organów bezpieczeństwa państwa w rozumieniu ustawy z dnia 11 kwietnia 1997 r. O ujawnieniu pracy lub służby w organach bezpieczeństwa państwa lub współpracy z nimi w latach 1944 – 1990 osób pełniących funkcje publiczne (Dz. U. Nr 70, poz. 443 oraz z 1998 r. Nr 113, poz. 715 i Nr 131, poz. 860).

TAK ☐ NIE ☐ NIE DOTYCZY ☐

12. Czy i kiedy oraz przez jaki organ w ciągu ostatnich 10 lat był Pan(-i) karany(-a) (jeśli tak, proszę podać nazwę organu oraz określić, za popełnienie jakiego przestępstwa lub wykroczenia.

.....

.....

13. Czy aktualnie toczą się wobec Pana(-i) postępowania o ukaranie za przestępstwa lub wykroczenia, o których Panu(-i) wiadomo?

.....

(jeśli tak, proszę podać, jaki organ prowadzi sprawę(-y) i ewentualnie jej numer)

.....

14. Czy cierpi Pan(-i) lub cierpiał(-a) w przeszłości na choroby psychiczne lub inne dolegliwości powodujące zakłócenia czynności psychicznych? Jeśli tak, proszę wyszczególnić, na jakie, w jakich okresach czasu oraz

podać, jaka placówka zdrowia lub lekarz zajmowała się lub nadal zajmuje się Pana(-i) osobą w związku w wyżej wymienionymi dolegliwościami lub chorobą.

(a) .....

.....

.....

(b) .....

.....

.....

15. Czy zażywa Pan(-i) lub zażywał(-a) kiedykolwiek narkotyki lub inne środki odurzające? Jeśli tak, proszę podać, jakie, kiedy oraz czy sytuacje takie nadal mają miejsce. Proszę nie wyszczególniać faktów podawania Panu(-i) narkotyków lub środków odurzających przez uprawnionych do tego lekarzy, o ile nie doprowadziło to do sytuacji, iż nadal musi Pan(-i) przyjmować tego typu środki i je przyjmuje.

.....

.....

.....

16. (a) Czy w okresie ostatnich 10 lat spożywał(-a) Pan(-i) lub spożywa alkohol w ilościach powodujących zaburzenia lub utratę świadomości? Jeśli tak, proszę podać częstotliwość tego typu sytuacji oraz okoliczności, w jakich one mają (lub miały) miejsce, a także, czy w związku z tym leczy się Pan(-i) lub leczył(-a) w poradniach specjalistycznych lub placówkach służby zdrowia (jakich – dokładna nazwa i adres.

.....

.....

.....

.....

.....

(b) Czy spożywanie alkoholu było kiedykolwiek przyczyną problemów w Pana(-i) pracy lub życiu prywatnym?

.....

.....

.....

17. Proszę podać dane dotyczące Pana(-i) zatrudnienia (służby) w okresie ostatnich 10 lat.

Okres		Pełna nazwa zakładu pracy i jego pełny adres	Ostatnie zajmowane stanowisko
od	do		

18. Czy Pan(-i), Pana(-i) współmałżonek lub inne osoby pozostające z Panem (-ią) we wspólnym gospodarstwie domowym jesteście zadłużeni u osób fizycznych lub prawnych (np. pożyczki, kredyty), których łączna kwota przekracza sumę stanowiącą sześciokrotność otrzymywanego przez Pana(-ią) wynagrodzenia? Jeśli tak, proszę podać, kto, w jakiej wysokości, wobec kogo, z jakiego tytułu oarz jaki jest ich planowany termin spłaty.

(a) .....
(nazwisko i imię) (rodzaj zobowiązania) (wysokość zobowiązania finansowego)

.....
(wobec kogo) (z jakiego tytułu) (termin spłaty)

(b) .....
(nazwisko i imię) (rodzaj zobowiązania) (wysokość zobowiązania finansowego)

.....
(wobec kogo) (z jakiego tytułu) (termin spłaty)

(c) .....
(nazwisko i imię) (rodzaj zobowiązania) (wysokość zobowiązania finansowego)

.....
(wobec kogo) (z jakiego tytułu) (termin spłaty)

19. Czy Pan(-i), Pana(-i) współmałżonek lub inne osoby pozostające z Panem(-ią) we wspólnym gospodarstwie domowym jesteście obciążeni innymi zobowiązaniami finansowymi (np. zaległości podatkowe, alimenty, spłaty hipoteki, zastawy, należności wynikające z orzeczeń sądowych)? Jeśli tak, proszę podać, kto, jakie, w jakiej wysokości, wobec kogo, z jakiego tytułu oraz planowany termin ich spłaty.

(a) .....
(nazwisko i imię) (rodzaj zobowiązania) (wysokość zobowiązania finansowego)

.....
(wobec kogo) (z jakiego tytułu) (termin spłaty)

(b) .....
(nazwisko i imię) (rodzaj zobowiązania) (wysokość zobowiązania finansowego)

.....
(wobec kogo) (z jakiego tytułu) (termin spłaty)

(c) .....
(nazwisko i imię) (rodzaj zobowiązania) (wysokość zobowiązania finansowego)

.....
(wobec kogo) (z jakiego tytułu) (termin spłaty)

20. Proszę podać wysokość dochodów uzyskanych przez Pana(-ią), Pana(-i) współmałżonka oraz inne osoby pozostające we wspólnym gospodarstwie domowym w roku poprzedzającym wypełnienie niniejszej ankiety bezpieczeństwa osobowego.

(a) .....
(nazwisko i imię) (wysokość dochodu netto)

(b) .....
(nazwisko i imię) (wysokość dochodu netto)

(c) .....
(nazwisko i imię) (wysokość dochodu netto)

21. Proszę podać, czy Pan(-i), Pana(-i) współmałżonek oraz inne osoby pozostające we wspólnym gospodarstwie domowym posiadacie nieruchomości, własne przedsiębiorstwo lub udział w innym przedsiębiorstwie. Jeżeli tak, proszę podać, kto, jakie i gdzie.

(a) .....
(nazwisko i imię) (posiadane nieruchomości, przedsiębiorstwa, udziały)

.....
(gdzie)

(b) .....
(nazwisko i imię) (posiadane nieruchomości, przedsiębiorstwa, udziały)

.....
(gdzie)

(c) .....
(nazwisko i imię) (posiadane nieruchomości, przedsiębiorstwa, udziały)

.....
(gdzie)

22. Czy kiedykolwiek był Pan(-i) upoważniony(-a) do dostępu do informacji niejawnych stanowiących tajemnicę państwową w Polsce lub w innym państwie. Jeśli tak, proszę podać następujące dane:

Pełna nazwa i adres instytucji, w której był(-a) Pan(-i) dopuszczony(-a) do takich informacji	Państwo	Zakres, klauzula informacji niejawnych, do których był(-a) Pan(-i) dopuszczony(-a)	Okres	
			od	do

23. Czy po ukończeniu 18 lat przebywał(-a) Pan(-i) kiedykolwiek za granicą dłużej niż 10 dni *(w tym podróże służbowe)*? Jeżeli tak, proszę podać następujące dane:

Okres zamieszkiwania lub pobytu		Państwo, miasto, ulica, nr domu i mieszkania, kod pocztowy	Powód pobytu
od	do		

24. Czy podczas pobytów za granicą podejmował(-a) Pan(-i) działalność zarobkową? Jeśli tak, proszę podać następujące dane:

Okres		Państwo, dokładny adres, nazwa zakładu pracy lub innego pracodawcy	Zajmowane stanowisko	Rodzaj wykonywanej pracy oraz uzyskiwane dochody
od	do			

25. Proszę podać okresy i miejsca zamieszkiwania w okresie ostatnich 10 lat (w Polsce lub innych państwach).

Okres zamieszkiwania lub zameldowania		Państwo, miejscowość (województwo, powiat, gmina), numer kodu pocztowego	Adresy: ulica, nr domu, nr mieszkania
od	do		

26. Proszę podać dane aktualnych współmieszkańców, z którymi zamieszkuje Pan(-i) w jednym mieszkaniu *(np. członkowie rodziny, sublokatorzy, właściciele mieszkania)*.

Nazwisko i imię *(imiona)*	Miejscowość i data urodzenia

27. Proszę podać dane właściciela aktualnie zamieszkiwanego przez siebie mieszkania *(nazwa instytucji/firmy, nazwisko właściciela – dokładny adres, nr telefonu)*.

28. a) Posiadane wykształcenie i tytuły zawodowe lub naukowe:

. . . . . .

(wyższe, średnie, podstawowe)

a) Proszę podać następujące dane dotyczące uczelni, szkół i kursów, które Pan(-i) ukończył(-a) w przeszłości:

Okres nauki		Nazwy i adresy wszystkich szkół, uczelni i kursów zawodowych	Uzyskane dyplomy, świadectwa ukończenia
od	do		

29. Czy Pan(-i) lub członkowie rodziny wymienieni w punktach 2 – 9 utrzymujecie lub utrzymywaliście w okresie ostatnich 20 lat kontakty służbowe lub prywatne (towarzyskie) z obywatelami innych państw. Jeżeli tak, proszę podać następujące dane:

Okres		Osoba	Państwo: dokładny adres	Powód, charakter kontaktu
od	do			

30. Czy należał(-a) lub należy Pan(-i) do zarejestrowanych lub nie zarejestrowanych polskich lub zagranicznych organizacji, partii politycznych lub stowarzyszeń.

Nazwa organizacji i jej dokładny adres	Pełniona w niej funkcja	Okres przynależności	
		od	do

31. proszę wskazać 3 osoby polecające, które znają Pana(-ią) przynajmniej od 2 lat *(nie mogą to być członkowie rodziny wymienieni w pkt 2 – 9, a także osoby, które obsługują Pana(-i) interesy majątkowe lub z którymi z racji wykonywanego przez nie zawodu łączą Pana(-ią) stosunki szczególnego zaufania).*

Imię i nazwisko	Miejsce pracy	Dokładny adres domowy nr telefonu

32. Czy kiedykolwiek podczas pobytu za granicą był Pan(-i) wypytywany(-a) lub w inny sposób indagowany(-a) przez obce władze (imigracyjne, skarbowe, inne) na tematy związane z zagadnieniami bezpieczeństwa lub obronności państwa? Czy wiadomo Panu(-i) coś o analogicznych zainteresowaniach wobec swojego współmałżonka lub innych osób pozostających we wspólnym gospodarstwie domowym bądź innych członków rodziny. Jeśli tak, proszę zakreślić właściwe pole. Proszę nie podawać żadnych dalszych szczegółów. Zostaną one z Panem(-ią) omówione przez przedstawiciela służby ochrony państwa, prowadzącego postępowanie sprawdzające.

☐ TAK ☐ NIE

33. Czy kiedykolwiek stwierdził Pan(-i) fakt zainteresowania swoją osobą ze strony zagranicznych służb specjalnych lub innych obcych instytucji aparatu ścigania (Policja, Straż Graniczna) bądź grup zorganizowanej przestępczości (polskich lub zagranicznych)? Czy wiadomo Panu(-i) coś o analogicznych zainteresowaniach wobec swojego współmałżonka lub innych osób pozostających we wspólnym gospodarstwie domowym bądź innych członków rodziny. Jeśli tak, proszę zakreślić właściwe pole. Proszę nie podawać żadnych dalszych szczegółów. Zostaną one z Panem(-ią) omówione przez przedstawiciela służby ochrony państwa, prowadzącego postępowanie sprawdzające.

 TAK

 NIE

Oświadczam, iż wypełniłem(-am) ankietę osobiście, zgodnie ze swoją wiedzą, świadom(-a), że każde fałszywe stwierdzenie lub pominięcie istotnego faktu będzie wystarczającym powodem do wstrzymania postępowania sprawdzającego i może stanowić podstawę odmowy wydania mi poświadczenia bezpieczeństwa.

Oświadczam, że zgadzam się na przeprowadzenie wobec mnie postępowania sprawdzającego według przepisów ustawy z dnia 22 stycznia 1999 r. O ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95) oraz stosownie do art. 7 pkt 5ustawy z dnia 29 sierpnia 1997 r. O ochronie danych osobowych (Dz. U. Nr 133, poz. 883); wyrażam zgodę na przetwarzanie, w rozumieniu art. 7 pkt 2 tej ustawy, moich danych osobowych zawartych w niniejszej ankiecie, z zastrzeżeniem ograniczeń wynikających w tym zakresie z wymienionej ustawy o ochronie informacji niejawnych.

Ilość kart stanowiących załącznik do ankiety 

Podpis osoby wypełniającej ankietę dla celów postępowania sprawdzającego

.....

Miejscowość .....

Data .....

.....

Czytelny podpis i pieczęć kierownika jednostki organizacyjnej oraz pełnomocnika ochrony

Miejscowość .....

Data .....

Załącznik Nr 7

.....
(pieczęć nagłówkowa służby ochrony państwa lub innej jednostki organizacyjnej z adresem i nr telefonu)

POŚWIADCZENIE BEZPIECZEŃSTWA Nr .....

Na podstawie art. 36 ust. 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11 poz. 95) po przeprowadzeniu na wniosek

.....
(wnioskodawca)

zwykłego / poszerzonego / specjalnego postępowania sprawdzającego

stwierdzam, że Pan(i) .....
(imię i nazwisko, data urodzenia)

uzyskał(a) poświadczenie bezpieczeństwa

upoważniające do dostępu do informacji niejawnych stanowiących tajemnicę służbową / państwową* oznaczonych klauzulą „tajne" / „ściśle tajne" na okres do

.....
(data ważności)

.....
(miejscowość i data)

.....
(imienna pieczęć i czytelny podpis pełnomocnika ochrony lub upoważnionego funkcjonariusza albo żołnierza służby ochrony państwa)

m.p.

- *Niepotrzebne skreślić*

UWAGA:

Poświadczenie bezpieczeństwa wydawane przez służbę ochrony państwa jest sporządzane na papierze offsetowym formatu A4 z tłem rastrowanym w kolorze zielonym i z tekstem o treści „służba ochrony pastwa" oraz wprowadzonym w miejsce linii mikrotekstem o treści „służba ochrony państwa".

Załącznik Nr 8

.....
(pieczęć nagłówkowa służby ochrony państwa lub innej jednostki organizacyjnej z adresem i nr telefonu)

ODMOWA WYDANIA POŚWIADCZENIA BEZPIECZEŃSTWA

Nr .....

Na podstawie art. 36 ust. 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11 poz. 95) po przeprowadzeniu na wniosek

.....
(wnioskodawca)

zwykłego / poszerzonego / specjalnego postępowania sprawdzającego

stwierdzam, że Panu(i)

.....
(imię i nazwisko, data urodzenia)

uzyskał(a) poświadczenie bezpieczeństwa

odmówiono wydania poświadczenia bezpieczeństwa w zakresie dostępu do informacji niejawnych stanowiących tajemnicę służbową / państwową* oznaczonych klauzulą „tajne" / „ściśle tajne"

.....
(miejscowość i data)

m.p.

.....
(imienna pieczęć i czytelny podpis pełnomocnika ochrony lub upoważnionego funkcjonariusza albo żołnierza służby ochrony państwa)

- Niepotrzebne skreślić

Załącznik Nr 9

Po wypełnieniu „Poufne"

.....
(nazwa przedsiębiorcy, jednostki
naukowej lub badawczo-rozwojowej)

KWESTIONARIUSZ BEZPIECZEŃSTWA PRZEMYSŁOWEGO

1) Pełna nazwa przedsiębiorstwa, jednostki naukowej lub jednostki badawczo-rozwojowej (nr REGON) .....

.....

.....

2) Pełny adres przedsiębiorstwa, jednostki naukowej lub jednostki badawczo-rozwojowej: miasto, ulica, nr domu, kod pocztowy, województwo, powiat, gmina, nr telefonu-faxu, nr poczty elektronicznej.....

.....

.....

3) Status prawny .....

.....

4) Dane o strukturze organizacyjnej .....

.....

5) Dane o strukturze kapitałowej .....

.....

6) Dane dotyczące władz lub organów zarządzających .....

.....

.....

7) Dane dotyczące systemu ochrony informacji niejawnych, w tym:

a) systemu ochrony osób .....

.....

b) systemu ochrony materiałów .....

.....

c) systemu zabezpieczenia obiektów .....

.....

8. Wykaz pracowników uprawnionych do dostępu do informacji niejawnych:

....

....

....

....

9. Wykaz pracowników, którzy powinni mieć dostęp do informacji niejawnych w związku z postępowaniem zmierzającym do zawarcia umowy lub jej wykonaniem:

....

....

....

....

10. Wykaz osób odpowiedzialnych za ochronę przekazanych jednostce organizacyjnej, wymienionej w pkt. 1, informacji niejawnych:

....

....

....

....

11. Wszelkie zmiany dotyczące danych zawartych w kwestionariuszu przekazuje się w formie uzupełnienia do kwestionariusza.

....

(miejscowość i data) *(pieczęć imienna i podpis kierownika jednostki organizacyjnej*

Uwaga:
W przypadku braku miejsca, informacje należy podać na dodatkowych arkuszach, wskazując punkty, których dotyczy uzupełnienie

Załącznik Nr 10

.....
(pieczęć nagłówkowa służby ochrony państwa z adresem i nr telefonu

ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO Nr .....

Zaświadcza się, że dnia .....

.....
(nazwa służby ochrony państwa)

wydała .....
(nazwa przedsiębiorstwa, jednostki naukowej, jednostki badawczo-rozwojowej nr REGON)

mieszczącemu się w .....
(adres przedsiębiorstwa, jednostki naukowej, jednostki badawczo-rozwojowej)

na podstawie art. 69 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95)

ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO

stwierdzając, że jednostka ta posiada zdolność do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą ..... w zakresie

.....
(oznaczenie umowy)

przed nieuprawnionym ujawnieniem.

..... m.p. .....
(miejscowość i data) *(pieczęć imienna i podpis upoważnionego funkcjonariusza albo żołnierza służby ochrony państwa)*

Załącznik Nr 11

.....
(pieczęć nagłówkowa służby ochrony państwa z adresem i nr telefonu

ODMOWA WYDANIA
ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO Nr .....

Na podstawie art. 69/70* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95)

.....
(nazwa służby ochrony państwa)

ODMÓWIŁA WYDANIA ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

.....
(nazwa przedsiębiorstwa, jednostki naukowej, jednostki badawczo-rozwojowej nr REGON)

stwierdzając, że ww. jednostka organizacyjna nie posiada zdolności do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą ..... w zakresie

.....
(oznaczenie umowy)

.....

przed nieuprawnionym ujawnieniem.

.....
(miejscowość i data)

m.p.

.....
(pieczęć imienna i podpis upoważnionego funkcjonariusza albo żołnierza służby ochrony państwa)

* *Niepotrzebne skreślić*

Załącznik Nr 12

WYSOKOŚĆ OPŁAT POBIERANYCH PRZEZ WOJSKOWE SŁUŻBY INFORMACYJNE ZA CZYNNOŚCI REALIZOWANE W RAMACH POSTĘPOWANIA SPRAWDZAJĄCEGO PRZED WYDANIEM ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO.

Podstawa: Rozporządzenie Prezesa Rady Ministrów z dnia 13 lipca 2001 roku w sprawie wysokości opłat za przeprowadzenie postępowania sprawdzającego przez służbę ochrony państwa oraz za wydanie świadectwa bezpieczeństwa przemysłowego (Dz. U. z dnia 20 lipca 2001 roku, Nr 74, poz. 788).

WYSZCZEGÓLNIENIE	KWOTA
Przeprowadzenie postępowania sprawdzającego wobec: - osób zajmujących stanowiska związane z kierowaniem, wykonaniem umowy lub z jej bezpośrednią realizacją u przedsiębiorcy, w jednostce naukowej lub badawczo – rozwojowej; - osób, które w imieniu przedsiębiorcy, jednostki naukowej lub badawczo – rozwojowej uczestniczą w czynnościach zmierzających do zawarcia umowy, jeżeli są one związane z dostępem do informacji niejawnych; - osób zatrudnionych w pionie ochrony; - działającego na rzecz i zlecenie przedsiębiorcy, jednostki naukowej lub badawczo – rozwojowej przedsiębiorcy, który uzyskał koncesję na prowadzenie działalności gospodarczej w zakresie wykonywania usług ochrony osób i mienia.	**1185,35 zł.** (0.5 krotności kwoty przeciętnego wynagrodzenia od każdej sprawdzanej osoby)
Sprawdzenie: - struktury i pochodzenia kapitału przedsiębiorcy; - struktury organizacyjnej przedsiębiorcy, jednostki naukowej lub badawczo – rozwojowej; - sytuacji finansowej i źródeł pochodzenia środków finansowych pozostających w dyspozycji przedsiębiorcy, jednostki naukowej lub badawczo – rozwojowej.	**5926,75 zł.** (2.5 krotności kwoty przeciętnego wynagrodzenia za dokonanie sprawdzenia)
Wydanie świadectwa bezpieczeństwa przemysłowego.	**2370,70 zł.** (1-krotność kwoty przeciętnego wynagrodzenia)

* Pobierane kwoty są krotnością kwoty przeciętnego, miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku w czwartym kwartale 2002 roku, tj. kwoty 2370,70 zł. (na podstawie Obwieszczenia prezesa Głównego Urzędu Statystycznego z dnia 16.01. 2003 roku – Dziennik Urzędowy GUS Nr 1 z 2003r.)

Załącznik Nr 13

JEDNOSTKA CERTYFIKUJĄCA WYROBY
W WOJSKOWYCH SŁUŻBACH INFORMACYJNYCH

CERTYFIKAT DLA SYSTEMU / SIECI TELEINFORMATYCZNEJ*
NR .....

Nazwa wyrobu: .....

Nazwa i adres posiadacza certyfikatu: .....
.....

Podstawa wydania certyfikatu: .....
.....

Sieć spełnia wymagania zawarte w: .....
.....

Certyfikat jest ważny wyłącznie dla systemu / sieci* teleinformatycznej wymienionej powyżej i eksploatowanej zgodnie z wymaganiami zawartymi w zatwierdzonych szczególnych Wymaganiach Bezpieczeństwa i Procedurach Bezpieczeństwa tej sieci.

Data ważności certyfikatu: .....

KIEROWNIK
Jednostki Certyfikującej Wyroby
w Wojskowych Służbach Informacyjnych

SZEF

Wojskowych Służb Informacyjnych

m.p.

Warszawa, dnia .....

*** niepotrzebne skreślić**

Załącznik Nr 14

WYSOKOŚĆ OPŁAT POBIERANYCH PRZEZ WOJSKOWE SŁUŻBY INFORMACYJNE ZA CZYNNOŚCI WARUNKUJACE WYDANIE CERTYFIKATU DLA SYSTEMU LUB SIECI TELEINFORMATYCZNEJ, URZADZENIA LUB NARZEDZIA KRYPTOGRAFICZNEGO ORAZ ZA WYDANIE TYCH CERTYFIKATÓW.

Podstawa: Rozporządzenie Prezesa Rady Ministrów z dnia 16 lipca 2001 roku w sprawie wysokości opłat za przeprowadzenie przez służbę ochrony państwa czynności warunkujących wydanie certyfikatu dla systemu lub sieci teleinformatycznej, urządzenia lub narzędzia kryptograficznego oraz za wydanie tych certyfikatów (Dz. U. z dnia 28 lipca 2001 roku, Nr 77, poz. 820)

Wyszczególnienie		Kwota
Wydanie certyfikatu dla urządzenia lub narzędzia kryptograficznego wchodzącego w skład systemu lub sieci teleinformatycznej, służącej do wytwarzania, przechowywania, przetwarzania lub przekazywania informacji niejawnych stanowiących tajemnicę państwową lub tajemnicę służbową, oznaczonych klauzulą POUFNE.		**1 185,35 zł** (0,5-krotności kwoty przeciętnego wynagrodzenia).
Przeprowadzane czynności	Badania mające na celu potwierdzenie przydatności do ochrony informacji niejawnych oznaczonych klauzulą POUFNE.	**592,67 zł** (0,25-krotności kwoty przeciętnego wynagrodzenia za godzinę pracy zespołu badawczego).
	Badania mające na celu potwierdzenie przydatności do ochrony informacji niejawnych oznaczonych klauzulą TAJNE.	**1 185,35 zł** (0,5-krotności kwoty przeciętnego wynagrodzenia za godzinę pracy zespołu badawczego).
	Badania mające na celu potwierdzenie przydatności do ochrony informacji niejawnych oznaczonych klauzulą ŚCIŚLE TAJNE.	**1 778,00 zł** (0,75-krotności kwoty przeciętnego wynagrodzenia za godzinę pracy zespołu badawczego).
Wydanie certyfikatu dla systemu lub sieci teleinformatycznej, służącej do wytwarzania, przechowywania, przetwarzania lub przekazywania informacji niejawnych stanowiących tajemnicę państwową.		**2 370,70 zł** (kwota jednego przeciętnego wynagrodzenia).
Przeprowadzane czynności	Dokonanie oceny szczególnych wymagań bezpieczeństwa systemu lub sieci teleinformatycznej przeznaczonej do ochrony stanowiących tajemnicę państwową.	**1 185,35 zł** (0,5-krotności kwoty przeciętnego wynagrodzenia za godzinę pracy zespołu badawczego). **** łączna ilość godzin nie może przekroczyć 40***
	Badanie i ocena zdolności systemu lub sieci teleinformatycznej oraz przeprowadzenie czynności mających na celu potwierdzenie ich zdolności do ochrony stanowiących tajemnicę państwową.	**1 185,35 zł** (0,5-krotności kwoty przeciętnego wynagrodzenia za godzinę pracy zespołu badawczego) **** łączna ilość godzin, oddzielnie dla każdej lokalizacji systemu lub sieci teleinformatycznej, nie może przekroczyć 16***

* Pobierane kwoty są krotnością kwoty przeciętnego, miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku w czwartym kwartale 2002 roku, tj. kwoty 2370,70 zł. (na podstawie Obwieszczenia prezesa Głównego Urzędu Statystycznego z dnia 16.01. 2003 roku – Dziennik Urzędowy GUS Nr 1 z 2003r.)

Załącznik Nr 15

.....
(pieczęć nagłówkowa służby ochrony państwa z adresem i nr telefonu)

ZAŚWIADCZENIE Nr .....

stwierdzające odbycie przeszkolenia w zakresie ochrony informacji niejawnych

Stwierdza się, że Pan(i):

- imię i nazwisko: .....
- data urodzenia: .....

odbył(a) przeszkolenie w zakresie ochrony informacji niejawnych wymagane przepisami ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11 poz. 95) przeprowadzone przez Urząd Ochrony Państwa / Wojskowe Służby Informacyjne*.

.....
(miejscowość i data)

m.p.

.....
(pieczęć imienna i podpis upoważnionego funkcjonariusza albo żołnierza służby ochrony państwa)

* Niepotrzebne skreślić

Załącznik Nr 16

Pfotograpf of applicant to be attache here

Size not less than 4cmx3.5 cm

PERSONAL PARTICULARS FORMS

(the information supplied below will be treated as strictly confidential)

1. Application for employment as: .....
2. Surname, in BLOCK CAPITALS: .....
   (and maiden name where applicable)
3. First names: .....
4. Date of birth:..... Place of birth: .....
5. Nationality: ..... Nationality at birth (if different): .....
6. Passport or ID card particulars: No. ..... Issued at: .....
   Date of issue: .....
7. If applicant, parents or spouse or cohabitant were naturalized, state:
   Name in which Certificate was issued: .....
   Number of Certificate: ..... Date of issue: .....

8. FATHER:
   Full name: .....
   Place of birth: ..... Date of birth: .....
   Nationality at birth: ..... Present nationality: .....
   Occupation: .....
   Present address: .....
   .....

9. MOTHER:
   Maiden name and first names: .....
   Place of birth: ..... Date of birth: .....
   Nationality at birth: ..... Present nationality: .....
   Occupation *(if any)*: .....
   Address *(if different from 8 above)*: .....
   .....

10. BROTHERS And .. SISTERS
    1.Full name: .....
    Present address: .....
    2. Full name: .....
    Present address: .....
    3. Full name: .....
    Present address: .....
    4. Full name: .....
    Present address: .....
    5. Full name: .....
    Present address: .....

11.SPOUSE Or CO-HABITANT

Name *(and maiden name where applicable)*: .....
First name: .....
Place of birth: ..... Date of birth: .....
Nationality at birth: ..... Present nationality: .....
Occupation: .....
Employer: .....
Date and place of marriage: .....
Present address *(if different from that given in paragraph 19)*: .....
.....

12. FATHER of 11.

Family name and first names: .....
Place of birth: ..... Date of birth: .....
Nationality at birth: ..... Present nationality: .....
Occupation: .....
Present address: .....
.....

13. MOTHER of 11.

Maiden name and first names: .....
Place of birth: ..... Date of birth: .....
Nationality at birth: ..... Present nationality: .....
Occupation *(if any)*: .....
Present address *(if different from 12 above)*: .....
.....

14. BROTHERS & SISTERS .....of 11.

1. Family name and first names: .....
Present address: .....
2. Family name and first names: .....
Present address: .....
3. Family name and first names: .....
Present address: .....

15. CHILDREN

1. Age: ..... First names: .....
Present address: .....
2. .Age: ..... First names: .....
Present address: .....
3. Age: ..... First names: .....
Present address: .....
4. Age: ..... First names: .....
Present address: .....

16. In case of remarriage(s) CHILDREN from the previous marriage(s) (also of cohabitant

1. Age: .....
   Full name: .....
   Present address: .....
2. Age: .....
   Full name: .....
   Present address: .....
3. Age: .....
   Full name: .....
   Present address: .....

17. If any of the persons referred to in questions 8 to 16 (over 18) are resident or have ever resided in a foreign country for more than three months, give particulars:

DATES		NAME OF PERSON	COUNTRY	REASONS
From	To			

18. Have you ever stayed – since the age of 18 – for a period exceeding three months in any foreign country (including travel in the Armed Forces)? If so, give particulars:

DATES		COUNTRY AND ADDRESSES	REASONS
From	To		

19. Periods of residence in home country, indicating present address, during the past 20 years:

DATES		LOCALITY (district, postal code number, etc.)	ADDRESS
From	TO		

20. Give the following details of any other persons with whom you share your accommodation (e.g.: grandparents, cousins, friends, domestic servants, etc.):

FULL NAME	PLACE AND DATE OF BIRTH

21. If the accommodation you occupy is not rented from the owner or real estate agent in your name, please give the name of the person who places it at your disposal:

22. Education: Give the following particulars of education, including any NATO sponsored courses (NATO Defence College, SHAPE School, stating course numbers and dates):

DATES		EDUCATION ESTABLISMENT AND ADDRESS	DIPLOMAS/CERTIFICATES OBTAINED
From	To		

23. Give the following particulars of all previous employment (including any NATO employment):

DATES		NAME AND ADDRESS OF EMPLOYER	POST OCCUPIED
From	To		

24. Have you – or any of the persons referred to in questions 8 to 16 above – maintained any personal relationship (or contacts) with any nationals of a country with a non-democratic regime. If so, give particulars:

DATES		PERSONS CONCERNED	COUNTRY (+address)	REASONS
From	To			

25. Have you been involved in NATO's Outreach programs (NACC/PfP). If so, do you maintain any contacts (official or social) with partner country participants? Please list names and nationalities of persons involved.

NAME	NATIONALITY

26. List three character referees who have known you for at least two years. If possible, one should be a NATO employee. (Relatives do not qualify, nor do bank managers, medical practitioners, priests etc. unless they you socially).

NAME	PROFESSION	PRIVATE ADDRESS

27. Any other remarks, if judged necessary or useful:

I have completed this document in the knowledge that any false statement or omission of material facts may be sufficient cause for rejection as a candidate for employment, or for the termination of any existing employment with a NATO body:

Signature: .....

Place: .....

Date: .....

Załącznik Nr 17

NATO UNCLASSIFIED

NATO PERSONNEL SECURITY CLEARANCE CERTIFICATE

1. Certification is hereby given that:

Full Name:

.....

Date and Place of Birth

.....

has been granted a security clearance by the Government of:

.....

in accordance with current NATO regulations, including the Security Annex to C-M(64)39 in the case of ATOMAL information, and is, therefore suitable to be entrusted with information classified up to and including[235]:

.....

.....

.....

2. The validity of certificate will expire not later than:

.....

Signed:

Title: Official government stamp

Date:

NATO UNCLASSIFIED

---

[235] Insert, as appropriate, one or more of the following:

(a) COSMIC TOP SECRET
(b) NATO SECRET
© NATO CONFIDENTIAL
(d) COSMIC TOP SECRET ATOMAL
(e) NATO SECRET ATOMAL
(f) NATO CONFIDENTIAL ATOMAL

Załącznik Nr 18

NATO UNCLASSIFIED

CERTIFICATE OF SECURITY CLEARANCE

Issued by .....
(member nation or NATO civil or military body)
Date and Place of Issue

.....

..... Valid until.....

This is to certify that:

Full Name .....
Date of Birth.....
Place of Birth.....
Nationality.....
Where employed.....
Purpose and Duration of Visit .....
.....
.....
Holder of Passport/Identity Card No.....
Issued at..... Dated.....
Military Rank and Number (where applicable).....
.....
has been granted access to NATO information classified up to and including ..... in accordance with current NATO security regulations, including the Security Annex to C-M(64)39 in the case of ATOMAL information, and has been briefed accordingly by
.....

Signed:

Title: Official government stamp (Optional)

Date:

NOTE: This certificate must be handled in accordance with the provisions of NATO Security Policy and its supporting directives.

NATO UNCLASSIFIED

Załacznik Nr 19

COURIER CERTIFICATE

Valid until .....

1. This is to certify that the bearer ....., holder of Passport/
(name and rank where applicable)
Identity Card No ..... is a member of .....
(parent organization)

2. On the journeys detailed overleaf, the bearer is traveling in the execution of his official functions and is designated as an official NATO courier. He is authorized to carry ..... (number) of packages of official NATO documents, the seals on which correspond to the specimen seal appearing against the appropriate journey.

3. All customs and immigration officials concerned are, therefore, requested to extend to the official correspondence and documents being carried under official seal by the bearer, the immunity from search or examination conferred by the Agreement on the Status of the North Atlantic Treaty Organisation National Representatives and International Staff, and the Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces.

Signature of Authorizing Official:

Designation:
(Name and rank in capitals)

Official stamp of NATO member
Nation or NATO civil or military body

Date

DETAILS OF ITINERARY

SPECIMENS OF SEAL USED

From	To	See note below
From	To	See note below

NOTE: In addition to an impression of the seal, the officer affixing the seal must print his name, rank and the name and address of his department, command, agency or facility.

Załącznik Nr 20

Facility Security Clearance Certificate (FSCC)

1. This is to certify that on ..... (date), the National Security Authority of ..... granted to the ..... (name of facility) located at ..... (address of facility) a NATO .....(classification) security clearance in accordance with provisions of the Industrial Security Directive supporting Enclosure "G" to the NATO Security Policy, C-M ....., valid until ..... (date).

2. The National Security Authority of .....(classification) confirms that the facility referred to in paragraph 1 above:

   (a) * possesses storage capabilities approved for the safeguarding of classified information up to the NATO ..... level;

   (b) * possesses NO storage capabilities approved for the safeguarding of NATO classified information.

.....	.....
(Signature)	(Stamp or seal of Issuing Authority)

---

* Delete (a) or (b) as applicable.

Załącznik Nr 21

Annex (es)

One-time
Recurring

REQUEST FOR VISIT

(x)Yes
( ) No

ADMINISTRATIVE DATA
1. REQUESTOR: DATE: TO: VISIT ID:
REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY
2. NAME: POSTAL ADDRESS: TELEX/FAX No.: TELEPHONE No.: POINT OF CONTACT:
GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED
3. NAME: ADDRESS: TELEX/FAX No.: TELEPHONE No.: POINT OF CONTACT:
4. DATES OF VISIT:
5. TYPE OF VISIT: (SELECT ONE FROM EACH COLUMN) ( ) GOVERNMENT INITIATIVE ( ) INITIATED BY REQUESTING AGENCY OR FACILITY ( ) COMMERCIAL INITIATIVE ( ) BY INVITATION OF THE FACILITY TO BE VISITED
6. SUBJECT TO BE DISCUSSED/JUSTIFICATION
7. ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED:
8. IS THE VISIT PERTINENT TO: (Y) SPECIFY A SPECIFIC EQUIPMENT OR WEAPON SYSTEM ( ) FOREIGN MILITARY SALES OR EXPORT LICENCE ( ) A PROGRAMME OR AGREEMENT ( ) A DEFENCE ACQUISITION PROCESS ( ) OTHER ( )

9. PARTICULARS FOR VISITORS	
NAME: DATE OF BIRTH: SECURITY CLEARANCE: POSITION COMPANY / AGENCY:	PLACE OF BIRTH: NATIONALITY ID/PP NUMBER:
NAME: DATE OF BIRTH: SECURITY CLEARANCE: POSITION COMPANY / AGENCY:	PLACE OF BIRTH: NATIONALITY ID/PP NUMBER:
10. THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY	
NAME:	TELEPHONE No:
SIGNATURE:	
11. CERTIFICATION OF SECURITY CLEARANCE	
NAME: ADDRESS: TELEPHONE: SIGNATURE:	STAMP (optional)
12. REQUESTING NATIONAL SECURITY AUTHORITY	
NAME: ADDRESS: TELEPHONE: SIGNATURE:	STAMP (optional)
13. REMARKS	

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 55871
Akademii Obrony Narodowej