# BEZPIECZEŃSTWO NARODOWE

Andrzej SZYMCZAK

## OCHRONA INFORMACJI NIEJAWNYCH W POLSKIM SYSTEMIE PRAWNYM

### Organizacja systemu ochrony

Dla każdego państwa szczególnie istotnym elementem bezpieczeństwa jest ochrona informacji o kluczowym znaczeniu. Dotyczy to zarówno informacji o charakterze cywilnym jak i wojskowym. Towarzyszy temu rosnąca rola infrastruktury informatycznej opartej na gromadzeniu, analizie i przesyłaniu wszelkiego rodzaju danych. Rozwinięte społeczeństwa w coraz większym stopniu polegają na automatycznych systemach przetwarzania informacji. Trudno dziś wyobrazić sobie kraj, w którym nie chroniono by danych obywateli (np. informacji medycznych, ubezpieczeniowych, podatkowych)[1]. Dotyczy to również informacji niejawnych bezpośrednio wpływających na bezpieczeństwo państwa, dotyczących kwestii obronnych, działania służb bezpieczeństwa oraz najistotniejszych interesów ekonomicznych.

Wspomniane kwestie uregulowano w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228) – zwanej w dalszej części artykułu ustawą oraz rozporządzeniach wydanych na jej podstawie. Zawarte w nich przepisy dotyczą następujących podmiotów:

a) organów władzy publicznej, w tym: Sejmu, Senatu, Prezydenta RP, organów administracji rządowej, organów jednostek samorządu terytorialnego, Narodowego Banku Polskiego;
b) innych podległych im lub nadzorowanych jednostek organizacyjnych;
c) sądów i trybunałów;

[1] W polskim systemie prawnym funkcjonuje kilkadziesiąt rodzajów tajemnic prawnie (ustawowo) chronionych. Szerzej: S. Hoc, *Ochrona informacji niejawnych i innych tajemnic prawnie chronionych– wybrane zagadnienia*, Wyd. Uniwersytetu Opolskiego, Opole 2006, s. 175–263.

d) organów kontroli państwowej i ochrony prawa;
e) jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;
f) państwowych osób prawnych i innych niż wymienione w lit. a–e – państwowych jednostek organizacyjnych;
g) jednostek organizacyjnych podległych organom władzy publicznej lub nadzorowanych przez te organy;
h) przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujących takie umowy oraz wykonujących zadania związane z dostępem do informacji niejawnych na podstawie przepisów prawa[2].

Oznacza to, że przepisom tym będą podlegać nie tylko funkcjonariusze publiczni, ale także podmioty prywatne, prowadzące działalność gospodarczą. Wspomniana ustawa zawiera również definicję informacji niejawnych o charakterze materialnym, opartą na korelacji dwóch czynników: treści informacji oraz możliwych skutków ich ujawnienia. Do ww. grupy zaliczymy informacje z zakresu:
1) ochrony niepodległości, suwerenności oraz integralności terytorialnej Polski;
2) bezpieczeństwa wewnętrznego oraz ochrony porządku konstytucyjnego;
3) sojuszy i pozycji międzynarodowej kraju;
4) gotowości obronnej;
5) interesów ekonomicznych Polski;
6) danych identyfikujących funkcjonariuszy, żołnierzy oraz pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, wykonującym czynności operacyjno-rozpoznawcze,
7) danych o działaniach funkcjonariuszy, żołnierzy lub pracowników, w zakresie wykonywanych przez nich czynności operacyjno-rozpoznawczych;
8) danych osób udzielających pomocy wspomnianym osobom opisanym w punktach 6–7;
9) informacji na temat świadków koronnych, osób im najbliższych oraz świadków, o których mowa w art. 184 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555 z późn. zm.), lub osób dla nich najbliższych.

Niezbędne jest także prawdopodobieństwo wystąpienia szkody, spowodowanej nieuprawnionym ujawnieniem informacji. Przy czym stopień owej szkody bezpośrednio wpływa na przypisanie określonej klauzuli. Ocena (klasyfikacja) informacji

[2] W stosunku do poprzedniej ustawy usunięto z grupy podmiotów objętych jej działaniem jednostki naukowe i badawczo-rozwojowe. Jest to spowodowanie ich likwidacją lub przekształceniem. Zob.: T. Szewc, *Ochrona informacji niejawnych. Komentarz,* Wydawnictwo C. H. Beck 2007, s. 63–68.

pod względem niejawności polega na porównaniu jej cech z treścią definicji ustawowej. Czynności tej dokonują osoby uprawnione do podpisywania dokumentów lub materiałów[3].

W ustawie przewidziano cztery klauzule tajności: „ściśle tajne", „tajne", „poufne", „zastrzeżone". Trzeba przy tym pamiętać, że ochronie podlegają informacje bez względu na ich substrat materialny (postać). W szczególności w formie dokumentu, przedmiotu (np. wyposażenia, urządzenia), strumienia lub zbioru danych, obrazu i dźwięku (lub ich nośnika).

W ustawie opisano cztery elementy, tworzące krajowy system ochrony informacji niejawnych w Polsce:

– bezpieczeństwo osobowe oparte na ścisłej kontroli dostępu osób fizycznych do informacji niejawnych;
– bezpieczeństwo fizyczne oparte na stosowaniu środków ochrony fizycznej i technicznej – adekwatnych do potrzeb konkretnej jednostki organizacyjnej. Dobór wspomnianych jest poprzedzony identyfikacją i oceną zagrożeń dla informacji niejawnych;
– bezpieczeństwo teleinformatyczne – oparte na zastosowaniu akredytowanych i certyfikowanych systemów teleinformatycznych oraz narzędzi kryptograficznych;
– bezpieczeństwo przemysłowe – łączące ww. elementy w spójny zbiór działań przewidywanych dla przedsiębiorców.

Na polski system prawny wpływają również akty prawa międzynarodowego, których stroną jest nasz kraj. Wynika to z członkostwa Polski w Unii Europejskiej i NATO oraz współpracy cywilno-wojskowej z innymi państwami. Są to m.in.:

– umowy dwustronne pomiędzy Polską a innymi krajami (np. Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Litewskiej *w sprawie wzajemnej ochrony informacji niejawnych,* podpisana w Warszawie dnia 12 maja 2008 r., Dz. U. z 2009 r. Nr 117, poz. 9808, czy też Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Federacji Rosyjskiej *o wzajemnej ochronie informacji niejawnych*, podpisana w Moskwie dnia 8 lutego 2008 r., Dz. U. Nr 217, poz. 1384);
– akty prawa międzynarodowego związane z członkostwem Polski w organizacjach międzynarodowych (np. Umowa między Stronami Traktatu Północnoatlantyckiego *o ochronie informacji*, sporządzona w Brukseli dnia 6 marca 1997 r., Dz. U. z 2000 r. Nr 64, poz. 740 oraz umowa między Stronami Traktatu

[3] Uznanie informacji za niejawną jest równoznaczne z zakazem jej udzielania na podstawie art. 2 ustawy z dnia 6 września 2001 r. *o dostępie do informacji publicznej*, Dz. U. Nr 112, poz. 1198 z późn. zm.

Północnoatlantyckiego o współpracy w dziedzinie informacji atomowych sporządzona w Paryżu dnia 18 czerwca 1964 r., Dz. U. z 2001 r. Nr 143, poz.1594);
– wewnętrzne uregulowania organizacji międzynarodowych, do których przynależy Polska (np. Decyzja Komisji 1999/218/WE z 25 lutego 1999 r. odnosząca się do procedur, w ramach których urzędnicy i pracownicy Komisji Europejskiej mogą uzyskiwać dostęp do informacji niejawnych będących w posiadaniu Komisji [notyfikowana jako dokument C(1999) 423] (Dz. Urz. WE L 80 z 25.03.1999 r.); Regulamin Komisji (C(2000) 3614) z 29 listopada 2000 r. (Dz. Urz. WE L 308 z 08.12.2000 r. z późn. zm.); Decyzja Rady 2011/292/EU z 31 marca 2011 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz. U. UE L 141 z 27.05.2011 r.).

Decyzja 2011/292/EU dotyczy przypadków, w których Rada, jej organy przygotowawcze oraz Sekretariat Generalny, wykorzystują informacje niejawne UE. Również państwa członkowskie (oraz ich organy i pracownicy) powinny przestrzegać zawartych tam przepisów w kontaktach z Radą (zgodnie z krajowymi przepisami ustawowymi i wykonawczymi). Za informacje niejawne UE uznaje się wszelkie informacje lub materiały objęte klauzulą tajności, których nieuprawnione ujawnienie mogłoby w różnym stopniu wyrządzić szkodę interesom Unii Europejskiej lub interesom co najmniej jednego państwa członkowskiego. Przyjęto następujące klauzule dla tych informacji: tres secret UE/EU top secret (odpowiednik klauzuli „ściśle tajne" w prawie polskim), secret UE/EU secret (odpowiednik klauzuli „tajne"), confidentiel UE/EU confidential (odpowiednik klauzuli „poufne"), restreint UE/EU restricted („zastrzeżone"). W decyzji zawarto kluczowe reguły zarządzania informacjami niejawnymi dotyczące ich oznaczania, oceny ryzyka, wymaganych środków i dokumentacji bezpieczeństwa. Wskazano zasady postępowania w zakresie bezpieczeństwa osobowego, fizycznego, teleinformatycznego, przemysłowego. Wyżej wymieniona decyzja Rady została przyjęta również przez Europol i Eurojust. Wymienione reguły stosuje się także, jeśli państwo członkowskie przekazuje strukturom Unii Europejskiej krajowe informacje niejawne, o równorzędnej klauzuli tajności. Systemem ochrony bezpośrednio zarządza Biuro ds. Bezpieczeństwa Sekretariatu Generalnego Rady. Nad przestrzeganiem wspomnianych przepisów czuwa również Komitet ds. Bezpieczeństwa, który analizuje i ocenia zagadnienia bezpieczeństwa. W jego skład wchodzą przedstawiciele KWB państw członkowskich, w obradach uczestniczy przedstawiciel Komisji Europejskiej i Europejskiej Służby Działań Zewnętrznych. Komitetowi przewodzi Sekretarz Generalny lub wyznaczona przez niego osoba. Zebrania zwołuje Rada, Sekretarz Generalny lub KWB[4].

[4] KWB – Krajowa Władza Bezpieczeństwa – organ upoważniony przez państwo członkowskie do jego reprezentowania w sprawach bezpieczeństwa informacji niejawnych

Regulamin Komisji Europejskiej (C(2000) 3614) dotyczy funkcjonowania tej instytucji. Zagadnieniom ochrony informacji poświęcono załącznik pn. „Zasady bezpieczeństwa Komisji". Przewidziano w nim powołanie członka Komisji odpowiedzialnego za zapewnienie przestrzegania zasad poufności przez urzędników, pracowników oraz osoby delegowane do pracy w Komisji we wszystkich jej obiektach (w tym przedstawicielstwach). Za stosowanie środków ochrony odpowiada wyspecjalizowana dyrekcja oraz rada ds. bezpieczeństwa. Kontrola poufności obejmuje również współpracę z podmiotami zewnętrznymi – w tym z państwa członkowskimi oraz innymi kontrahentami publicznymi i prywatnymi. W takim przypadku udostępnienie informacji niejawnych UE strukturom zewnętrznym jest możliwe dopiero po przedstawieniu zapewnienia, że stosują one środki i zasady ochrony poufności odpowiadające przepisom Komisji. W przypadku zawierania umów z tymi strukturami Komisja powinna umieścić w nich stosowne gwarancje przestrzegania zasad bezpieczeństwa. Podstawą działalności Komisji w tym zakresie są następujące zasady ogólne: legalność, przejrzystość, odpowiedzialność, pomocniczość. Legalność oznacza obowiązek przestrzegania prawa z uwzględnieniem przepisów dyscyplinarnych i karnych. Przejrzystość nakazuje zapewnienie jednoznaczności wszelkich uregulowań w zakresie bezpieczeństwa. W praktyce oznacza to potrzebę opracowania zrozumiałych procedur dotyczących środków bezpieczeństwa. Odpowiedzialność oznacza, że w sferze bezpieczeństwa mogą istnieć tylko precyzyjnie określone zakresy obowiązków. Co więcej, wymaga się regularnego sprawdzania, czy przewidziane obowiązki są egzekwowane. Pomocniczość, oznacza, że struktury bezpieczeństwa należy tworzyć na najniższym możliwym poziomie organizacji – lecz tylko tam gdzie są one niezbędne. Oznacza to również, że środki ochrony muszą być adekwatne do znaczenia informacji oraz do faktycznych lub potencjalnych zagrożeń, powodując możliwie najmniejsze utrudnienia działania. Zadeklarowano pełną zgodność regulaminu z przepisami zawartymi w decyzji Rady.

Przepisy NATO zawarto w umowie między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzonej w Brukseli dnia 6 marca 1997 r. (Dz. U. z 2000 r. Nr 64, poz. 740). Strony zobowiązały się do ochrony informacji wytwarzanych przez instytucje traktatu oraz udostępnianych tym instytucjom przez państwa członkowskie lub od nich otrzymywanych. Podstawowe zasady ochrony są

– w Polsce rolę tę pełni Szef ABW. W sferze wojskowej działa za pośrednictwem Szefa SKW. Główne zadania to: wdrożenie standardów bezpieczeństwa NATO i UE, zapewnienie właściwego poziomu ochrony informacji niejawnych NATO i UE, nadzorowanie systemu ochrony w stosunkach Polski z innymi państwami lub organizacjami międzynarodowymi, współpraca ze strukturami bezpieczeństwa wspomnianych organizacji oraz KWB innych państw (art. 11 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych).

zbieżne ze standardami Unii Europejskiej, której przepisy wzorowano na uregulowaniach traktatu. W umowie określono jako niejawne informacje lub materiały, wymagające ochrony przed nieuprawnionym ujawnieniem, oznaczone odpowiednimi klauzulami. W nomenklaturze NATO przyjęto następujące klauzule tajności: Cosmic top secret (odpowiednik polski to: ściśle tajne), NATO secret (odpowiednik polski: tajne), NATO confidential (odpowiednik: poufne), NATO restricted (odpowiednik: zastrzeżone)[5].

Organami odpowiedzialnymi za wdrożenie i przestrzeganie zasad ochrony są: Komitet Bezpieczeństwa (NATO Security Comitee – NSC), Sekretarz Generalny, oraz podległe mu Biuro Bezpieczeństwa (NATO Security Office – NOS)[6]. Na podstawie umowy sporządzono dokument C-M(2002)49 z 17 czerwca 2002 r. z późn. zm. – „Bezpieczeństwo w ramach organizacji Traktatu Północnoatlantyckiego" oraz dyrektywy wykonawcze:

– AC/35-D/2000 – Dyrektywa Bezpieczeństwa Osobowego;
– AC/35-D/2001 – Dyrektywa Bezpieczeństwa Fizycznego;
– AC/35-D/2002 – Dyrektywa Bezpieczeństwa Obiegu Informacji;
– AC/35-D/2003 – Dyrektywa Bezpieczeństwa Przemysłowego;
– AC/35-D/2004 – Dyrektywa podstawowa INFOSEC;
– AC/35-D/2005 – Dyrektywa zarządzania INFOSEC w systemach Teleinformatycznych (CIS).

Wspomniane przepisy wpływają na ochronę informacji niejawnych – np. w związku z koniecznością powołania KWB oraz wydania dokumentów

[5] Dokumenty zawierające informacje atomowe Stanów Zjednoczonych noszą oznaczenia NATO oraz klauzule bezpieczeństwa równorzędne do nadanych przez USA przed wyrazem *ATOMAL* oraz adnotację: „Dokument ten zawiera informacje atomowe Stanów Zjednoczonych (Dane Zastrzeżone lub Dane Uprzednio Zastrzeżone) udostępnione w ramach *Umowy NATO o współpracy w dziedzinie informacji atomowych,* podpisanej 18 czerwca 1964 r., i będzie podlegał właściwej ochronie".

[6] W skład Urzędu Sekretarza Generalnego wchodzą: Sekretariat Wykonawczy, Biuro Informacji i Prasy oraz Biuro Bezpieczeństwa NATO. Biuro Bezpieczeństwa koordynuje, monitoruje i realizuje politykę bezpiecznego funkcjonowania Sojuszu. Dyrektor biura pełni funkcję głównego doradcy Sekretarza Generalnego do spraw bezpieczeństwa oraz przewodniczy Komitetowi Bezpieczeństwa NATO, kieruje służbą Ochrony Kwatery Głównej NATO i odpowiada za koordynację ochrony NATO. Działa również organ konsultacyjny dla służb bezpieczeństwa państw członkowskich NATO – Cywilny Komitet Wywiadowczy (Civilian Intelligence Committee), przygotowując raporty o zagrożeniach dla Sojuszu i doradzając Radzie Północnoatlantyckiej. Szerzej w: *NATO Handbook. Part III – Nato's civilian and military structures*, wyd. NATO Public Diplomacy Division, Bruksela 2006, s. 73–84 i 134.

poświadczających dostęp osób fizycznych do informacji niejawnych Unii Europejskiej i NATO[7].

## Bezpieczeństwo osobowe

Uregulowania dotyczące bezpieczeństwa osobowego umieszczono w rozdziale 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228). Najistotniejszym jej elementem jest wprowadzenie zasady udzielania dostępu do informacji niejawnych tylko osobom upoważnionym, spełniających łącznie trzy warunki. Pierwszym z nich jest posiadanie ważnego poświadczenia bezpieczeństwa, pisemnego upoważnienia lub przynależność do grupy osób zwolnionych z tego obowiązku. Drugim jest udział w szkoleniu specjalistycznym z zakresu ochrony informacji niejawnych. Trzecim warunkiem jest, aby dostęp do informacji był związany z wykonaniem zadań służbowych[8].

Dostęp do informacji oznaczonych klauzulą „zastrzeżone", wiąże się z wydaniem pisemnego upoważnienia. Czyni to kierownik jednostki organizacyjnej. W treści ustawy nader skąpo opisano treść oraz zasięg czasowy ważności tego dokumentu. Należy przyjąć że powinno ono zawierać następujące elementy: miejsce i datę wydania, podstawę prawną, dane osoby upoważnionej, zakres przyznanych uprawnień (określony przez wskazanie klauzuli tajności), zakres czasowy obowiązywania – w postaci terminu ważności lub zwrotu „wydano na czas zatrudnienia", podpis osoby udzielającej upoważnienia. Nie dotyczy to kierownika jednostki organizacyjnej, który automatycznie uzyskuje dostęp do informacji oznaczonych klauzulą „zastrzeżone", z tytułu zajmowanego stanowiska. W związku z wydawaniem upoważnień nie przeprowadza się dodatkowych procedur sprawdzających. Przyczyną utraty upoważnienia może być naruszenie przepisów o ochronie informacji niejawnych oraz ustanie potrzeby jego dalszego posiadania[9]. Odwołanie upoważ-

[7] W dniu 31.12.2010 r. Szef ABW działając jako Krajowa Władza Bezpieczeństwa wydał wytyczne w sprawie postępowania z informacjami niejawnymi międzynarodowymi.

[8] „Cytowany przepis art. 3 ustawy o ochronie informacji niejawnych wskazuje na konieczność – co jest istotne w sprawie – istnienia niezbędności żądanej informacji do wykonywania przez daną osobę pracy lub pełnienia służby na zajmowanym stanowisku. Posiadanie uprawnień do dostępu do informacji niejawnej (stosowny certyfikat) nie jest wystarczające, jeżeli dostęp do nich nie jest związany z wykonywaniem pracy lub pełnieniem służby na zajmowanym stanowisku" (z wyroku WSA w Warszawie z 14 sierpnia 2007 r. sygn. II SA/Wa 280/07).

[9] W ustawie nie uregulowano powyższej kwestii. Należy więc przyjąć ogólne zasady w tym zakresie.

nienia powinno nastąpić w formie analogicznej, do jego udzielenia tj. na piśmie. W ustawie nie przewidziano możliwości wniesienia odwołania od rozstrzygnięcia w tej sprawie. Co prowadzi do wniosku, że środek odwoławczy w takim przypadku nie przysługuje

Udzielania dostępu do informacji wyższych klauzul („poufne", „tajne", „ściśle tajne") powinno zostać poprzedzone postępowaniem sprawdzającym i wydaniem odrębnego dokumentu – poświadczenia bezpieczeństwa. Celem postępowania jest ustalenie czy osoba sprawdzana daje rękojmię zachowania tajemnicy. Pojęcie rękojmi zdefiniowano w art. 2 pkt 2 ustawy jako zdolność do spełnienia wymogów wymienionych w ustawie dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem.

Udzielenie dostępu do informacji oznaczonych klauzulą „poufne" wymaga przeprowadzenia zwykłego postępowania sprawdzającego. Natomiast poszerzone postępowanie sprawdzające przeprowadza się w przypadku udzielania dostępu do informacji o klauzuli „tajne", „ściśle tajne". Podlegają mu również obowiązkowo pełnomocnicy ds. ochrony, kandydaci na to stanowisko oraz kierownicy jednostek organizacyjnych, w których przetwarza się informacje niejawne co najmniej „poufne"[10].

Zwykłe postępowania sprawdzające przeprowadzają pełnomocnicy ds. ochrony informacji niejawnych. Czynią to wobec osób zatrudnionych we własnych jednostkach organizacyjnych. Podstawą czynności jest polecenie kierownika jednostki wydane na piśmie.

Poszerzone postępowania sprawdzające przeprowadzają:

- Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego – zgodnie z kompetencjami ustawowymi opisanymi w art. 10 ustawy;
- Agencja Wywiadu, CBA, Biuro Ochrony Rządu, Policja, Służba Więzienna, Służba Wywiadu Wojskowego, Straż Graniczna oraz Żandarmeria Wojskowa. Czynią to wobec własnych funkcjonariuszy, żołnierzy i pracowników oraz osób ubiegających się o przyjęcie do służby lub pracy i osób wykonujących czynności zlecone lub ubiegających się o ich wykonywanie (art. 23 ust. 5 ustawy o ochronie informacji niejawnych)[11].

---

[10] Postępowania sprawdzające są szczególną odmianą postępowań administracyjnych. Szerzej: T. Szewc, *Publicznoprawna ochrona informacji,* Wydawnictwo C. H. Beck, Warszawa 2007, s. 152–180.

[11] Poświadczenia wydane w ten sposób zachowują ważność jedynie przez czas pracy lub służby w powyższych instytucjach. Nie dotyczy to jednak poświadczeń wydanych pod rządami poprzedniej ustawy – tj. do dnia 1 stycznia 2011 r. Wynika to z treści przepisów intertemporalnych zawartych w art. 182 wspomnianej ustawy.

Czynności polegają na sprawdzeniu informacji zawartych w rejestrach, ewidencjach i kartotekach (obowiązkowo w Krajowym Rejestrze Karnym). Dokonuje się również sprawdzeń w ewidencjach powszechnie niedostępnych (pozostających we władaniu służb specjalnych).

Zakres postępowań poszerzonych jest większy i może objąć badanie rachunków bankowych, dokumentów podatkowych, zobowiązań finansowych osoby sprawdzanej, kontrolę dokumentacji medycznej, wywiad środowiskowy. W szczególnych wypadkach można również żądać poddania się specjalistycznym badaniom lekarskim.

Podstawą ww. działań są przede wszystkim informacje zawarte w ankiecie bezpieczeństwa osobowego sporządzonej przez osobę sprawdzaną.

W obu przypadkach procedura może się zakończyć:
- wydaniem poświadczenia bezpieczeństwa;
- odmową wydania poświadczenia bezpieczeństwa;
- umorzeniem postępowania (przyczyny wymieniono w art. 31 ustawy).

Poświadczenia bezpieczeństwa wydaje się na czas oznaczony, odmienny dla każdej z klauzul. Dla klauzuli „ściśle tajne" zapewnia ono dostęp do informacji niejawnych:
a) oznaczonych jako „ściśle tajne" – przez okres 5 lat od daty wystawienia;
b) oznaczonych jako „tajne" – przez okres 7 lat;
c) oznaczonych jako „poufne" – przez okres 10 lat.

Dla klauzuli „tajne" zapewnia dostęp do informacji niejawnych o klauzuli:
a) oznaczonych jako „tajne" – przez okres 7 lat;
b) oznaczonych jako „poufne" – przez okres 10 lat.

W przypadku klauzuli „poufne" – poświadczenie pozostaje ważne przez 10 lat[12].

Poświadczenie umożliwiające dostęp do informacji o wyższej klauzuli umożliwia dostęp także do informacji o niższej klauzuli (określa się to niekiedy jako „kaskadowość" jego obowiązywania). Postępowanie powinno trwać nie dłużej niż 3 miesiące, licząc od daty złożenia ankiety bezpieczeństwa osobowego. Termin ten ma charakter instrukcyjny.

Kierownicy jednostek organizacyjnych opisanych w ustawie mogą udzielać jednorazowej zgody na udostępnienie takiej informacji lub wydać zgodę tymczasową

[12] W latach 1999–2005 (tj. pod rządami poprzedniej ustawy z dnia 22 stycznia 1999 o ochronie informacji niejawnych – Dz. U. Nr 11, poz. 95) stosowano inne terminy ważności poświadczeń. Było to 3 lata dla klauzuli „ściśle tajne", 5 lat dla klauzuli „tajne". W przypadku informacji oznaczonych jako „poufne" i „zastrzeżone" termin wynosił tak jak obecnie 10 lat. Po dokonaniu jej nowelizacji wydłużono termin ważności wydanych uprzednio dokumentów.

osobie, wobec której wszczęto już postępowanie sprawdzające na czas trwania tego postępowania (art. 34 ust. 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych). Zgoda tymczasowa jest ważna przez okres trwania wspomnianego postępowania. Pozostali kierownicy jednostek organizacyjnych mogą wydać zgodę tymczasową tylko do klauzuli „poufne".

W art. 34 ww. ustawy wskazano grupę osób wyłączonych spod działania zwykłych procedur sprawdzających. Należy do niej m.in. Prezydent RP, Marszałkowie Sejmu i Senatu, Premier, ministrowie, posłowie i senatorowie. Ponadto Prezydent RP i Premier w stanach nadzwyczajnych mogą wyrazić zgodę na odstąpienie od przeprowadzenia postępowania sprawdzającego.

Organ prowadzący postępowanie odmawia przyznania poświadczenia jeśli osobę sprawdzaną skazano prawomocnym wyrokiem sądu na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, lub umyślne przestępstwo skarbowe (jeżeli czyn sprawcy, wywołuje poniższe wątpliwości). Ponadto, powodem odmowy jest wystąpienie nie dającej się usunąć wątpliwości opisanej w art. 24 ust. 2 i 3 ww. ustawy (dotyczącej m.in.: prawdopodobnej działalności terrorystycznej, sabotażowej, szpiegowskiej, zagrożenia ze strony obcych służb specjalnych, przestrzegania porządku konstytucyjnego, uczestnictwa i wspierania działalności zakazanych partii lub innych organizacji, o których mowa w art. 13 Konstytucji RP, ukrywania informacji ważnych dla ochrony informacji niejawnych, podatności na szantaż, niewłaściwego postępowania z informacjami niejawnymi). Ponadto dotyczące poziomu życia (w szczególności jeśli przewyższa on poziom dochodów), informacji o zakłóceniach czynności psychicznych lub chorobie psychicznej, które mogą negatywnie wpłynąć na zdolność do wykonywania prac, związanych z dostępem do informacji niejawnych, uzależnienia od alkoholu, środków odurzających lub psychotropowych (tylko w postępowaniu poszerzonym).

Możliwe jest wszczęcie kontrolnego postępowania sprawdzającego, jeżeli po wydaniu poświadczenia bezpieczeństwa pojawią się okoliczności wskazujące, że osoba taka nie daje rękojmi zachowania tajemnicy. Podmiotem uprawnionym jest organ właściwy do przeprowadzenia kolejnego postępowania: pełnomocnik zatrudniony u aktualnego pracodawcy oraz ABW lub SKW w sytuacji uzasadnionej względami bezpieczeństwa państwa. Postępowanie to powinno zostać zakończone w terminie 6 m-cy. Istnieje możliwość jego przedłużenia o dalsze 6 miesięcy. W okresie trwania postępowania kontrolnego osoba sprawdzana nie posiada dostępu do informacji niejawnych[13].

[13] Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 30 listopada 2007 r. II SA/Wa 1350/07 rozstrzygnął sprawę funkcjonariusza Biura Ochrony Rządu, któremu prawomocną decyzją cofnięto poświadczenie bezpieczeństwa. Zgodnie z art. 23 ust. 4 usta-

Umorzenie postępowania, odmowa wydania poświadczenia bezpieczeństwa lub jego cofnięcie następuje w formie decyzji administracyjnej, wydawanej przez organ prowadzący postępowanie. W tej sytuacji zastosowanie znajdują przepisy art. 3 i art. 30 ustawy oraz art. 104 Kodeksu postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071, z późn. zm.). Prawo do wniesienia odwołania zawsze posiada osoba objęta postępowaniem sprawdzającym – której dotyczy umorzenie, odmowa wydania poświadczenia bezpieczeństwa lub jego cofnięcie[14].

W odniesieniu do decyzji wydawanych z zastosowaniem przepisu art. 23 ust. 5 ustawy w Policji, BOR, Żandarmerii Wojskowej, Straży Granicznej, Agencji Wywiadu, Służbie Więziennej, Centralnym Biurze Antykorupcyjnym, Służbie Wywiadu Wojskowego (wymienione instytucje prowadzą samodzielnie postępowania sprawdzające wobec osób tam służących, zatrudnionych oraz ubiegających się o pracę lub przyjęcie do służby) oraz ABW i SKW – organem odwoławczym jest Prezes

---

wy z 16 marca 2001 r. *o Biurze Ochrony Rządu* (Dz. U. z 2004 r. Nr 163, poz. 1712 ze zm.) warunkiem pozostawania w służbie czynnej funkcjonariuszy tej formacji jest posiadanie ważnego poświadczenia bezpieczeństwa. W wyroku podkreślono, że brak dostępu do informacji niejawnych będący następstwem wszczęcia postępowania kontrolnego nie stanowi wystarczającej przesłanki do zwolnienia ze służby. Jest to to możliwe dopiero po uprawomocnieniu się decyzji o cofnięciu poświadczenia.

[14] W art. 42 ust. 1 ustawy z dnia 22 stycznia 1999 r. *o ochronie informacji niejawnych* (Dz. U. Nr 11, poz. 95) zapisano, że do postępowania sprawdzającego nie mają zastosowania przepisy Kodeksu postępowania administracyjnego i przepisy o zaskarżaniu do Naczelnego Sądu Administracyjnego. Wspomniany przepis został zaskarżony do Trybunału Konstytucyjnego przez Rzecznika Praw Obywatelskich jako niezgodny z następującymi zasadami konstytucyjnymi: prawem do sądu opisanym w art. 45 ust 1, zakazem zamykania drogi sądowej w celu dochodzenia naruszonych wolności i praw – opisane w art. 77 ust. 2 oraz prawo dostępu do służby publicznej – przyznane w art. 60. Trybunał Konstytucyjny wyrokiem z 10 maja 2000 r. (sygn. Akt k. 21/99) uznał kwestionowany przepis za niezgodny z art. 45 i art. 77 Konstytucji RP. Uznając argumentację RPO wskazano również na niezgodność zaskarżonego przepisu z art. 13 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności sporządzonej w Rzymie 4 listopada 1950 r. (Dz. U. z 1993 r. Nr 61, poz. 284). Uznano za niedopuszczalne pozbawienie osoby sprawdzanej jakiegokolwiek skutecznego środka zaskarżenia. W orzeczeniu TK zawarł szereg wniosków, które wpłynęły na treść przepisów dotyczących postępowań odwoławczych. Efektem wspomnianego orzeczenia było uchwalenie ustawy z dnia 3 lutego 2001 r. *o zmianie ustawy o ochronie informacji niejawnych* (Dz. U. Nr 22, poz. 247), która weszła w życie 8 kwietnia 2001 r. Całkowicie zmieniono treść art. 42 oraz uchylono art. 43. Do ustawy wprowadzono rozdział 5a zatytułowany „Postępowanie odwoławcze i skargowe". W art. 48a zapisano: „*osobie sprawdzanej przysługuje skarga do Naczelnego Sądu Administracyjnego, w terminie 30 dni od dnia doręczenia decyzji lub postanowienia*".

Rady Ministrów. W przypadku postępowań prowadzonych przez pełnomocników – organem odwoławczym jest Szef Agencji Bezpieczeństwa Wewnętrznego albo Szef Służby Kontrwywiadu Wojskowego[15]. Podział kompetencji ABW i SKW w rozpatrywania odwołań jest analogiczny do właściwości obu służb w ramach postępowań sprawdzających. Organ odwoławczy wydając decyzję, może rozstrzygać w następujących granicach:

1) utrzymuje w mocy decyzję organu, który przeprowadził postępowanie sprawdzające lub kontrolne postępowanie sprawdzające;
2) uchyla decyzję wydaną w toku kontrolnego postępowania sprawdzającego zakończonego cofnięciem poświadczenia bezpieczeństwa;
3) uchyla decyzję podmiotu, który przeprowadził postępowanie sprawdzające i nakazuje mu wydanie poświadczenia bezpieczeństwa;
4) uchyla decyzję podmiotu, który przeprowadził postępowanie sprawdzające lub kontrolne postępowanie sprawdzające i przekazuje sprawę do ponownego rozpatrzenia;
5) stwierdza nieważność decyzji podmiotu, który przeprowadził postępowanie sprawdzające lub kontrolne postępowanie sprawdzające[16].

Wniesienie odwołania powoduje, że decyzja taka nie przesądza definitywnie o odmowie dostępu do informacji niejawnych. Od decyzji przysługuje ponadto skarga do wojewódzkiego sądu administracyjnego[17].

Warunkiem otrzymania dostępu do informacji niejawnych jest ponadto udział w szkoleniu opisanym w art. 19 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Funkcjonariusze ABW lub SKW szkolą kierowników jednostek organizacyjnych, w których przetwarza się informacje oznaczone klauzulą, co najmniej „tajne" oraz Pełnomocników. Pełnomocnik czyni to wobec pozostałych osób

---

[15] Szerzej H. Sawicka, *Postępowanie odwoławcze od decyzji pełnomocników do spraw ochrony informacji niejawnych – 10 lat doświadczeń szefa ABW jako organu II instancji*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 7 (4), s. 51–66.

[16] Organ prowadzący postępowania sprawdzające może wznowić postępowanie zakończone decyzją ostateczną o odmowie wydania albo o cofnięciu poświadczenia bezpieczeństwa. Warunkiem jest, aby jedynym powodem wydania decyzji było przedstawienie osobie sprawdzanej zarzutu popełnienia przestępstwa, postawienie jej w stan oskarżenia lub skazanie za przestępstwo umyślne (ścigane z oskarżenia publicznego) lub umyślne przestępstwo skarbowe. Jeśli nastąpiło umorzenie lub zakończenie uniewinnieniem wspomnianego postępowania karnego.

[17] Kwestie proceduralne dotyczące odwołań obszerniej poruszył Naczelny Sąd Administracyjny w swojej uchwale z 17.04.2012 r. (sygn. I OPS 1/12).

zatrudnionych we własnej jednostce organizacyjnej lub wykonujących na jej rzecz prace zlecone[18].

Szkolący wydaje uczestnikom pisemne zaświadczenie. Osoba przeszkolona jest ponadto zobowiązana do podpisania oświadczenia o zapoznaniu się z treścią przepisów[19]. Szkolenia należy przeprowadzać cyklicznie – co najmniej raz na 5 lat.

## Bezpieczeństwo fizyczne

Jednostki organizacyjne, przetwarzające informacje niejawne, stosują środki bezpieczeństwa fizycznego opisane w art. 45 ustawy. Ich zakres powinien być dostosowany do klauzul informacji oraz poziomu zagrożeń. Metodykę oceny zagrożeń i standardy bezpieczeństwa opisano w rozporządzeniu Rady Ministrów z dnia 29 maja 2012 r. w prawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. poz. 683). Procedura zapewnienia bezpieczeństwa fizycznego ma charakter dwuetapowy.

W pierwszej kolejności należy dokonać oceny poziomu zagrożeń z uwzględnieniem następujących kryteriów: klauzul tajności przetwarzanych informacji, liczby materiałów niejawnych, postaci informacji, liczby osób (dopuszczonych do informacji niejawnych), lokalizacji miejsc przechowywania, dostępu osób do budynku. Dopuszcza się zastosowanie dodatkowych kryteriów (chodzi tu o czynniki realnie wpływające na bezpieczeństwo: szpiegostwo, pożar, powódź, kradzież). Oceny należy dokonać poprzez przyznanie określonej liczby punktów, która odpowiada istotności każdego kryterium. Suma punktów wpływa na przyporządkowanie jednostki do jednego z trzech poziomów zagrożenia: wysokiego, średniego albo niskiego (związanego z określonym przedziałem punktowym).

W drugim etapie następuje określenie wymagań dla ustalonego uprzednio poziomu zagrożeń. Wymagania zostały zawarte w formie tabel zawierających 6 typów zabezpieczeń: szafy przeznaczone do przechowywania informacji, pomieszczenia, budynki, kontrola dostępu, personel bezpieczeństwa i systemy sygnalizacji włamania i napadu, granice (ogrodzenie, kontrola dostępu). Możliwe jest zastosowanie zmiennych kompilacji środków różnego rodzaju. Oznacza to, że środki ochrony jednego rodzaju mogą zostać uzupełnione zabezpieczeniem innego typu

[18] Zob.: S. Hoc, *Ustawa o ochronie informacji niejawnych. Komentarz,* Wyd. LexisNexis 2010, s. 141–146.

[19] Treść oświadczenia nie została dokładnie określona w ustawie. Należy jednak przyjąć, że powinno w sposób jasny potwierdzać znajomość zasad odpowiedzialności dyscyplinarnej i karnej na wypadek naruszenia przepisów.

o wyższym standardzie. Przy czym niezbędne jest osiągnięcie minimalnej – wymaganej liczby punktów dla wszystkich środków ochrony (dla skonkretyzowanego poziomu zagrożenia i klauzuli przetwarzanych informacji niejawnych).

Swoboda w doborze środków ochrony została ograniczona przez wprowadzenie obowiązkowych elementów, wymienionych w rozdziale 7 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych oraz wspomnianym rozporządzeniu. Należą do nich np. strefy ochronne – obowiązkowe w jednostce przetwarzającej informacje o klauzuli co najmniej „poufne". Strefa III – obejmuje pomieszczenie lub obszar o wyraźnych granicach, w obrębie których dokonuje się kontroli osób i pojazdów. Strefa II – obejmuje pomieszczenie lub obszar, w których przetwarza się informacje niejawne oznaczone klauzulą „poufne" lub wyższą w taki sposób, że wstęp nie umożliwia bezpośredniego dostępu do tych informacji Wstęp do niej możliwy jest tylko z innej strefy ochronnej. Strefa I – obejmuje pomieszczenie lub obszar, w których są przetwarzane informacje o klauzuli „poufne" lub wyższej. Wstęp do niej umożliwia bezpośredni dostęp do tych informacji niejawnych. Wejście do niej jest możliwe tylko ze strefy ochronnej. Jeśli pojawi się konieczność ochrony tajności na najwyższym poziomie wyznacza się ponadto specjalną strefę ochronną – umieszczoną w obrębie strefy I lub II. Jest ona zabezpieczona przed podsłuchem i podglądem oraz musi spełniać następujące wymagania:

- posiada systemu sygnalizacji włamania i napadu;
- pozostaje zamknięta poza czasem użytkowania;
- jest zabezpieczona przed wstępem osób nieuprawnionych;
- podlega regularnym inspekcjom ABW lub SKW (co najmniej raz w roku);
- jest pozbawiona infrastruktury telekomunikacyjnej, telefonów oraz sprzętu elektrycznego i elektronicznego (z wyjątkiem wyposażenia opisanego w dokumentacji bezpieczeństwa).

### Bezpieczeństwo teleinformatyczne

Do przetwarzania informacji niejawnych służą akredytowane systemy teleinformatyczne – tj. specjalnie przygotowane do tego celu.

Zapewnienie bezpieczeństwa obejmuje wszystkie etapy przygotowania i eksploatacji systemu, w tym:

a) planowanie – polegającego na ustaleniu parametrów systemu (tj. jego przeznaczenia, klauzul przetwarzanych informacji, liczby użytkowników, lokalizacji);
b) projektowanie – na tym etapie należy przeprowadzić wstępne oszacowanie ryzyka, dokonać wyboru zabezpieczeń – fizycznych i technicznych oraz uzyskać

ich wstępną akceptację, uzgodnić plan i harmonogram czynności z organem prowadzącym akredytację, opracować dokument pn. „*szczególne wymagania bezpieczeństwa teleinformatycznego*";

c) wdrożenie – na tym etapie należy dokonać zakupu i montażu uprzednio wybranych elementów systemu, w tym narzędzi kryptograficznych, następnie należy opracować dokument pn. „*procedury bezpiecznej eksploatacji*" oraz przeprowadzić akredytację systemu teleinformatycznego;
d) eksploatację – należy zapewnić ciągłość i niezawodność działania systemu oraz zgodność tego działania z dokumentacją bezpieczeństwa;
e) wycofywanie – na tym etapie należy zakończyć eksploatację systemu, powiadomić organ akredytujący zwracając wydane świadectwa akredytacji. Należy również bezpowrotnie usunąć informacje niejawne z systemu, w szczególności przez ich przeniesienie do innego systemu, zarchiwizowanie lub zniszczenie nośników danych.

Akredytacja jest poprzedzona opracowaniem dokumentacji wymienionej w rozporządzeniu Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 159, poz. 948). Akredytacji dokonuje kierownik jednostki organizacyjnej, w której system działa jeśli jest przeznaczony do przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone". W terminie 30 dni przesyła ABW albo SKW dokumentację bezpieczeństwa. Wspomniana służba w ciągu 30 dni przekazuje zalecenia kierownikowi jednostki, jeśli system wymaga zmian. Może również nakazać wstrzymanie dalszego przetwarzania danych[20].

Jeśli system jest dedykowany do przetwarzania informacji oznaczonych klauzulą „poufne" lub wyższą – akredytacji dokonuje ABW albo SKW w formie odrębnego dokumentu na czas określony, nie dłuższy niż pięć lat. Dokumentem tym jest świadectwo akredytacji[21]. ABW i SKW w toku akredytacji przeprowadzają audyt bezpieczeństwa badając najistotniejsze parametry systemu, w tym: usytuowanie

---

[20] Z obowiązku akredytacji zwolniono systemy przeznaczone wyłącznie do pozyskiwania i przekazywaniu w sposób niejawny informacji uzyskanych w toku czynności operacyjno-rozpoznawczych prowadzonych przez uprawnione do tego podmioty. I. Stankowska, *Ustawa o ochronie informacji niejawnych, komentarz.* Wyd. LexisNexis 2010, s. 181–182.

[21] Zasady akredytacji systemów teleinformatycznych uregulowano w art. 60 ustawy z dnia 22 stycznia 1999 r. *o ochronie informacji niejawnych* (Dz. U. Nr 11, poz. 95) w którym nie wyznaczono terminu obowiązywania akredytacji. Należy przyjąć, że pojawienie się nowych przepisów (zawierających taki termin) nakłada obowiązek ponownej akredytacji po upływie 5 lat – także dla systemów dopuszczonych do użytkowania na podstawie poprzednich przepisów (tj. bezterminowo).

urządzeń, systemy zabezpieczeń (w tym organizację stref ochronnych, zastosowane zabezpieczenia techniczne) oraz struktury zarządzania. W systemach przeznaczonych do przetwarzania informacji o klauzuli „poufne" lub wyższej należy zastosować środki ochrony elektromagnetycznej, certyfikowane przez ABW i SKW. Certyfikaty są wydawane na okres nie krótszy niż 3 lata. Dokumentację bezpieczeństwa bada wewnętrzna jednostka akredytacyjna ABW albo SKW. Możliwe jest odstąpienie od audytu jeśli system jest przeznaczony do przetwarzania informacji o klauzuli „poufne". W ustawie nie wskazano przesłanek podjęcia takiej decyzji. Zwykle następuje to w sytuacji, gdy zastosowane środki ochrony znacznie przewyższają wymagania w tym zakresie. W obecnym stanie prawnym nie przysługuje odwołanie od odmowy akredytacji.

W toku sporządzania szczególnych wymagań bezpieczeństwa należy przeprowadzić szacowanie ryzyka dla bezpieczeństwa informacji niejawnych. Obejmuje ono analizę ryzyka, na którą składają się: jego identyfikacja, określenie wielkości ryzyk, ich ocena. Identyfikację ryzyka powinna uwzględniać: zasoby systemu teleinformatycznego (liczbę i klauzule dokumentów), realne zagrożenia, podatności, zabezpieczenia, skutki wystąpienia incydentu bezpieczeństwa. W procesie określania wielkości ryzyk należy wyznaczyć ich poziomy. W procesie oceny należy porównać wyznaczone poziomy ryzyka z tymi, które można zaakceptować oraz podjąć decyzję co do dalszego z nimi postępowania. Szacowanie powinno zostać ponowione w przypadku wprowadzania istotnych zmian w systemie, w przypadku wykrycia nowych zagrożeń oraz cyklicznie w ramach zarządzania bezpieczeństwem. Kierownik jednostki organizującej system odpowiada za zapewnienie ciągłości procesu zarządzania ryzykiem.

Osoby odpowiedzialne za działanie systemu teleinformatycznego wyznacza wspomniany kierownik jednostki. Są nimi administrator systemu teleinformatycznego oraz inspektor bezpieczeństwa teleinformatycznego. Osoby te powinny posiadać dostęp do informacji niejawnych o klauzuli nie niższej niż klauzula przetwarzanych informacji niejawnych. Muszą również przejść szkolenie zorganizowane przez ABW oraz udokumentowane pisemnym zaświadczeniem. Obowiązki związane tymi stanowiskami powinny zostać opisane w dokumentacji bezpieczeństwa systemu. Administrator jest odpowiedzialny za jego właściwe funkcjonowanie oraz bezpieczeństwo przetwarzania informacji, wdrożenie zabezpieczeń, nadzór nad kontami użytkowników, utrzymanie zgodności systemu z jego dokumentacją, szkolenie użytkowników, dokumentowanie czynności w dzienniku administratora. Inspektor odpowiada za udostępnianie stanowiska użytkownikom, bieżącą kontrolę zgodności funkcjonowania systemu z dokumentacją, prowadzenie dziennika systemu teleinformatycznego. Wspomniane osoby uczestniczą w opracowaniu i aktualizacji

dokumentacji bezpieczeństwa. Należy pamiętać, że użytkownicy systemów są zobowiązani do ścisłego przestrzegania treści wykonanej dokumentacji bezpieczeństwa oraz poleceń ww. osób.

## Bezpieczeństwo przemysłowe

Bezpieczeństwem przemysłowym nazywamy przedsięwzięcia mające na celu zapewnienie ochrony informacji niejawnych przetwarzanych przez przedsiębiorcę w toku wykonania umów lub zadań powierzonych mu na podstawie przepisów prawa. Przedmiotem ochrony są informacje niejawne oraz system organizacyjno-techniczny. Podmiotem może być również przedsiębiorca ubiegający się o dostęp do informacji.

Jeśli wykonanie zadań jest związane z przetwarzaniem informacji niejawnych oznaczonych klauzulą „poufne", „tajne" lub „ściśle tajne", przedsiębiorca musi uzyskać odpowiednie świadectwo bezpieczeństwa przemysłowego. Obowiązek ten nie dotyczy osób fizycznych prowadzących działalność gospodarczą jednoosobowo (osobiście). Osoby te wykonują zadania na podstawie poświadczenia bezpieczeństwa. Świadectwo bezpieczeństwa poświadcza zdolność przedsiębiorcy do zapewnienia ochrony informacji niejawnych, przed nieuprawnionym ujawnieniem. Dokument ten przyznaje Agencja Bezpieczeństwa Wewnętrznego albo Służba Kontrwywiadu Wojskowego po przeprowadzeniu postępowania bezpieczeństwa przemysłowego, które ma na celu ustalenie, czy przedsiębiorca jest zdolny do należytej ochrony informacji niejawnych. Badaniu podlegają kwestie: finansowe, organizacyjne oraz kadrowe. W ramach procedur przeprowadza się postępowania sprawdzające wobec osób, które uzyskają dostęp do informacji niejawnych. Natomiast obowiązkiem zleceniodawcy zadania jest wprowadzenie do treści umowy lub zlecenia instrukcji bezpieczeństwa przemysłowego, w której zawarte są wymagania dotyczące ochrony informacji niejawnych, skutki oraz zakres odpowiedzialności z tytułu niewykonania obowiązków wynikających z ustawy lub instrukcji.

Jeśli przedsiębiorca zamierza przetwarzać informacje niejawne oznaczone klauzulą „poufne" lub wyższą powinien złożyć do ABW lub SKW wniosek o przeprowadzenie postępowania bezpieczeństwa przemysłowego. Procedura obejmuje sprawdzenie źródeł finansowania przedsiębiorcy (w tym struktury kapitału i powiązań w tym zakresie), pochodzenia środków finansowych i sytuacji finansowej oraz osób wchodzących w skład organów zarządzających i kontrolnych (lub działających z ich upoważnienia). W uzasadnionych wypadkach sprawdzeniu podlegają również osoby dysponujące aktualnymi poświadczenia bezpieczeństwa. Ocenie poddaje się

strukturę organizacyjną oraz system ochrony informacji niejawnych. Powyższych czynności dokonuje się na podstawie kwestionariusza, który wnioskodawca wypełnia i przekazuje ABW albo SKW.

W toku wspomnianej procedury przeprowadza się postępowania sprawdzające wobec następujących osób:

– kierownika przedsiębiorcy;
– pełnomocnika ochrony lub jego zastępcy oraz pracowników pionu ochrony;
– administratora systemu oraz inspektora bezpieczeństwa teleinformatycznego;
– pozostałych osób, które powinny mieć dostęp do informacji niejawnych.

Postępowanie powinno trwać nie dłużej niż 6 miesięcy, licząc od daty złożenia przez przedsiębiorcę wszystkich niezbędnych dokumentów. Czynności przeprowadza się w oparciu o dane zawarte w rejestrach i ewidencjach, w tym również niedostępnych powszechnie.

Postępowanie może się zakończyć:

– wydaniem świadectwa bezpieczeństwa przemysłowego;
– umorzeniem postępowania;
– odmową wydania świadectwa (przyczyny wymieniono w art. 64 ustawy o ochronie informacji niejawnych).

Świadectwo bezpieczeństwa przemysłowego występuje w trzech odmianach, zależnie od stopnia zdolności do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej:

1) pierwszego stopnia – jeśli potwierdza pełną zdolność do ochrony tych informacji;
2) drugiego stopnia – jeśli potwierdza zdolność do ochrony informacji, z wyłączeniem możliwości ich przetwarzania we własnych systemach teleinformatycznych;
3) trzeciego stopnia – jeśli potwierdza zdolność do ochrony informacji, z wyłączeniem możliwości ich przetwarzania w obiektach użytkowanych przez przedsiębiorcę.

Świadectwo zachowuje ważność przez określony czas, odmienny dla każdej z klauzul. Jest to:

– 10 lat w przypadku informacji oznaczonych klauzulą „poufne";
– 7 lat w przypadku informacji oznaczonych klauzulą „tajne";
– 5 lat w przypadku informacji oznaczonych klauzulą „ściśle tajne.

ABW oraz SKW mają prawo cofnięcia świadectwa bezpieczeństwa przemysłowego jeśli wspomniane powody ujawnią się w toku dokonywanych przez te instytucje – sprawdzeń lub kontroli przestrzegania zasad bezpieczeństwa przez przedsiębiorcę. Umorzenie, odmowa przyznania świadectwa bezpieczeństwa prze-

mysłowego oraz jego cofnięcie mają charakter decyzji administracyjnej, od której przysługuje odwołanie do Prezesa Rady Ministrów oraz skarga do sądu administracyjnego na podstawie K.p.a. Zakres orzekania jest analogiczny jak w przypadku bezpieczeństwa osobowego.

W stosunku do przepisów obowiązujących w latach 1999–2010 nastąpiło zmniejszenie liczby niezbędnych procedur oraz dokumentacji. W szczególności uproszczono dostęp do informacji oznaczonych klauzulą „zastrzeżone" (po rezygnacji z postępowań sprawdzających w tym zakresie). Ograniczono wymóg posiadania kancelarii tajnej wyłącznie do jednostek przetwarzających informacje o najwyższych klauzulach („tajne" i „ściśle tajne"). Zlikwidowano również obowiązek prowadzenia wykazu stanowisk i prac związanych z dostępem do informacji niejawnych oraz wykazu tychże informacji[22].

Obowiązujące rozwiązania należy uznać za nowoczesne oraz spełniające światowe standardy w zakresie ochrony prawnej informacji niejawnych. Polska ukształtowała system ochrony opierając się na uregulowaniach obecnych od wielu lat w państwach sojuszniczych o utrwalonym systemie demokratycznym[23]. Przyjęte instytucje mają charakter głównie zapobiegawczy. Dlatego najistotniejszą rolę odgrywają procedury o charakterze prawno-administracyjnym przy pomocniczym znaczeniu przepisów karnych, zawartych w art. 265-266 Kodeksu karnego[24]. Znajdą one zastosowanie dopiero w sytuacji drastycznego naruszenia reguł ochrony. Należy również podkreślić zgodność przyjętych rozwiązań z treścią art. 61 ust. 3 Konstytucji RP z 1997 r. Ograniczenia w dostępie do informacji niejawnych w niewielkim stopniu wpływają na istotę praw obywatelskich. Powodem ograniczeń pozostaje troska o bezpieczeństwa państwa.

---

[22] Ocenę zmian zawarto w artykule S. Smykli, *Najważniejsze zmiany w systemie ochrony informacji niejawnych wprowadzone przez nową ustawę o ochronie informacji niejawnych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 3, s. 105–111.

[23] Uregulowania obowiązujące na terenie wybranych państw opisano w pracy M. Poloka, *Ochrona tajemnicy państwowej i tajemnicy służbowej w polskim systemie prawnym,* Wyd. LexisNexis, Warszawa 2006, s. 147–185 oraz w raporcie M. Mroza, *Standardy ochrony informacji osobistych w postępowaniu sprawdzającym wobec osób mających dostęp do informacji niejawnych: niemiecka ustawa o weryfikacji gwarancji bezpieczeństwa a polska ustawa o ochronie informacji niejawnych,* Raport nr 170. Biuro Studiów i Ekspertyz Sejmu RP – 2000 r.

[24] Kwestiom prawno-karnej ochrony informacji niejawnych poświęcono pracę doktorską wydaną w formie książki M. Leciaka, *Tajemnica państwowa i jej ochrona w prawie karnym materialnym i procesie karnym.* Wyd. TNOIK Dom Organizatora, Toruń 2009.

## Bibliografia


Hoc S., *Ochrona informacji niejawnych i innych tajemnic ustawowo chronionych – wybrane zagadnienia*, Wyd. Uniwersytetu Opolskiego, Opole 2006.

Hoc S., *Ustawa o ochronie informacji niejawnych. Komentarz,* Wyd. LexisNexis 2010.

Leciak M., *Tajemnica państwowa i jej ochrona w prawie karnym materialnym i procesie karnym,* Wyd. TNOIK Dom Organizatora, Toruń 2009.

Mróz M., *Standardy ochrony informacji osobistych w postępowaniu sprawdzającym wobec osób mających dostęp do informacji niejawnych: niemiecka ustawa o weryfikacji gwarancji bezpieczeństwa a polska ustawa o ochronie informacji niejawnych,* Raport nr 170, Biuro Studiów i Ekspertyz Sejmu RP – 2000 r.

Polok M., *Ochrona tajemnicy państwowej i tajemnicy służbowej w polskim systemie prawnym,* Wyd. LexisNexis, Warszawa 2006.

Sawicka H., *Postępowanie odwoławcze od decyzji pełnomocników do spraw ochrony informacji niejawnych – 10 lat doświadczeń szefa ABW jako organu II instancji,* „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 7 (4).

Smykla S., *Najważniejsze zmiany w systemie ochrony informacji niejawnych wprowadzone przez nową ustawę o ochronie informacji niejawnych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 3.

Stankowska I., *Ustawa o ochronie informacji niejawnych, komentarz,* Wyd. LexisNexis, 2010.

Szewc T., *Ochrona informacji niejawnych. Komentarz*, Wydawnictwo C. H. Beck, Warszawa 2007.

Szewc T., *Publicznoprawna ochrona informacji*, Wydawnictwo C. H. Beck, Warszawa 2007.