Polski system ochrony informacji niejawnych

ARTUR J. DUBIEL
- EKSPERT EUROPEAN INSTITUTE FOR STRATEGIC STUDIES
- WYDAWCA PORTALU SZTAB.ORG
- WYKŁADOWCA WSB W POZNANIU, WZ W CHORZOWIE
- DOKTORANT AKADEMII SZTUKI WOJENNEJ W WARSZAWIE

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych

OPRACOWANO NA PODSTAWIE: DZ. U. Z 2010 R. NR 182, POZ. 1228, Z 2015 R. POZ. 21, 1224, 2281, Z 2016 R. POZ. 749

Informacja niejawna

Ustawa określa zasady ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla RP albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania, zwanych dalej „informacjami niejawnymi”, to jest zasady:

Informacja niejawna

1) klasyfikowania informacji niejawnych
2) organizowania ochrony informacji niejawnych
3) przetwarzania informacji niejawnych
4) postępowania sprawdzającego (…) czy osoba nim objęta daje rękojmię zachowania tajemnicy, zwanego dalej odpowiednio „postępowaniem sprawdzającym” lub „kontrolnym postępowaniem sprawdzającym”
5) postępowania (…) zwanego dalej „postępowaniem bezpieczeństwa przemysłowego”
6) organizacji kontroli stanu zabezpieczenia informacji niejawnych
7) ochrony informacji niejawnych w systemach teleinformatycznych
8) stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych.

Przepisy ogólne

2. Przepisy ustawy mają zastosowanie do:

1) organów władzy publicznej, w szczególności:

a) Sejmu i Senatu,

b) Prezydenta Rzeczypospolitej Polskiej,

c) organów administracji rządowej,

d) organów jednostek samorządu terytorialnego, a także innych podległych im jednostek organizacyjnych lub przez nie nadzorowanych,

e) sądów i trybunałów,

f) organów kontroli państwowej i ochrony prawa;

Przepisy ogólne

2. Przepisy ustawy mają zastosowanie do:

2) jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych

3) Narodowego Banku Polskiego

4) państwowych osób prawnych i innych niż wymienione w pkt 1–3 państwowych jednostek organizacyjnych

5) jednostek organizacyjnych podległych organom władzy publicznej lub nadzorowanych przez te organy

6) przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do IN lub wykonujących takie umowy albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do IN.

Wybrane definicje

Jednostka organizacyjna – podmiot wymieniony w art. 1 ust. 2

Rękojmia zachowania tajemnicy – zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony IN przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego

Dokument – każda utrwalona informacja niejawna

Materiał – dokument lub przedmiot albo dowolna ich część, chronione jako IN, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia

Wybrane definicje

Przetwarzanie IN – wszelkie operacje wykonywane w odniesieniu do IN i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie

System teleinformatyczny – jest system teleinformatyczny w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną

Akredytacja bezpieczeństwa teleinformatycznego – dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych

Certyfikacja – jest proces potwierdzania zdolności urządzenia, narzędzia lub innego środka do ochrony informacji niejawnych

Wybrane definicje

Audyt bezpieczeństwa systemu teleinformatycznego – weryfikacja poprawności realizacji wymagań i procedur, określonych w dokumentacji bezpieczeństwa systemu teleinformatycznego

Ryzyko – kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji

Szacowanie ryzyka – całościowy proces analizy i oceny ryzyka

Zarządzanie ryzykiem – skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka

Udostępnienie IN

IN 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 wykonywania czynności zleconych.

Zasady zwalniania od obowiązku zachowania w tajemnicy IN oraz sposób postępowania z aktami spraw zawierającymi IN w postępowaniu przed sądami i innymi organami określają przepisy odrębnych ustaw.

Jeżeli przepisy odrębnych ustaw uprawniają organy, służby lub instytucje albo ich upoważnionych pracowników do dokonywania kontroli, w szczególności do swobodnego dostępu do pomieszczeń i materiałów, a jej zakres dotyczy IN, uprawnienia te są realizowane z zachowaniem przepisów niniejszej ustawy.

Klasyfikowanie IN

Klauzule:

- ŚCIŚLE TAJNE
- TAJNE
- POUFNE
- ZASTRZEŻONE

Ściśle tajne

IN nadaje się klauzulę „ściśle tajne”, jeżeli ich nieuprawnione ujawnienie spowoduje **wyjątkowo poważną szkodę** dla RP przez to, że:

1) zagrozi niepodległości, suwerenności lub integralności terytorialnej RP
2) zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu RP
3) zagrozi sojuszom lub pozycji międzynarodowej RP
4) osłabi gotowość obronną RP
5) doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności O-R, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie
6) zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności O-R, lub osób udzielających im pomocy w tym zakresie
7) zagrozi lub może zagrozić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych, osób, którym udzielono środków ochrony i pomocy przewidzianych w ustawie (…) o ochronie i pomocy dla pokrzywdzonego i świadka albo świadków, o których mowa w Kpk, lub osób dla nich najbliższych

Tajne

IN nadaje się klauzulę „tajne”, jeżeli ich nieuprawnione ujawnienie spowoduje **poważną szkodę** dla RP przez to, że:

1) uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego RP
2) pogorszy stosunki RP z innymi państwami lub organizacjami międzynarodowymi
3) zakłóci przygotowania obronne państwa lub funkcjonowanie SZ RP
4) utrudni wykonywanie czynności O-R prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione
5) w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości
6) przyniesie stratę znacznych rozmiarów w interesach ekonomicznych RP

Poufne

IN nadaje się klauzulę „poufne”, jeżeli ich nieuprawnione ujawnienie spowoduje **szkodę** dla RP przez to, że:

1) utrudni prowadzenie bieżącej polityki zagranicznej RP
2) utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową SZ RP
3) zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli
4) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów RP
5) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości
6) zagrozi stabilności systemu finansowego RP
7) wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej

Zastrzeżone

IN nadaje się klauzulę „zastrzeżone”, jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć **szkodliwy wpływ** na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

Klauzule tajności

IN przekazane przez organizacje międzynarodowe lub inne państwa (…) oznacza się polskim odpowiednikiem posiadanej klauzuli tajności.

Klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału. Osoba ta może określić datę lub wydarzenie, po których nastąpi zniesienie lub zmiana klauzuli tajności.

Zniesienie lub zmiana klauzuli tajności są możliwe wyłącznie po wyrażeniu pisemnej zgody przez w/w osobę, albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony (…).

IN podlegają ochronie w sposób określony w ustawie do czasu zniesienia lub zmiany klauzuli tajności (…).

Kierownicy j.o. przeprowadzają nie rzadziej niż raz na 5 lat przegląd materiałów w celu ustalenia, czy spełniają ustawowe przesłanki ochrony.

Klauzule tajności

Uprawnienia w zakresie zniesienia lub zmiany klauzuli tajności materiału przechodzą, w przypadku rozwiązania, zniesienia, likwidacji, upadłości obejmującej likwidację majątku upadłego, przekształcenia lub reorganizacji jednostki organizacyjnej, na jej następcę prawnego. W razie braku następcy prawnego uprawnienia w tym zakresie przechodzą na ABW lub SKW (…).

Klauzule tajności

Chronione bez względu na upływ czasu (…) są:

1) dane mogące doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb i instytucji, uprawnionych do wykonywania na podstawie ustawy czynności O-R jako funkcjonariuszy, żołnierzy lub pracowników wykonujących te czynności

2) dane mogące doprowadzić do identyfikacji osób, które udzieliły pomocy w zakresie czynności operacyjno-rozpoznawczych służbom i instytucjom uprawnionym do ich wykonywania na podstawie ustawy

3) IN uzyskane od organów innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia.

Ochronie nie podlegają dane (…) zawarte w dokumentach, zbiorach danych, rejestrach i kartotekach, a także w aktach funkcjonariuszy i żołnierzy organów bezpieczeństwa państwa, przekazanych do IPN.

Klauzule tajności

IN którym nadano określoną klauzulę tajności:

1) mogą być udostępnione wyłącznie osobie uprawnionej (…) do dostępu do określonej klauzuli tajności

2) muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności;

3) muszą być chronione, odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie (…)

Organizacja ochrony IN

ABW i SKW nadzorują funkcjonowanie systemu ochrony IN w j.o. pozostających w ich właściwości (…):

1) prowadzą kontrolę ochrony IN i przestrzegania przepisów obowiązujących w tym zakresie;

2) realizują zadania w zakresie bezpieczeństwa systemów teleinformatycznych

3) prowadzą postępowania sprawdzające, kontrolne postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego

4) zapewniają ochronę IN wymienianych między RP a innymi państwami lub organizacjami międzynarodowym

5) prowadzą doradztwo i szkolenia w zakresie ochrony IN.

Organizacja ochrony IN

SKW realizuje zadania w odniesieniu do:

1) MON oraz j.o. podległych Ministrowi ON lub przez niego nadzorowanych

2) ataszatów obrony w placówkach zagranicznych

3) żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe w innych jednostkach organizacyjnych niż wymienione w pkt 1 i 2

ABW realizuje zadania w odniesieniu do j.o. i osób podlegających ustawie, niewymienionych powyżej.

Krajowa Władza Bezpieczeństwa

Szef ABW pełni funkcję krajowej władzy bezpieczeństwa.

Krajowa władza bezpieczeństwa jest właściwa do nadzorowania systemu ochrony IN w stosunkach RP z innymi państwami lub organizacjami międzynarodowymi i wydawania dokumentów upoważniających do dostępu do IN NATO, UE lub innych organizacji międzynarodowych, zwanych dalej „IN międzynarodowymi”.

Szef ABW pełni funkcję krajowej władzy bezpieczeństwa w odniesieniu do podmiotów, o których mowa w art. 10 ust. 2, za pośrednictwem Szefa SKW.

Organizacja ochrony IN

Kierownik j.o., w której są przetwarzane IN, odpowiada za ich ochronę, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony.

Kierownikowi j.o. bezpośrednio podlega (…) pełnomocnik do spraw ochrony informacji niejawnych, zwany dalej „pełnomocnikiem ochrony”, który odpowiada za zapewnienie przestrzegania przepisów o ochronie IN.

Bezpieczeństwo osobowe

Dopuszczenie do pracy / służby / zlecenia na stanowiskach związanych z dostępem do IN może nastąpić po odbyciu szkolenia w zakresie ochrony IN oraz

- pisemnym upoważnieniu przez kierownika j.o. (jeśli nie posiada poświadczenia bezpieczeństwa) – klauzula ZASTRZEŻONE

- uzyskaniu poświadczenia bezpieczeństwa (zwykłe postępowanie sprawdzające) – klauzula POUFNE

- uzyskaniu poświadczenia bezpieczeństwa (poszerzone postępowanie sprawdzające) – klauzule TAJNE i ŚCIŚLE TAJNE

Bezpieczeństwo osobowe

Postępowanie sprawdzające ma na celu ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.

W toku postępowania sprawdzającego ustala się, czy istnieją uzasadnione wątpliwości dotyczące:

1) uczestnictwa, współpracy lub popierania przez osobę sprawdzaną działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej wymierzonej przeciwko RP

2) zagrożenia osoby sprawdzanej ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania z nią kontaktu

3) przestrzegania porządku konstytucyjnego RP, a przede wszystkim, czy osoba sprawdzana uczestniczyła lub uczestniczy w działalności partii politycznych lub innych organizacji, o których mowa w art. 13 Konstytucji RP, albo współpracowała lub współpracuje z takimi partiami lub organizacjami

Bezpieczeństwo osobowe

4) ukrywania lub świadomego niezgodnego z prawdą podawania w ankiecie bezpieczeństwa osobowego, (…) lub postępowaniu sprawdzającym przez osobę sprawdzaną informacji mających znaczenie dla ochrony IN

5) wystąpienia związanych z osobą sprawdzaną okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji

6) niewłaściwego postępowania z IN, jeżeli:

a) doprowadziło to bezpośrednio do ujawnienia tych informacji osobom nieuprawnionym,

b) było to wynikiem celowego działania,

c) stwarzało to realne zagrożenie ich nieuprawnionym ujawnieniem i nie miało charakteru incydentalnego,

d) dopuściła się tego osoba szczególnie zobowiązana na podstawie ustawy do ochrony IN: pełnomocnik ochrony, jego zastępca lub kierownik kancelarii tajnej.

Bezpieczeństwo osobowe

W toku poszerzonego postępowania sprawdzającego ustala się ponadto, czy istnieją wątpliwości dotyczące:

1) poziomu życia osoby sprawdzanej wyraźnie przewyższającego uzyskiwane przez nią dochody

2) informacji o chorobie psychicznej lub innych zakłóceniach czynności psychicznych ograniczających sprawność umysłową i mogących negatywnie wpłynąć na zdolność osoby sprawdzanej (…)

3) uzależnienia od alkoholu, środków odurzających lub substancji psychotropowych.

W razie niedających się usunąć wątpliwości, o których mowa w ust. 2 lub 3, interes ochrony IN ma pierwszeństwo przed innymi prawnie chronionymi interesami.

Zwykłe postępowanie

Zwykłe postępowanie sprawdzające obejmuje:

1) sprawdzenie, w niezbędnym zakresie, w bazach danych informacji zawartych w ankiecie oraz innych ustaleń, celem sprawdzenia czy osoba daje rękojmię zachowania tajemnicy

2) sprawdzenie w bazach danych niedostępnych powszechnie informacji zawartych w ankiecie oraz innych ustaleń, celem sprawdzenia czy osoba daje rękojmię zachowania tajemnicy

W toku sprawdzenia ABW albo SKW ma prawo przeprowadzić rozmowę z osobą sprawdzaną w celu usunięcia nieścisłości lub sprzeczności zawartych w uzyskanych informacjach.

Poszerzone postępowanie

Poszerzone postępowanie sprawdzające obejmuje czynności dot. zwykłego postępowania, a ponadto jeżeli to konieczne (…):

1) rozmowę z przełożonymi osoby sprawdzanej oraz z innymi osobami

2) przeprowadzenie wywiadu w miejscu zamieszkania osoby sprawdzanej

3) sprawdzenie stanu i obrotów na rachunku bankowym oraz zadłużenia osoby sprawdzanej, w szczególności wobec SP

Poszerzone postępowanie

W przypadku osób ubiegających się o uzyskanie dostępu do informacji o klauzuli „ściśle tajne” pps obejmuje także, jeżeli jest to konieczne (…), rozmowę z trzema osobami wskazanymi przez osobę sprawdzaną w celu uzyskania innych informacji mogących mieć znaczenie dla oceny dawania rękojmi zachowania tajemnicy

W celu dokonania ustaleń (…) organ prowadzący pps może zobowiązać osobę sprawdzaną do poddania się specjalistycznym badaniom oraz udostępnienia wyników tych badań.

Postępowanie sprawdzające

Postępowanie sprawdzające kończy się:

1) wydaniem poświadczenia bezpieczeństwa
2) odmową wydania poświadczenia bezpieczeństwa
3) umorzeniem

Po zakończeniu postępowania sprawdzającego z wynikiem pozytywnym organ prowadzący postępowanie wydaje **poświadczenie bezpieczeństwa** i przekazuje osobie sprawdzanej, zawiadamiając o tym wnioskodawcę.

Poświadczenie bezpieczeństwa

Poświadczenie bezpieczeństwa wydaje się na okres:

10 lat – dostęp do IN o klauzuli POUFNE

7 lat – dostęp do IN o klauzuli TAJNE

5 lat – dostęp do IN o klauzuli ŚCIŚLE TAJNE

Poświadczenie bezpieczeństwa upoważniające do dostępu do IN o wyższej klauzuli tajności uprawnia do dostępu do IN o niższej klauzuli tajności, odpowiednio przez okresy, o których mowa (…), także w odniesieniu do poświadczeń bezpieczeństwa organizacji międzynarodowych.

Poświadczenie bezpieczeństwa

Poświadczenia bezpieczeństwa wydane w wyniku przeprowadzenia postępowań sprawdzających (…), zachowują ważność wyłącznie w okresie pracy lub służby w organie, który przeprowadził postępowanie sprawdzające.

Poświadczenie bezpieczeństwa

Postępowanie sprawdzające wobec osoby, której odmówiono wydania poświadczenia bezpieczeństwa, można przeprowadzić najwcześniej po roku od daty doręczenia decyzji o odmowie wydania poświadczenia bezpieczeństwa.

Umorzenie postępowania sprawdzającego następuje w przypadku:

1) śmierci osoby sprawdzanej

2) rezygnacji osoby sprawdzanej z ubiegania się o stanowisko albo zajmowania stanowiska lub wykonywania prac, związanych z dostępem do IN

3) odstąpienia przez kierownika j.o. od zamiaru obsadzenia osoby sprawdzanej na stanowisku lub zlecenia jej prac, związanych z dostępem do IN

4) gdy postępowanie z innej przyczyny stało się bezprzedmiotowe

Poświadczenie bezpieczeństwa

Na pisemny wniosek kierownika j.o., złożony co najmniej na 6 miesięcy przed upływem terminu ważności poświadczenia bezpieczeństwa, właściwy organ przeprowadza kolejne postępowanie sprawdzające, które powinno się zakończyć przed upływem terminu ważności dotychczasowego poświadczenia bezpieczeństwa.

Poświadczenie bezpieczeństwa

W przypadku gdy o osobie, której wydano poświadczenie bezpieczeństwa, zostaną ujawnione nowe informacje wskazujące, że nie daje ona rękojmi zachowania tajemnicy, przeprowadza się kontrolne postępowanie sprawdzające. O wszczęciu takiego postępowania zawiadamia się: kierownika j.o. (…), pełnomocnika ochrony oraz osobę sprawdzaną.

Kontrolne postępowanie sprawdzające kończy się:

1) decyzją o cofnięciu poświadczenia bezpieczeństwa;

2) poinformowaniem (…) o braku zastrzeżeń

3) decyzją o umorzeniu postępowania, w przypadku gdy postępowanie to nie zostanie zakończone przed upływem 12 miesięcy od dnia jego wszczęcia.

Poświadczenie bezpieczeństwa

Szefowie Kancelarii Prezydenta RP, Kancelarii Sejmu, Kancelarii Senatu lub Kancelarii Prezesa RM albo minister właściwy dla określonego działu administracji rządowej, Prezes NBP, Prezes NIK lub kierownik urzędu centralnego, a w przypadku ich braku ABW albo SKW, mogą:

1) w szczególnie uzasadnionych przypadkach (…) wyrazić pisemną zgodę na jednorazowe udostępnienie określonych IN osobie nieposiadającej odpowiedniego poświadczenia bezpieczeństwa;

2) wyrazić pisemną zgodę na udostępnienie IN o klauzuli „tajne” lub „ściśle tajne” osobie, wobec której wszczęto poszerzone postępowanie sprawdzające.

W stanach nadzwyczajnych Prezydent RP lub Prezes RM (…) może wyrazić zgodę na odstąpienie od przeprowadzenia postępowania sprawdzającego.

Postępowania sprawdzające

Postępowania sprawdzającego nie przeprowadza się (…) wobec:

1) Prezydenta RP oraz osoby wybranej na ten urząd
2) Marszałków Sejmu i Senatu
3) Prezesa i członka Rady Ministrów
4) Prezesów NBP, NIK, IPN
5) Rzecznika Praw Obywatelskich
6) Generalnego Inspektora Ochrony Danych Osobowych
7) członków Rady Polityki Pieniężnej i KRRiT
8) Szefów Kancelarii: Prezydenta RP, Sejmu, Senatu i Prezesa RM
9) posła i senatora
10) sędziów, prokuratorów, asesorów i ławników

Środki bezpieczeństwa fizycznego

Kierownik jednostki organizacyjnej, w której są przetwarzane IN o klauzuli „tajne” lub „ściśle tajne”, tworzy kancelarię, zwaną dalej „kancelarią tajną”, i zatrudnia jej kierownika.

Środki bezpieczeństwa fizycznego

Jednostki organizacyjne, w których są przetwarzane IN, stosują środki bezpieczeństwa fizycznego odpowiednie do poziomu zagrożeń w celu uniemożliwienia osobom nieuprawnionym dostępu do takich informacji, w szczególności chroniące przed:

1) działaniem obcych służb specjalnych

2) zamachem terrorystycznym lub sabotażem

3) kradzieżą lub zniszczeniem materiału

4) próbą wejścia osób nieuprawnionych do pomieszczeń, w których są przetwarzane IN

5) nieuprawnionym dostępem do informacji o wyższej klauzuli tajności niewynikającym z posiadanych uprawnień.

Środki bezpieczeństwa fizycznego

W celu uniemożliwienia osobom nieuprawnionym dostępu do IN o klauzuli „poufne” lub wyższej należy w szczególności:

1) zorganizować strefy ochronne

2) wprowadzić system kontroli wejść i wyjść ze stref ochronnych

3) określić uprawnienia do przebywania w strefach ochronnych

4) stosować wyposażenie i urządzenia służące ochronie IN, którym przyznano certyfikaty.

Bezpieczeństwo teleinformatyczne

Systemy teleinformatyczne, w których mają być przetwarzane IN, podlegają akredytacji bezpieczeństwa teleinformatycznego.

Akredytacji udziela się na czas określony, nie dłuższy niż 5 lat.

ABW albo SKW udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania IN o klauzuli „poufne” lub wyższej.

Bezpieczeństwo przemysłowe

Warunkiem dostępu przedsiębiorcy do IN w związku z wykonywaniem umów albo zadań wynikających z przepisów prawa, jest zdolność do ochrony IN.

Dokumentem potwierdzającym zdolność do ochrony IN o klauzuli „poufne” lub wyższej jest świadectwo bezpieczeństwa przemysłowego, wydawane przez ABW albo SKW po przeprowadzeniu postępowania bezpieczeństwa przemysłowego.

W przypadku przedsiębiorcy wykonującego działalność jednoosobowo i osobiście zdolność do ochrony IN potwierdza poświadczenie bezpieczeństwa upoważniające do dostępu do IN o klauzuli tajności „poufne” lub wyższej, wydawane przez ABW albo SKW (i zaświadczenie o odbytym przeszkoleniu).

Bezpieczeństwo przemysłowe

W zależności od stopnia zdolności do ochrony IN o klauzuli „poufne” lub wyższej wydaje się świadectwo:

1) pierwszego stopnia – potwierdzające pełną zdolność przedsiębiorcy do ochrony tych informacji

2) drugiego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, z wyłączeniem możliwości ich przetwarzania we własnych systemach teleinformatycznych

3) trzeciego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, z wyłączeniem możliwości ich przetwarzania w użytkowanych przez niego obiektach.

Odpowiedzialność

Odpowiedzialność karna, dyscyplinarna i służbowa za ujawnienie informacji niejawnych:

- Ustawa o z dnia 6 czerwca 1997 r. Kodeks postępowania karnego
- Ustawa z dnia 6 czerwca 1997 r. Kodeks karny

Ujawnienie informacji

Art. 265 § 1. Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje niejawne o klauzuli „tajne” lub „ściśle tajne”, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Jeżeli informację określoną w § 1 ujawniono osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 3. Kto nieumyślnie ujawnia informacje określoną w § 1, z którą zapoznał się w związku z pełnieniem funkcji publicznej lub otrzymanej upoważnieniem, podlega grzywnie, karze ograniczenia wolności lub pozbawienia wolności do roku.

Ujawnienie informacji

Art. 266 § 1. Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informacje, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli „zastrzeżone” lub „poufne” lub informacje, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes podlega karze pozbawienia wolności do lat 3.

§ 3. Ściganie przestępstwa określonego w § 1 następuje na wniosek pokrzywdzonego.

Odpowiedzialność karna

Wyłączenie odpowiedzialności karnej za ujawnienie tajemnicy państwowej lub służbowej

Nie podlegają odpowiedzialności karnej:

– osoby, które z mocy prawa są upoważnione do udostępniania informacji stanowiących tajemnicę państwową lub służbową określonym w art. 49 ust. 1, 2 i 3 kpk,

– osoby zwolnione z obowiązku zachowania tajemnicy państwowej i służbowej

(art. 179, 180 § 1)

Przestępstwo komputerowe

Art. 269 § 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając nośnik informacji lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

Przestępstwo komputerowe

Art. 269a Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Art. 269b § 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe do popełnienia przestępstwa a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej podlega karze pozbawienia wolności do lat 3.

§ 2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy