ORGANIZACJA SYSTEMU OCHRONY INFORMACJI NIEJAWNYCH RP

Definicje (1/3)

Przetwarzaniem informacji niejawnych – są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazanie (w tym również ustnie) lub udostępnienie (art. 2 pkt 5).

Definicje (2/3)

Rękojmią zachowania tajemnicy – jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego (art. 2 pkt 2).

Zatrudnieniem – jest również odpowiednio powołanie, mianowanie lub wyznaczenie (art. 2 pkt 18).

Definicje (3/3)

Dokumentem – jest każda utrwalona informacja niejawna (art. 2 pkt 3).

Materiałem – jest dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia (art. 2 pkt 4).

Klasyfikowanie informacji niejawnych (1/14)

Kryterium podziału klauzul tajności związane jest z pojęciem **szkody**, jaką ujawnienie informacji niejawnych mogłoby przynieść dla bezpieczeństwa i interesów RP.

W przypadku informacji niejawnych o klauzulach „ściśle tajne", „tajne" i „poufne" **muszą być spełnione łącznie dwie przesłanki:**

1) nieuprawnione ujawnienie tych informacji **musi zagrażać** wymienionym enumeratywnie (zróżnicowanym adekwatnie do klauzuli) dobrom;

2) nieuprawnione ujawnienie tych informacji spowoduje dla RP – w przypadku informacji „ściśle tajnych" – **szkodę wyjątkowo poważną**, „tajnych" – **szkodę poważną**, „poufnych" – **szkodę.**

Klasyfikowanie informacji niejawnych (2/14)

Informacjom niejawnym nadaje się klauzulę **„ściśle tajne” („00”)**, 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 sojuszowi lub pozycji międzynarodowej RP;

Klasyfikowanie informacji niejawnych (3/14)

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 wykonają czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;

Klasyfikowanie informacji niejawnych (4/14)

6) zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, 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 z dnia 28 listopada 2014 r. o ochronie i pomocy dla pokrzywdzonego i świadka, albo świadków, o których mowa w art. 184 ustawy z dnia 6 czerwca 1997 r. – kodeks postępowania karnego lub osób dla nich najbliższych.

(art. 5 ust. 1).

Klasyfikowanie informacji niejawnych (5/14)

Informacjom niejawnym nadaje się klauzulę **„tajne” („0”)**, 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 Sił Zbrojnych RP;

Klasyfikowanie informacji niejawnych (6/14)

4) utrudni wykonywanie czynności operacyjno-rozpoznawczych 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.

(art. 5 ust. 2)

Klasyfikowanie informacji niejawnych (7/14)

Informacjom niejawnym nadaje się klauzulę **„poufne” („Pf”)**, 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 Sił Zbrojnych RP;
3) zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;

Klasyfikowanie informacji niejawnych (8/14)

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 skarbowych oraz organom wymiaru sprawiedliwości;

6) zagrozi stabilności systemu finansowego RP;

7) wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

(art. 5 ust. 3)

Klasyfikowanie informacji niejawnych (9/14)

Informacjom niejawnym nadaje się klauzulę **„zastrzeżone” („Z”)**, 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 RP (art. 5 ust.4).

Klasyfikowanie informacji niejawnych (10/14)

- Klauzulę tajności nadaje osoba, która jest **uprawniona do podpisania dokumentu lub oznaczenia** innego niż dokument materiału (art. 6 ust. 1).
- Informacje niejawne podlegają ochronie w sposób określony w ustawie **do czasu zniesienia lub zmiany klauzuli tajności** (art. 6 ust. 2).
- Osoba, która nadaje klauzulę tajności, może określić **datę lub wydarzenie**, po których nastąpi zniesienie lub zmiana klauzuli tajności (art. 6 ust. 2).

Klasyfikowanie informacji niejawnych (11/14)

- Zniesienie lub zmiana klauzuli tajności są możliwe wyłącznie po wyrażeniu **pisemnej zgody** przez osobę, która nadała klauzulę, albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony (art. 6 ust. 3).

- **Pisemną zgodę** na zniesienie lub zmianę klauzuli tajności w przypadku informacji niejawnych o klauzuli **„ściśle tajne” wyraża kierownik jednostki organizacyjnej**, w której materiałowi została nadana klauzula tajności (art. 6 ust. 5).

Klasyfikowanie informacji niejawnych (12/14)

- Kierownicy jednostek organizacyjnych przeprowadzają **nie rzadziej niż raz na 5 lat przegląd materiałów** w celu ustalenia, czy spełniają ustawowe przesłanki ochrony (art. 6 ust. 4).
- 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 (art. 6 ust. 7).

Klasyfikowanie informacji niejawnych (13/14)

- Odbiorca materiału, w przypadku stwierdzenia zawyżenia lub zaniżenia klauzuli tajności, może zwrócić się do osoby, która ją nadała, albo przełożonego tej osoby z **wnioskiem** o dokonanie stosownej zmiany (art. 9 ust. 1).
- W przypadku odmowy dokonania zmiany lub nieudzielania odpowiedzi w ciągu 30 dni od daty złożenia wniosku, odbiorca materiału może zwrócić się odpowiednio do ABW lub SKW o **rozstrzygnięcie sporu** (art. 9 ust. 2).

Klasyfikowanie informacji niejawnych (14/14)

- Spór **ABW lub SKW rozstrzyga** w terminie **30 dni** od daty złożenia wniosku o jego rozstrzygnięcie (art. 9 ust. 3).

- Jeżeli stroną sporu jest ABW albo SKW, to spór rozstrzyga Prezes Rady Ministrów w terminie 30 dni od daty złożenia wniosku o jego rozstrzygnięcie (art. 9 ust. 4).

Ochrona informacji niejawnych

Chronione bez względu na upływ czasu pozostają (art. 7 ust. 1):

- dane mogące doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb i instytucji, uprawnionych do wykonywania na podstawie ustawy **czynności operacyjno-rozpoznawczych** jako funkcjonariuszy, żołnierzy lub pracowników wykonujących te czynności;
- dane mogące doprowadzić do identyfikacji osób, które **udzieliły pomocy w zakresie czynności operacyjno-rozpoznawczych** służbom i instytucjom uprawnionym do ich wykonywania na podstawie ustawy;
- informacje niejawne uzyskane od organów innych państw lub organizacji międzynarodowych, **jeżeli taki był warunek ich udostępnienia.**

UWAGA: Powyższe nie dotyczy w/w danych, które zostały przekazane do IPN.

Okresy ochronne a okresy przechowywania informacji niejawnych

- Okresy ochronne informacji niejawnych determinują **przesłanki określone w art. 5 ustawy.**
- Okresy przechowywania związane są z **przepisami archiwalnymi**, tj. ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz rozporządzeniem Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej **(wyjątek – tzw. archiwa wyodrębnione i przedsiębiorcy).**

Okres ochronny

Do czasu zniesienia klauzuli tajności informacje są chronione i udostępniane zgodnie z zasadami przewidzianymi dla nadanej klauzuli tajności.

UWAGA:

W przypadku zniesienia klauzuli tajności należy dokonać czynności materialno-technicznych, polegających na skreśleniu dotychczasowej klauzuli oraz dokonaniu stosownych adnotacji.

Powyższe kwestie będą szczegółowo omawianie w bloku dotyczącym „Zasad ewidencji i obiegu materiałów niejawnych”.

Archiwizowanie i brakowanie materiałów niejawnych – jednostki państwowe (1/2)

- Na podstawie tzw. „przepisów archiwalnych” w jednostce organizacyjnej niebędącej przedsiębiorcą należy opracować **jednolity rzeczowy wykaz akt**, który określa klasyfikację dokumentacji powstającej w toku działalności jednostki oraz zawiera kwalifikację archiwalną.
- W przypadku informacji niejawnych mających wartość archiwalną należy je przechowywać zgodnie z okresem przechowywania wynikającym z jednolitego rzeczowego wykazu akt i w warunkach przewidzianych dla nadanej klauzuli tajności (w przypadku zniesienia klauzuli tajności dokument przechowywany z wyłączeniem stosowania przepisów o.i.n.).

Archiwizowanie i brakowanie materiałów niejawnych – jednostki państwowe (2/2)

- Brakowanie (niszczenie) dokumentacji niearchiwalnej, w tym oznaczonej kategorią „Bc”, następuje na podstawie zgody właściwego państwowego archiwum (wyjątek - archiwa wyodrębnione).
- Fakt dokonania brakowania dokumentują **protokoły brakowania** (zniszczenia), które wymagają zatwierdzenia przez kierownika jednostki.

Brakowanie materiałów niejawnych – przedsiębiorcy

- Brakowanie dokumentacji niejawnej przetwarzanej u przedsiębiorców następuje przy uwzględnieniu zapisów zawartych w instrukcji bezpieczeństwa przemysłowego (nie jest wymagana zgoda archiwum państwowego).
- Fakt dokonania brakowania dokumentują **protokoły brakowania** (zniszczenia), które wymagają zatwierdzenia przez kierownika przedsiębiorcy.

Rozwiązania instytucjonalne (1/10)

- Kierownik jednostki organizacyjnej **odpowiada za ochronę informacji niejawnych**, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony.
- Kierownikiem jednostki organizacyjnej jest osoba, która zgodnie z obowiązującymi daną jednostkę przepisami prawa, umocowana jest do **kierowania (zarządzania) jednostką.**

Rozwiązania instytucjonalne (2/10)

- Niedopuszczalnym i sprzecznym z art. 14 ust. 1 ustawy jest wyznaczenie do pełnienia funkcji kierownika jednostki organizacyjnej w rozumieniu przepisów ustawy, innej osoby niż faktycznie kierująca daną jednostką, np. zastępcy, bądź innego podległego pracownika.
- Dopuszczalnym jest natomiast **imienne upoważnienie** przez kierownika jednostki organizacyjnej podległych mu pracowników **do wykonywania jego ustawowych zadań (szczegółowo wymienionych)** w obszarze ochrony informacji niejawnych.

Wyjątek – bezpieczeństwo przemysłowe

Rozwiązania instytucjonalne (3/10)

Z uwagi na odpowiedzialność kierownika jednostki organizacyjnej za ochronę informacji niejawnych, wymagane jest aby posiadał odpowiednie uprawnienia dostępowe, tj.:

- ✓ **poświadczenie bezpieczeństwa** upoważniające do dostępu do najwyższej klauzuli przetwarzanych w jednostce informacji niejawnych;
- ✓ **aktualne zaświadczenie o przeszkoleniu** w zakresie ochrony informacji niejawnych.

Wyjątki w zakresie obowiązku posiadania poświadczenia bezpieczeństwa:

- ✓ **art. 34 ust. 10 ustawy;**
- ✓ w przypadku przetwarzania informacji niejawnych o najwyższej klauzuli **„zastrzeżone”** – dostęp kierownika jednostki następuje **z mocy prawa.**

Rozwiązania instytucjonalne (4/10)

Kierownik jednostki organizacyjnej w obszarze ochrony informacji niejawnych w szczególności:

- zatrudnia pełnomocnika ochrony oraz jego zastępcę lub zastępców i organizuje pion ochrony;
- określa szczegółowy zakres czynności zastępcy pełnomocnika ochrony;
- tworzy kancelarię tajną, jeżeli w podległej mu jednostce przetwarzane są informacje oznaczone klauzulą **„tajne”** lub **„ściśle tajne”** i zatrudnia jej kierownika;
- może wyrazić zgodę na przetwarzanie w kancelarii tajnej informacji niejawnych o klauzuli „poufne” lub „zastrzeżone”;

Rozwiązania instytucjonalne (5/10)

- wyraża pisemną zgodę na **zniesienie lub zmianę klauzuli tajności** w przypadku informacji niejawnych o klauzuli „ściśle tajne” wytworzonych w jednostce organizacyjnej;
- przeprowadza **nie rzadziej niż raz na 5 lat** przegląd materiałów w celu ustalenia, czy spełniają ustawowe przesłanki ochrony (powyższy przegląd odnosi się wyłącznie do dokumentów niejawnych **wytworzonych w danej jednostce**; istotny jest fakt udokumentowania przedmiotowego przeglądu);

Rozwiązania instytucjonalne (6/10)

- współdziała ze służbami i instytucjami uprawnionymi do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego, w szczególności udostępniając funkcjonariuszom, pracownikom albo żołnierzom tych służb i instytucji, po przedstawieniu przez nich pisemnego upoważnienia, pozostające w ich dyspozycji informacje i dokumenty niezbędne do realizacji czynności w ramach tych postępowań;
- wnioskuje odpowiednio do ABW lub SKW o przeprowadzenie poszerzonego postępowania sprawdzającego (art. 23 ust. 2);
- wydaje pisemne polecenie przeprowadzenia zwykłego postępowania sprawdzającego (art. 23 ust. 1);
- wnioskuje **co najmniej 6 miesięcy** przed upływem terminu ważności poświadczenia bezpieczeństwa do właściwego organu o przeprowadzenie kolejnego postępowania sprawdzającego (art. 32 ust. 1);

Rozwiązania instytucjonalne (7/10)

- informuje w **terminie 7 dni** organ, który wydał poświadczenie bezpieczeństwa, oraz odpowiednio ABW lub SKW o zatrudnieniu osoby przedstawiającej takie poświadczenie (art. 34 ust. 2);
- wydaje pisemne upoważnienie do dostępu do informacji niejawnych do klauzuli **„zastrzeżone”** osobie, która nie posiada poświadczenia bezpieczeństwa (art. 21 ust. 4);
- informuje odpowiednio ABW lub SKW o utworzeniu lub likwidacji kancelarii tajnej, z określeniem klauzuli tajności przetwarzanych w niej informacji niejawnych;
- zatwierdza opracowaną przez pełnomocnika ochrony dokumentację odnoszącą się do obszaru ochrony informacji niejawnych (o której szczegółowo w bloku dotyczącym „Zadań pełnomocnika ochrony”);

Rozwiązania instytucjonalne (8/10)

Kierownik jednostki organizacyjnej w przypadku przetwarzania informacji niejawnych w systemach teleinformatycznych:

- udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli **„zastrzeżone”** przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego (art. 48 ust. 9);
- w ciągu **30 dni** od udzielenia akredytacji, o której mowa powyżej, przekazuje odpowiednio ABW lub SKW dokumentację bezpieczeństwa systemu teleinformatycznego;
- akceptuje wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych oraz jest odpowiedzialny za właściwą organizację bezpieczeństwa teleinformatycznego (art. 49 ust. 7);

Rozwiązania instytucjonalne (9/10)

- wyznacza pracownika lub pracowników pionu ochrony pełniących funkcję **inspektora bezpieczeństwa teleinformatycznego**, odpowiedzialnych za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji (art. 52 ust. 1 pkt 1);
- wyznacza osobę lub zespół osób, niepełniących funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego, zwanych **administratorem systemu** (art. 52 ust. 1 pkt 2).

Rozwiązania instytucjonalne (10/10)

Ponadto **kierownik jednostki organizacyjnej** organizującej system odpowiada za opracowanie oraz przekazanie odpowiednio ABW lub SKW dokumentacji bezpieczeństwa systemu teleinformatycznego w przypadku gdy system ten będzie funkcjonował **w więcej niż jednej jednostce organizacyjnej** (art. 49 ust. 6).

Podsumowanie

- Odpowiedzialność kierownika jednostki organizacyjnej.
- Uprawnienia dostępowe kierownika jednostki organizacyjnej.
- Możliwość wykonywania zadań kierownika jednostki wyłącznie na podstawie pisemnego upoważnienia i w jego imieniu.