

Szkolenie wojskowe  
Legia Akademicka, Uniwersytet Szczeciński  
edycja 4, 2021.

## OCHRONA INFORMACJI NIEJAWNYCH

dr Mariusz Sikora, mail: [mariusz.sikora@usz.edu.pl](mailto:mariusz.sikora@usz.edu.pl)

zespół LA US

[legiaakademicka@usz.edu.pl](mailto:legiaakademicka@usz.edu.pl)

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Akty prawne regulujące ochronę informacji niejawnych w Polsce

1. Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. 2019, poz. 742)
- Rozporządzenie RM z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. 2017 poz. 1558)

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Akty prawne regulujące ochronę informacji niejawnych w RP

- Rozporządzenie Prezesa RM z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. 2011. 288.1692)
- Rozporządzenie Prezesa RM z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne. (Dz. U. 2011. Nr 271, poz. 1603)
- Rozporządzenie Prezesa RM z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego. (Dz. U. 2011. Nr 159, poz. 948)

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Akty prawne regulujące ochronę informacji niejawnych w RP

- Rozporządzenie RM z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. 2012 poz. 683, z 2017 poz. 522)
- Rozporządzenie Prezesa RM z dnia 20 lipca 2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego . (Dz. U. 2011. 156. 926)
- Rozporządzenie Prezesa RM z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych. (Dz. U. 2011.93. 541)

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Akty wykonawcze dotyczące ochrony informacji niejawnych

- Rozporządzenie Prezesa RM z dnia 6 lutego 2015 r. w sprawie wzorów poświadczeń bezpieczeństwa (Dz. U. 2015 poz. 220)
- Rozporządzenie Prezesa RM z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (Dz. U. 2010.258.1753)
- Rozporządzenie Prezesa RM z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz. U. 2010. 258.1754)
- Rozporządzenie Prezesa RM z dnia 11 lutego 2015 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (Dz. U. 2015 poz. 205)

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Akty wykonawcze dotyczące ochrony informacji niejawnych

- Rozporządzenie Prezesa RM z dnia 28 grudnia 2010 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego. (Dz. U.2010.258.1750)

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Podstawowe pojęcia Ochrona Informacji Niejawnych

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Podstawowe pojęcia

- **Informacje niejawne** – to informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować **szkody** dla RP albo byłyby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Definicja UE – Informacja niejawna

- **Informacje niejawne UE** to wszelkie informacje lub materiały objęte klauzulą tajności UE, których nieuprawnione ujawnienie mogłoby w różnym stopniu wyrządzić **szkodę interesom UE** lub interesom co najmniej jednego państwa członkowskiego.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Podstawowe pojęcia

- **Rękojmia zachowania tajemnicy** – jest to zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Podstawowe pojęcia

- **Dokument** – jest to każda utrwalona informacja niejawna
- **Materiał** – dokument lub przedmiot albo dowolna jego część, chroniona jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowana albo będąca w trakcie produkcji, a także składniki użyte do ich wytworzenia

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Podstawowe pojęcia

- **Przetwarzanie informacji niejawnych** – są to wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Podstawowe pojęcia

- Akredytacją bezpieczeństwa teleinformatycznego jest dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Podstawowe pojęcia

- Dokumentacja bezpieczeństwa systemu teleinformatycznego – stanowi dokumenty:
  1. Szczególne Wymagania Bezpieczeństwa
  2. Procedury Bezpiecznej Eksploatacji systemu teleinformatycznego,które są opracowywane zgodnie z zasadami określonymi w ustawie.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Podstawowe pojęcia

- **Ryzykiem** – jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencje
- **Szacowaniem ryzyka** - jest całościowy proces analizy i oceny ryzyka
- **Zarządzanie ryzykiem** - skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Zasady ochrony informacji niejawnych

- Klasyfikowanie informacji niejawnych
- Organizacja ochrony informacji niejawnych – nadzór i kontrola:
  - Bezpieczeństwo osobowe
  - Bezpieczeństwo fizyczne
  - Bezpieczeństwo teleinformatyczne
- Kontrola stanu zabezpieczenia

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## KLASYFIKOWANIE INFORMACJI NIEJAWNYCH

To przyznanie informacji niejawnej jednej z przewidzianych w ustawie **klauzul tajności**

Przyznana klauzula tajności musi być w sposób wyraźny (widoczny) na materiał naniesiona.

Ta sama zasada obowiązuje w przypadku przekazu ustnego, prezentacji, projekcji itp.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Klasyfikowanie informacji

Informacjom niejawnym przyznajemy następujące klauzule tajności:

- Ścisłe Tajne
- Tajne
- Poufne
- Zastrzeżone

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### ŚCIŚLE TAJNE (1)

to takie informacje, których

- Nieuprawnione ujawnienie spowoduje **wyjątkowo poważną szkodę** dla RP
- zagrazi niepodległości, suwerenności lub integralności terytorialnej RP;
- zagrazi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu RP;
- zagrazi sojuszom i pozycji międzynarodowej RP;
- osłabi gotowość obronną RP;
- doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu;

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### ŚCIŚLE TAJNE (2)

- zagrazi lub może zagrazić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze lub osób udzielających im pomocy w tym zakresie;
- zagrazi lub może zagrazić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych;

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### TAJNE (1)

to takie informacje, których

- nieuprawnione ujawnienie spowoduje **poważne szkody** dla RP
- uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego RP;
- pogorszy stosunki RP z innymi państwami lub organizacjami międzynarodowymi;
- zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych RP;

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## TAJNE (2)

- utrudni wykonywanie czynności operacyjno – rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione;
- zakłóci w istotny sposób funkcjonowanie organów ścigania i wymiaru sprawiedliwości;
- przyniesie stratę znacznych rozmiarów w interesach ekonomicznych RP;

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## POUFNE (1)

to takie informacje, których

- nieuprawnione ujawnienie spowoduje **szkodę** dla RP
- utrudni prowadzenie bieżącej polityki zagranicznej RP;
- utrudni realizację przedsięwzięć obronnych;
- zakłóci porządek publiczny lub zagrazi bezpieczeństwu obywateli;
- utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów RP;

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## POUFNE (2)

- utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
- zagrazi stabilności systemu finansowego RP;
- wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej;

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---



## ZASTRZEŻONE

to takie informacje, którym

- nie nadano 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 i bezpieczeństwa publicznego
  - polityki zagranicznej
  - przestrzegania praw i wolności obywateli
  - wymiaru sprawiedliwości
  - interesów ekonomicznych RP

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Cezury ochronne ochrony informacji niejawnych

- Informacje niejawne podlegają ochronie do czasu zniesienia lub zmiany klauzuli tajności.
- Osoba, która nadała klauzulę tajności 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 osobę, która klauzulę nadała.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Cezury ochronne informacji niejawnych

- Również zgodę na zniesienie lub zmianę klauzuli tajności może pisemnie wyrazić przełożony osoby, która była uprawniona do podpisania dokumentu, w przypadku ustania lub zmiany ustawowych przesłanek ochrony.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Cezury ochronne informacji niejawnych

- Ze względu na to, że osoba podpisująca dokument sama wedle swojej wiedzy określa cezury ochronne, ustawodawca nakazuje kierownikom jednostek organizacyjnych przeprowadzić nie rzadziej niż raz na 5 lat przegląd materiałów w celu ustalenia czy nadal spełniają ustawowe przesłanki ochrony.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## ORGANIZACJA OCHRONY INFORMACJI NIEJAWNYCH – NADZÓR I KONTROLA

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Organizacja Ochrony Informacji Niejawnych

- **ABW i SKW** – nadzorują funkcjonowanie systemu ochrony informacji niejawnych w jednostkach organizacyjnych pozostających w ich właściwości

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## KRAJOWA WŁADZA BEZPIECZEŃSTWA

- Szef ABW pełni funkcję krajowej władzy bezpieczeństwa w sferze cywilnej i za pośrednictwem szefa SKW w sferze wojskowej
- Krajowa władza bezpieczeństwa jest właściwa do nadzorowania systemu ochrony informacji niejawnych w stosunkach RP z innymi państwami lub organizacjami międzynarodowymi (NATO, UE)

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## UPRAWNIENIA ABW W ZAKRESIE STANU ZABEZPIECZENIA I KONTROLI INFORMACJI NIEJAWNYCH

- Prawo wstępu do obiektów i pomieszczeń jednostki kontrolowanej
- Wglądu do dokumentów związanych z organizacją ochrony inf. niej.
- Żądania udostępnienia do kontroli systemów teleinformatycznych
- Przeprowadzania oględzin obiektów, składników majątkowych i czynności związanych z oin
- Uczestniczenia w posiedzeniach kierownictwa, organów zarządzających, nadzorczych, opiniotwórczo-doradczych w sprawach dotyczących problematyki oin

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

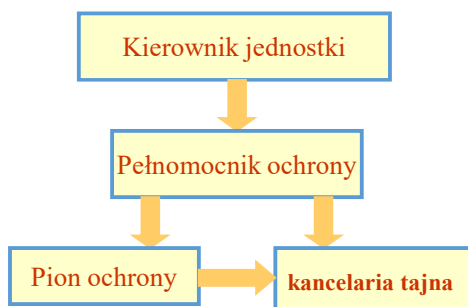
---

---

---

---

## Podmioty właściwe w zakresie ochrony informacji niejawnych



---

---

---

---

---

---

---

---

### Kierownik jednostki -zadania

- Prezydent/Burmistrz/Wójt/Dowódca – odpowiada za ochronę informacji niejawnych w Urzędzie, szczególnie za zorganizowanie i zapewnienie funkcjonowania tej ochrony.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Kierownik jednostki – zadania

- Powołuje **pełnomocnika ochrony**
- Organizuje **kancelarię tajną** lub inną komórkę
- Wydaje **upoważnienia** do przetwarzania inf. niej. o klauzuli *zastrzeżone*
- Wydaje polecenia przeprowadzenia **zwykłego postępowania sprawdzającego** i wnioskuje o wszczęcie poszerzonego postępowania sprawdzającego
- Zapewnia **przeszkolenie pracowników** w zakresie ochrony inf. niej.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Kierownik jednostki – zadania

- Zatwierdza **instrukcję** dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w komórkach organizacyjnych
- Zatwierdza sposób i tryb przetwarzania informacji niejawnych o klauzuli „poufne”
- Opracowanie **szczególnych wymagań bezpieczeństwa (SWB)** systemów i sieci teleinformatycznych
- **Wyznacza** administratora systemu i inspektora bezpieczeństwa systemów i sieci teleinformatycznych

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Pełnomocnik ochrony – zadania

- Pełnomocnik do spraw ochrony informacji niejawnych – odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych w jednostce organizacyjnej

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Pełnomocnik ochrony – zadania

- Przeprowadza zwykłe oraz kontrolne postępowania sprawdzające (tj. do poziomu „poufne”).
- Informuje ABW o wydanych poświadczeniach bezpieczeństwa do poziomu „poufne” i wszystkich wydanych odmowach lub decyzjach o cofnięciu poświadczenia.
- Organizuje szkolenia z zakresu ochrony informacji niejawnych w stosunku do osób zatrudnionych w jednostce organizacyjnej.
- Prowadzi aktualny wykaz osób zatrudnionych, pełniących służbę lub wykonujących prace zlecone z dostępem do informacji niejawnych w jednostce organizacyjnej.
- Prowadzi aktualny wykaz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub mu je cofnięto.

OCHRONA INFORMACJI  
NIEJAWNYCH

---

---

---

---

---

---

---

---

### Pełnomocnik ochrony – odpowiada

- Zapewnienie ochrony inf. niej. w tym stosowanie środków bezpieczeństwa fizycznego.
- Zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane inf. niej.
- Opracowanie planu ochrony inf. niej. w jednostce, w tym w razie wprowadzenia stanu nadzwyczajnego.
- Zarządzanie ryzykiem, a w szczególności szacowanie ryzyka.
- Kontrola ochrony inf. niej.
- Przechowywanie akt zakończonych postępowań sprawdzających.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Odpowiedzialność pełnomocnika

W przypadku stwierdzenia naruszenia przepisów o oin pełnomocnik:

- zawiadamia kierownika jednostki,
- podejmuje niezwłocznie działania zmierzające do wyjaśnienia okoliczności,
- ogranicza jego negatywne skutki.

W przypadku stwierdzenia naruszenia przepisów o oin o klauzuli "poufne" lub wyższej:

- niezwłocznie zawiadamia ABW.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

PIERWSZY FILAR OCHRONY INFORMACJI  
NIEJAWNYCH

BEZPIECZEŃSTWO OSOBOWE

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

Zasady dostępu  
do informacji niejawnych

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Zasada ograniczonego dostępu

- Informacje niejawne mogą być udostępnione wyłącznie:

- osobie, która daje rękojmię zachowania tajemnicy
- w zakresie niezbędnym do wykonywania przez nią pracy na zajmowanym stanowisku lub innej zleconej pracy

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Zasada kontroli wytwórcy

- Klauzulę tajności nadaje osoba uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału,
- Bez jej pisemnej zgody albo jej przełożonego nie można zmienić lub znieść klauzuli tajności

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Zasada adekwatności środków bezpieczeństwa fizycznego

- Dostosowanie zakresu środków bezpieczeństwa fizycznego odpowiednio do poziomu zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Dostęp do informacji niejawnych

- Dopuszczenie osoby do pracy na stanowisku związanym z dostępem do informacji niejawnych może nastąpić po:
  - przeprowadzeniu postępowania sprawdzającego
  - pisemnym upoważnieniu przez kierownika jednostki (tylko do klauzuli „zastrzeżone”)
  - odbyciu szkolenia w zakresie ochrony informacji niejawnych

### Uwaga:

wyjątki od powyższej zasady może określać tylko ustawa.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Dostęp do informacji niejawnych

- Nie przeprowadza się postępowania sprawdzającego, jeżeli osoba, której postępowanie ma dotyczyć przedstawi odpowiednie poświadczenie bezpieczeństwa. Kierownik jednostki organizacyjnej informuje w terminie 7 dni organ, który wydał poświadczenie bezpieczeństwa, o zatrudnieniu osoby przedstawiającej to poświadczenie oraz ABW

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Rodzaje postępowań sprawdzających

- Zwykłe – do poziomu „poufne”
- Poszerzone – do poziomu „tajne” i „ściśle tajne”

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---



## Podmiot prowadzący postępowanie

- **Pełnomocnik ochrony** – zwykle postępowania sprawdzające.
- **ABW albo SKW** – postępowania poszerzone (do klauzuli tajne i ściśle tajne) oraz wobec kandydatów na pełnomocników ochrony oraz kierowników jednostek organizacyjnych.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Postępowanie sprawdzające

- Rękojmię zachowania tajemnicy sprawdza się poprzez czynności ściśle określone ustawą.  
W toku postępowania sprawdzającego ustala się, czy istnieją wątpliwości dotyczące:
  - Uczestnictwa, współpracy lub popierania przez osobę sprawdzaną działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej wymierzonej przeciwko RP.
- Ukrywania lub świadomego niezgodnego z prawdą podawania przez osobę sprawdzaną w postępowaniu sprawdzającym informacji mających znaczenie dla ochrony informacji niejawnych.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

- 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, albo współpracuje lub współpracowała z takimi partiami lub organizacjami.
- Zagrożenia osoby sprawdzanej ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania z nią kontaktu.
- Wystąpienia związanych z osobą sprawdzaną okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji.
- Niewłaściwego postępowania z informacjami niejawnymi.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### W toku postępowania sprawdzającego prowadzonego przez ABW

(poszerzone) ponadto ustala się, czy istnieją wątpliwości dotyczące:

1. Poziomu życia osoby sprawdzanej wyraźnie przewyższającego uzyskiwane przez nią dochody.
2. Informacjami o chorobie psychicznej lub innych zakłóceniach czynności psychicznych ograniczających sprawność umysłową i mogących negatywnie wpłynąć na zdolność osoby sprawdzanej do wykonywania prac związanych z dostępem do informacji niejawnych.
3. Uzależnienia od alkoholu, środków odurzających lub substancji psychotropowych.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Rodzaje postępowań sprawdzających

- Zakres prowadzonej procedury sprawdzającej jest uzależniony od poziomu dostępu do informacji niejawnych osoby sprawdzanej
- **Zwykłe postępowanie** sprawdzające obejmuje:
  - sprawdzenie, w niezbędnym zakresie, w ewidencjach, rejestrach i kartotekach, a w szczególności w Krajowym Rejestrze Karnym danych zawartych w wypełnionej i podpisanej przez osobę sprawdzaną ankiecie bezpieczeństwa osobowego;
  - sprawdzenie innych informacji uzyskanych w toku postępowania sprawdzającego w zakresie niezbędnym do ustalenia rękojmi zachowania tajemnicy

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Rodzaje postępowań sprawdzających

- sprawdzenie, na pisemny wniosek pełnomocnika ochrony, przez ABW w ewidencjach i kartotekach niedostępnych powszechnie, zawartych w ankiecie danych i innych informacji uzyskanych w toku postępowania sprawdzającego, w zakresie niezbędnym do ustalenia rękojmi zachowania tajemnicy;
- rozmowę z osobą sprawdzaną, w celu usunięcia nieścisłości lub sprzeczności zawartych w uzyskanych informacjach;

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

**Poszerzone postępowanie sprawdzające obejmuje:**

- czynności, o których mowa w art. 25 ust.1;
- rozmowę z przełożonymi osoby sprawdzanej;
- przeprowadzenie wywiadu w miejscu zamieszkania osoby sprawdzanej;
- sprawdzenie stanu i obrotów na rachunku bankowym oraz zadłużenia osoby sprawdzanej, w szczególności wobec Skarbu Państwa
- rozmowę z trzema osobami wskazanymi przez osobę sprawdzaną w celu uzyskania innych informacji mogących mieć znaczenie dla oceny dawania rękojmi (ściśle tajne)

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---



**Postępowania sprawdzające nie można przeprowadzić bez zgody osoby sprawdzanej**

OCHRONA INFORMACJI  
NIEJAWNYCH

---

---

---

---

---

---

---

---

**Wszczęcie postępowania**

- na pisemne polecenie kierownika jednostki organizacyjnej ⇒ pełnomocnik ds. ochrony informacji niejawnych
- na pisemny wniosek kierownika jednostki organizacyjnej lub osoby uprawnionej do obsady stanowiska lub zlecenie prac ⇒  
ABW lub SKW

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## UMORZENIE POSTĘPOWANIA SPRAWDZAJĄCEGO

- Umorzenie następuje w przypadku:
- śmierci osoby sprawdzanej;
- rezygnacji osoby sprawdzanej z ubiegania się o stanowisko albo zajmowania stanowiska lub wykonywania prac, związanych z dostępem do informacji niejawnych;
- odstąpienia przez kierownika jednostki organizacyjnej od zamiaru obsadzenia osoby sprawdzanej na stanowisku lub zlecenia jej prac związanych z dostępem do informacji niejawnych.
- gdy postępowanie z innej przyczyny stało się bezzasadne

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

---

---

ABW, SKW lub pełnomocnik ochrony mogą **zawiesić postępowanie** sprawdzające w przypadku:

- trwającej powyżej 30 dni choroby osoby sprawdzanej, uniemożliwiającej skuteczne przeprowadzenie postępowania sprawdzającego;
- wyjazdu za granicę osoby sprawdzanej na okres przekraczający 30 dni;
- wszczęcia przeciwko osobie sprawdzanej postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe;
- z innych przyczyn niezależnych od organu prowadzącego

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

---

---

## Zakończenie postępowania

- Postępowanie sprawdzające kończy się:
  - wydaniem poświadczenia bezpieczeństwa
  - odmową wydania poświadczenia bezpieczeństwa

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

---

---

## Ważność poświadczenia

- Poświadczenie bezpieczeństwa upoważnia osobę do dostępu do informacji klasyfikowanych przez:
  - 5 lat – do poziomu „ściśle tajne”
  - 7 lat – do poziomu „tajne”
  - 10 lat – do poziomu „poufne”

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Kontrolne Postępowanie Sprawdzające

W przypadku gdy w odniesieniu do osoby, której wydano poświadczenie bezpieczeństwa, zostaną ujawnione nowe fakty wskazujące, że nie daje ona rękojmi zachowania tajemnicy, ABW, SKW lub pełnomocnik ochrony przeprowadzają **kontrolne postępowanie sprawdzające** bez obowiązku wypełnienia nowej ankiety przez osobę sprawdzaną.

Kontrolne postępowanie sprawdzające prowadzone w/w podmioty kończy się:

- wydaniem decyzji o cofnięciu poświadczenia bezpieczeństwa ;
- poinformowaniem kierownika jednostki organizacyjnej lub osoby odpowiedzialnej za obsadę stanowiska i osoby sprawdzanej o braku zastrzeżeń w stosunku do osoby, którą objęto kontrolnym postępowaniem sprawdzającym, z jednoczesnym potwierdzeniem jej dalszej zdolności do zachowania tajemnicy w zakresie określonym w posiadanym przez nią poświadczeniu bezpieczeństwa.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Tryb odwoławczy

- Od decyzji o odmowie wydania lub decyzji o cofnięciu poświadczenia bezpieczeństwa albo umorzeniu postępowania sprawdzającego osobie sprawdzanej służy odwołanie do:
  - Szefa ABW albo SKW– w przypadku decyzji wydanej przez pełnomocnika ochrony
  - Prezesa Rady Ministrów – w przypadku odmowy wydanej przez ABW albo SKW

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Odpowiedzialność za ujawnienie informacji niejawnych



---

---

---

---

---

---

---

---

## Ujawnienie informacji

- Nie sporządza się kopii, odpisów, wypisów, wyciągów i tłumaczeń bez uzyskania stosownej zgody.
- Każdy wytworzony w ten sposób dokument podlega ochronie jak oryginał



---

---

---

---

---

---

---

---

## Przestępstwo ujawnienia informacji niejawnej o klauzuli ściśle tajne lub tajne

- **Art. 265. § 1.** Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje 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 informację określoną w § 1, z którą zapoznał się w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku



---

---

---

---

---

---

---

---

**Przestępstwo ujawnienia informacji niejawniej o klauzuli ściśle tajne lub tajne**

Art.265 kk

- **Strona przedmiotowa** - nieumyślne ujawnienie informacji o klauzuli ściśle tajne lub tajne
- **Podmiot** – osoba, która zapoznała się z informacjami w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem
- **Strona podmiotowa** – nieumyślność
- **Sankcja** – grzywna, kara ograniczenia wolności albo pozbawienia wolności do 1 roku

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

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

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

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

Art. 266 k.k.

- **Strona przedmiotowa** - ujawnienie lub wykorzystanie, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu informacji z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową
- **Podmiot** – osoba, na której ciąży ustawowy obowiązek nieujawnienia lub niewykorzystania uzyskanych informacji lub która obowiązek nieujawnienia lub niewykorzystywania przekazanych jej wiadomości na siebie przejęła
- **Strona podmiotowa** – umyślność
- **Sankcja** – grzywna, kara ograniczenia wolności albo pozbawienia wolności do 2 roku

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

**Przestępstwo ujawnienia informacji niejawnych o klauzuli poufne i zastrzeżone**

Art.266 § 2 Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli „zastrzeżone” lub „poufne” lub informacji, 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

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

Art. 266 k.k.

- Strona przedmiotowa – ujawnienie osobie nieuprawnionej informacji o klauzuli „zastrzeżone” lub „poufne” lub informacji uzyskanej w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes
- Podmiot – funkcjonariusz publiczny
- Strona podmiotowa – umyślność
- Sankcja – kara pozbawienia wolności do lat 3

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

**Przestępstwo nieuprawnionego uzyskania informacji**

Art.267 §1 – kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---



### Przestępstwo nieuprawnionego uzyskania informacji

Art.267 §2 Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego

- §3 Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem
- §4 Tej samej karze podlega, kto informację uzyskaną w sposób określony w §1-3 ujawnia innej osobie.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Przestępstwo nieuprawnionego uzyskania informacji

- Strona przedmiotowa – bezprawne zapoznanie się z treścią informacji poprzez: otwarcie zamkniętego pisma, podłączenie się do przewodu służącego do przekazywania informacji lub przełamanie zabezpieczeń: elektronicznych, magnetycznych albo innych szczególnych
- Podmiot – powszechny
- Strona podmiotowa – umyślność
- Sankcja – grzywna, kara ograniczenia wolności albo pozbawienia wolności do lat 2

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Przestępstwo niszczenia informacji

• Art.268 §1 – Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

**§2 – Jeżeli czyn określony w §1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.**

**§3 – Kto, dopuszczając się czynu określonego w §1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.**

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Przestępstwo niszczenia informacji

#### art.268 §1

- Strona przedmiotowa – nieuprawnione niszczenie, uszkodzenie, usuwanie lub zmiana zapisu istotnej informacji albo w inny sposób udaremnianie lub znaczne utrudnianie osobie uprawnionej zapoznanie się z tą informacją.
- Podmiot – powszechny
- Strona podmiotowa – umyślność
- Sankcja – grzywna, kara ograniczenia wolności albo pozbawienia wolności do lat 2

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Przestępstwo niszczenia informacji

#### art. 268 §2

- Strona przedmiotowa – nieuprawnione niszczenie informacji na nośniku komputerowym
- Podmiot – powszechny
- Strona podmiotowa – umyślność
- Sankcja – kara pozbawienia wolności 3 miesiące – 5 lat

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Przestępstwo niszczenia informacji

#### art. 268 §3

- Strona przedmiotowa – znaczna szkoda majątkowa powstała w wyniku zniszczenia informacji
- Podmiot – powszechny
- Strona podmiotowa – umyślność
- Sankcja – kara pozbawienia wolności 3 miesiące – 5 lat

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## Przestępstwo niszczenia danych informatycznych

art. 268 a

§1 kto nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§2 kto dopuszczając się czynu określonego w §1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 m. do lat 5

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

---

---

## Przestępstwo niszczenia danych informatycznych

- Strona przedmiotowa- nieuprawnione niszczenie, uszkadzanie, usuwanie, zmiana lub utrudnianie dostępu do danych informatycznych albo zakłócanie lub uniemożliwianie w istotnym stopniu automatycznego przetwarzania, gromadzenia lub przekazywania takich danych
- Podmiot – powszechny
- Strona podmiotowa – umyślność
- Sankcja – kara pozbawienia wolności do lat 3

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

---

---

## Przestępstwo sabotażu komputerowego

• 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 m. do lat 3

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

---

---

### Przestępstwo sabotażu komputerowego

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

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Przestępstwo komputerowe

• Art.269 b  
§1Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 §1 pkt 4, art. 267 §3, art. 268a §1 albo §2 w związku z §1, art. 269 §2 albo art. 269a, 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.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

### Kodeks karny

• Art. 269 - przestępstwo sabotażu komputerowego.  
Zagrożone sankcją pozbawienia wolności od 6 miesięcy do 8 lat.

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## WAŻNE ZASADY OCHRONY INFORMACJI NIEJAWNYCH

- **Nie wolno udostępniać** materiałów niejawnych osobie niewskazanej w rozdzielniku (dekretacji). Chodzi zarówno o umożliwienie wglądu w dokument klasyfikowany, jak i o ustne przekazanie jego treści
- Należy przestrzegać zakazu wnoszenia informacji klasyfikowanych poza strefy ochronne
- Należy pamiętać o właściwym archiwizowaniu i niszczeniu nośników informacji niejawnych
- wadliwy czy zbędny wydruk, wypis, wyciąg, kalka – to też dokumenty niejawne!

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---

## WAŻNE ZASADY OCHRONY INFORMACJI NIEJAWNYCH

- Informacje niejawne należy wytwarzać, przetwarzać i przechowywać wyłącznie w strefach ochronnych i z wykorzystaniem odpowiedniego, certyfikowanego sprzętu
- Nie sporządza się kopii, odpisów, wypisów, wyciągów i tłumaczeń bez uzyskania stosownej zgody. Każdy wytworzony w ten sposób dokument podlega ochronie jak oryginał.
- Należy sprawdzać zgodność liczby stron pobieranego dokumentu niejawnego i kwitować jego odbiór
- Należy pamiętać o wypełnianiu karty zapoznania się z dokumentem o klauzuli tajne i ściśle tajne

OCHRONA INFORMACJI  
NIEJAWNYCH

UNIWERSYTET SZCZECIŃSKI  
INSTYTUT NAUK O POLITYCE  
I BEZPIECZEŃSTWIE  
Katedra Studiów nad Bezpieczeństwem



---

---

---

---

---

---

---

---