



## KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Zarządzanie bezpieczeństwem systemów informatycznych

---

### Przedmiot

Kierunek studiów

Inżynieria Zarządzania

Studia w zakresie (specjalność)

Poziom studiów

pierwszego stopnia

Forma studiów

niestacjonarne

Rok/semestr

3/6

Profil studiów

ogólnoakademicki

Język oferowanego przedmiotu

polski

Wymagalność

obieralny

---

### Liczba godzin

Wykład

8

Ćwiczenia

10

Laboratoria

Projekty/seminaria

Inne (np. online)

### Liczba punktów ECTS

2

---

### Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:

dr inż. Maciej Siemieniak

e-mail: [maciej.siemieniak@put.poznan.pl](mailto:maciej.siemieniak@put.poznan.pl)

tel. 616653389

Wydział Inżynierii Zarządzania

ul. J.Rychlewskiego 2, 60-965 Poznań

Odpowiedzialny za przedmiot/wykładowca:

---

### Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę nt. systemów



informatycznych i informacyjnych. Powinien również posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł oraz mieć gotowość do podjęcia współpracy w ramach zespołu.

### Cel przedmiotu

Przekazanie studentom podstawowej wiedzy z zakresu bezpieczeństwa informacji i systemów informatycznych oraz doboru środków bezpieczeństwa i ochrony informacji, niezbędnych do prawidłowego projektowania, zarządzania i usprawniania systemów bezpieczeństwa teleinformatycznego. Rozwijanie u studentów umiejętności rozwiązywania problemów bezpieczeństwa informacji i systemów informatycznych.

### Przedmiotowe efekty uczenia się

#### Wiedza

Student definiuje kluczowe pojęcia i zasady związane z bezpieczeństwem informacji i systemów informatycznych, w tym cykl życia informacji i atrybuty bezpieczeństwa [P6S\_WG\_01].

Student identyfikuje i opisuje różne etapy w cyklu życia systemów społeczno-technicznych, ze szczególnym uwzględnieniem aspektów bezpieczeństwa informacji [P6S\_WG\_13].

Student wyjaśnia podstawowe zasady zarządzania jakością i ich zastosowanie w kontekście bezpieczeństwa systemów informatycznych [P6S\_WK\_02].

#### Umiejętności

Student analizuje wyniki eksperymentów i symulacji komputerowych dotyczących bezpieczeństwa systemów informatycznych i wyciąga wnioski dotyczące ich skuteczności i zastosowań [P6S\_UW\_09].

Student stosuje metody analityczne i narzędzia symulacyjne do projektowania i wdrażania strategii bezpieczeństwa w systemach informatycznych [P6S\_UW\_10].

Student integruje wiedzę teoretyczną i praktyczne umiejętności do rozwiązywania złożonych problemów związanych z bezpieczeństwem systemów informatycznych w różnorodnych środowiskach organizacyjnych [P6S\_UW\_11].

#### Kompetencje społeczne

Student opracowuje strategie i plany wdrożenia systemów bezpieczeństwa informatycznego, uwzględniając różnorodne aspekty techniczne, ekonomiczne, prawne i organizacyjne [P6S\_KO\_02].

Student podejmuje odpowiedzialne decyzje dotyczące zarządzania bezpieczeństwem systemów informatycznych, uwzględniając ich wpływ na środowisko i społeczność [P6S\_KR\_01].

### Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta na wykładach weryfikowana jest przez jedno kolokwium, które odbywa się na ostatnich zajęciach. Kolokwium składa się z 10 pytań testowych różnie punktowanych. Próg zaliczeniowy: 50% prawidłowych odpowiedzi. Zagadnienia zaliczeniowe obejmują wyłącznie materiał z wykładów.



Na ćwiczeniach studenci pracują indywidualnie i w małych grupach nad zadanymi tematami, które prezentują w formie prezentacji multimedialnej. Za każde zadanie studenci otrzymują oceny. Treść zadań związana jest z przedmiotem, a zakres zadań obejmuje zagadnienia z wykładów.

### Treści programowe

Wykłady:

Prezentacja multimedialna dla studentów o tematyce:

1. bezpieczeństwo informacji (znaczenie i definicje informacji, cykl życia informacji, istota bezpieczeństwa informacji, pojęcia związane z bezpieczeństwem informacji, incydenty, elementy bezpieczeństwa informacji, ewolucja systemu zarządzania bezpieczeństwem informacji (ISMS), standardy ISMS, polityka ISMS w organizacji, model ISMS, ryzyko, wdrożenie ISMS w organizacji, metody szacowania ryzyka).
2. bezpieczeństwo systemów informatycznych (pojęcia, definicje, odniesienie do bezpieczeństwa informacji, atrybuty bezpieczeństwa, strategie zarządzania ryzykiem i jego redukcji, trójpoziomowy model odniesienia, model hierarchii zasobów, strategia wyboru zabezpieczeń, czynności wdrożeniowe i powdrożeniowe).

Zajęcia ćwiczeniowe:

Prowadzący:

Wyjaśnienie istoty stosowanych narzędzi i sposobu wykonania zadań dla poniższych tematów: mapa myśli, diagram Ishikawy, drzewo błędów i zdarzeń, diagram przepływu, mini wykład o maxi sprawach, wykład z przedmiotu; Tematy zadań związane z bezpieczeństwem informacji i systemów informatycznych.

Studenci:

1. mapa myśli dla pojęcia "informacja" - prezentacja multimedialna lub graficzna (plakat) z omówieniem;
2. diagram Ishikawy dla problemu "nieuprawniony dostęp do danych lub informacji w przedsiębiorstwie" (rodzaj danych/informacji dowolny: finansowe, osobowe, technologiczne, produkcyjne, badanie i rozwój, strategii sprzedaży, itp.) - prezentacja multimedialna lub graficzna (plakat) z omówieniem;
3. drzewo błędów i zdarzeń dla zdarzenia "skradziono laptop z samochodu prezesa" - prezentacja multimedialna z omówieniem;
4. diagram przepływu - na podstawie tekstu opisującego proces wprowadzania danych do systemu IT (algorytm, procesy decyzyjne, działania, wykonawcy) - prezentacja multimedialna z omówieniem;
5. mini wykład o maxi sprawach - prezentacja multimedialna w formie wykładu/odczytu (kryptologia, przestępczość komputerowa, cyberterroryzm, spam, łańcuszek internetowy, hacker, cracker, złośliwe oprogramowanie - profilaktyka i zabezpieczenia, zagrożenia w internecie - ochrona, zapobieganie,



najpopularniejsze serwisy społecznościowe - negatywne zjawiska, jak bezpiecznie z nich korzystać, bezpieczne zakupy w internecie, bezpieczne logowanie, bezpieczne hasła);

6. zarządzanie bezpieczeństwem systemów informatycznych - prezentacja multimedialna w formie wykładu/odczytu (zarys problemu, najważniejsze zagadnienia, na podstawie wykładów);

### **Metody dydaktyczne**

Wykłady: prezentacja multimedialna - tekst, rysunki, schematy, tabele, przykłady wyjaśniające, krótka rozmowa ze studentami.

Ćwiczenia: prowadzący - prezentacja multimedialna, studenci - prezentacja multimedialna, graficzna (plakat), krótki wykład, odczyt, dyskusja.

### **Literatura**

#### Podstawowa

1. Białas A. (2023), Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. Wydawnictwo Naukowe PWN, WNT
2. Jason A., (2021), Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie. Wydawnictwo Helion
3. Kowalewski J., Kowalewski M., (2021), Zarządzanie ryzykiem w bezpieczeństwie informacji organizacji. Oficyna Wydawnicza Politechniki Warszawskiej
4. Jacek Łuczak, Marcin Tyburski, Systemowe zarządzanie bezpieczeństwem informacji. Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Poznań 2010.

#### Uzupełniająca

1. Molendowska M., Miernik R., (2021), Bezpieczeństwo w cyberprzestrzeni. Wybrane zagadnienia. Wydawnictwo Adam Marszałek
2. Andrzej Borucki, Gospodarka elektroniczna. Wydawnictwo Politechniki Poznańskiej, 2013.
3. Andrzej Borucki, E-biznes. Wydawnictwo Politechniki Poznańskiej, 2012.
4. Stokłosa J. i inni, Ochrona danych i zabezpieczenia w systemach teleinformatycznych, Wydawnictwo Politechniki Poznańskiej 2003
5. Anderson R., Inżynieria zabezpieczeń, Wydawnictwo Naukowo - Techniczne 2005



**Bilans nakładu pracy przeciętnego studenta**

	Godzin	ECTS
Łączny nakład pracy	50	2,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	20	1,0
Praca własna studenta (studia literaturowe, przygotowanie do ćwiczeń, przygotowanie do kolokwium) <sup>1</sup>	30	1,0

<sup>1</sup> niepotrzebne skreślić lub dopisać inne czynności