POLSKO-JAPOŃSKA AKADEMIA TECHNIK KOMPUTEROWYCH

SYLABUS PRZEDMIOTU

Nazwa przedmiotu:	**Bezpieczeństwo systemów informacyjnych (BSI)**
Kod przedmiotu:	BSI
Kierunek / Profil:	Informatyka / praktyczny
Tryb studiów:	stacjonarny
Rok / Semestr:	3 / 5
Charakter:	obowiązkowy
Odpowiedzialny:	dr Andrzej Bobyk
Wersja z dnia:	19.02.2026

1. Godziny zajęć i punkty ECTS

Wykłady	Ćwiczenia	Laboratori	Z prowa-dzącym	Praca własna	Łącznie	ECTS
15 h	15 h	15 h	45 h	55 h	100 h	**4**

2. Forma zajęć

Forma zajęć	Sposób zaliczenia
Wykład	Nieoceniany

3. Cel dydaktyczny

Celem przedmiotu jest zapoznanie słuchaczy z zasadami i metodami ochrony informacji w systemach i sieciach komputerowych.

4. Przedmioty wprowadzające

Przedmiot	Wymagane zagadnienia
ALG, SKOA	Podstawy algebry, wiedza z zakresu systemów operacyjnych i sieci komputerowych.

5. Treści programowe

1. Polityka bezpieczeństwa systemów informatycznych: etapy tworzenia struktur bezpieczeństwa, zasady efektywnej strategii i polityki bezpieczeństwa. Usługi związane z ochroną informacji, kategorie zagrożeń systemów informatycznych.
2. Elementy kryptografii: podstawowe techniki szyfrowania, zastosowania technik szyfrowania, algorytmy symetryczne (DES, 3DES, IDEA).Algorytmy asymetryczne: (RSA, El-Gamal), uwierzytelnianie i sygnatury cyfrowe. Podpis elektroniczny.
3. Bezpieczeństwo w sieciach: usługi i protokoły kryptograficzne (SSL, SSH, Kerberos), bezpieczeństwo poczty elektronicznej; protokoły PGP i PEM, zarządzanie kluczami, certyfikaty.
4. Praktyka ochrony danych w systemach komputerowych: programy złośliwe (wirusy, robaki, konie trojańskie), archiwizacja danych – procedury, metody, programy.

6. Efekty kształcenia

Wiedza

- Student zna i rozumiepodstawowe zagadnienia i pojęcia kryptografii i kryptoanalizy oraz zasady działania algorytmów kryptograficznych.
- Student zna problematykę bezpieczeństwa w nowoczesnych systemach informatycznych; rozumie pojęcia związane z poufnością, integralnością, dostępnością, uwierzytelnianiem, autoryzacją i ewidencjonowaniem.
- Student zna i rozumie pojęcia związane z implementowaniem zapór ogniowych, ochrony przed wtargnięciami do sieci, systemów kryptograficznych, implementacji wirtualnych sieci prywatnych i zarządzania bezpiecznymi sieciami komputerowymi; zna metody zabezpieczania urządzeń sieciowych i systemów komputerowych.

Umiejętności

- Brak danych.

7. Kryteria oceny

- Ćwiczenia / Laboratorium:
- rozwiązywanie zadań
- Ćwiczenia/Laboratorium

- Kryteria oceny
- Ćwiczenia/Laboratorium
- Student jest zobowiązany uzyskać ponad 50% punktów możliwych do zdobycia w trakcie trwania semestru.

8. Metody dydaktyczne

Wykład, laboratoria, praca własna studenta.

9. Literatura

Podstawowa:

- D. E. Robling Denning: Kryptografia i ochrona danych. WNT, Warszawa 1993.
- S. Garfinkel, G. Spafford: Bezpieczeństwo w Unixie i Internecie. RM, Warszawa 1997 (+A. Schwartz: Practical UNIX and Internet Security. 3rd Edition. O'Reilly Media 2003).
- W. Stallings: Ochrona danych w sieci i intersieci. W teorii i praktyce. WNT, Warszawa 1997.
- M. Kutyłowski, W.-B. Strothmann: Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych (wyd. 2). Read Me, Warszawa 1999.
- J.-P. Aumasson: Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania. PWN, Warszawa 2018.
- J. Andress: Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie. Helion, Gliwice 2021.

Uzupełniająca:

- C. Adams, S. Lloyd: Podpis elektroniczny. Klucz publiczny. Robomatic, Warszawa 2002.
- R. Wobst: Kryptologia. Budowa i łamanie zabezpieczeń. RM, Warszawa, 2002.
- F. L. Bauer: Sekrety kryptografii. Helion, Gliwice 2002.
- D. R. Stinson: Kryptografia. WNT, Warszawa, 2005.