# Wstęp do kryptologii - opis przedmiotu

## Informacje ogólne

| | |
|---|---|
| Nazwa przedmiotu | Wstęp do kryptologii |
| Kod przedmiotu | 14.1--Poli2P-WK-S22 |
| Wydział | Wydział Nauk Społecznych |
| Kierunek | Politologia |
| Profil | ogólnoakademicki |
| Rodzaj studiów | pierwszego stopnia |
| Semestr rozpoczęcia | semestr zimowy 2022/2023 |

## Informacje o przedmiocie

| | |
|---|---|
| Semestr | 4 |
| Liczba punktów ECTS do zdobycia | 2 |
| Występuje w specjalnościach | Służby specjalne w świecie współczesnym |
| Typ przedmiotu | obowiązkowy |
| Język nauczania | polski |
| Sylabus opracował | • dr inż. Janusz Jabłoński |

## Formy zajęć

| Forma zajęć | Liczba godzin w semestrze (stacjonarne) | Liczba godzin w tygodniu (stacjonarne) | Liczba godzin w semestrze (niestacjonarne) | Liczba godzin w tygodniu (niestacjonarne) | Forma zaliczenia |
|---|---|---|---|---|---|
| Ćwiczenia | 30 | 2 | - | - | Zaliczenie na ocenę |

## Cel przedmiotu

Zapoznanie studentów z zagadnieniami związanymi z bezpieczeństwem informacji oraz bezpieczeństwem systemów informatycznych. Zapoznanie studentów z obowiązującymi normami i przepisami w zakresie bezpieczeństwa informacyjnego i ochrony danych. Wprowadzenie w zagadnienia dotyczące poziomu bezpieczeństwa systemów kryptograficznych w zabezpieczaniu informacji oraz wprowadzenia do krypto-analizy w przełamywaniu zabezpieczeń.

## Wymagania wstępne

Brak

## Zakres tematyczny

1. Teorią i praktyka bezpieczeństwa informacji - interpretacja atrybutów bezpieczeństwa.
2. Rola informacji we współczesnym świecie - ukrywanie informacji z użyciem Kryptologii.
3. Kryptografia symetryczna i asymetryczna generatory pseudolosowe - teoria i praktyka.
4. Kryptogrficzne i formalno prawne aspekty uwierzytelniania i kontroli dostepu - przykłady użycia.
5. Systemy kryptograficzne poziom bezpieczeństwa a metody kryptoanalizy - jak to wyznaczyć?
6. System informatyczny i operacyjny w ochronie danych i informacji - ustawienia i funkcje.
7. Podpis cyfrowy i Blockchain - nowe technologie dla bezpieczeństwa kryptograficznego.
8. Normalizacja i legislacja dla podnoszenia poziomów bezpieczeństwa informacyjnego.

## Metody kształcenia

Wprowadzenie do ćwiczeń z wykorzystaniem prezentacji multimedialnej. Praca ze źródłami literaturowymi i Internetu. Dyskusja i rozwiązywanie zadań pod nadzorem prowadzącego i poza zajęciami.

## Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

| Opis efektu | Symbole efektów | Metody weryfikacji | Forma zajęć |
|---|---|---|---|
| zasady bezpieczeństwa cyfrowego oraz podatności i zagrożenia bezpieczeństwa informacji w kontekście Cyberbezpieczeństwa | • KP1_W11 | • aktywność w trakcie zajęć<br>• sprawdzian z progami punktowymi | • Ćwiczenia |
| prowadzenie na poziomie podstawowym prac dotyczących analizy zagrożeń Cybernetycznych oraz rozpoznawać metody przeciwdziałania zagrożeniom bezpieczeństwa informacyjnego | • KP1_U11 | • aktywność w trakcie zajęć<br>• test z pytaniami zamkniętymi i otwartymi | • Ćwiczenia |
| wykorzystanie kompetencji społecznych w obszarze bezpieczeństwa informacji opartego na kryptologii | • KP1_K07 | • aktywność w trakcie zajęć<br>• test z pytaniami zamkniętymi i otwartymi | • Ćwiczenia |

## Warunki zaliczenia

Uzyskanie 30 punktów. Realizacja zadań na ćwiczeniach sumaryczna liczba punktów do uzyskania 15, udział w dyskusji suma punktów do uzyskania 5, sprawdzian podsumowujący liczba punktów do uzyskania 10. Ocena za uzyskane punkty: 0-14 niedostateczny, 15 - 18 dostateczny, 19 - 22 dostateczny plus, 22-25 dobry, 26 - 28 dobry plus, 29-30 bardzo dobry.

## Literatura podstawowa


1. N. Koblitz, Wykład z teorii liczb i kryptografii, Warszawa WNT -2018
2. W. Stallings, L. Brown, Bezpieczeństwo Systemów Informatycznych, tom 1 i 2, Gliwice Helion - 2019
3. A. Chrzęszczeyk, Algorytmy teorii liczb i kryptografii w przykładach, Legionowo BTC - 2010


## Literatura uzupełniająca


1. M. Karbowski, Podstawy kryptografii, Gliwice Helion - 2014
2. A. Menezes, P. van Oorschot, S. Vanstone „Handbook of Applied Cryptography" Springer-Verlag 1996.
3. Internetowy System Aktów Prawnych (sejm.gov.pl)


## Uwagi

Zmodyfikowane przez dr inż. Janusz Jabłoński (ostatnia modyfikacja: 17-05-2022 13:20)