KARTA PRZEDMIOTU DLA NABORU 2019/2020

INFORMACJE OGÓLNE

1. **Nazwa przedmiotu kształcenia**
   Bezpieczeństwo i ochrona danych w systemach komputerowych
2. **Nazwa jednostki prowadzącej moduł** Zakład Informatyki
3. **Grupa treści kształcenia** -
4. **Typ przedmiotu** obowiązkowy
5. **Poziom studiów** pierwszego stopnia
6. **Liczba punktów ECTS** 2
7. **Poziom przedmiotu** podstawowy
8. **Rok studiów, semestr** III rok, semestr 6
9. **Liczba godzin w semestrze** wykład 15, laboratorium 15
10. **Język wykładowy:** polski
11. **Wykładowca (wykładowcy)** Zofia Lubańska, mgr inż.

INFORMACJE SZCZEGÓŁOWE

12. Wymagania wstępne

1) Wiedza z zakresu podstaw informatyki i architektury systemów komputerowych, budowa komputera
2) Podstawy działania sieci komputerowych, systemów operacyjnych, bazy danych

13. Cele przedmiotu

C1 poznanie prawnych, organizacyjnych i technicznych aspektów przestępczości komputerowej

C2 poznanie podstawowych zasad z zakresu kryptologii

C2 znajomość struktur organizacyjnych, norm z zakresu cyberbezpieczeństwa

C3 poznanie zastosowania nowoczesnych rozwiązań teleinformatycznych z zakresu cyberbezpieczeństwa

14. Efekty uczenia się w zakresie wiedzy, umiejętności i kompetencji społecznych

Student, który zaliczył przedmiot potrafi:	odniesienie do kierunkowych efektów uczenia się
WIEDZA	
EU01 zna podstawowe metody, techniki, narzędzia programowe oraz aparaturę i sprzęt stosowane przy rozwiązywaniu prostych zadań inżynierskich z zakresu systemów informatycznych	I1P_W05 I1P_W20 I1P_W21
EU02 orientuje się w obecnym stanie i najnowszych trendach rozwojowych w informatyce	
EU03 ma elementarną wiedzę na temat cyklu życia urządzeń i systemów informatycznych	
UMIEJĘTNOŚCI	
EU04 potrafi ocenić przydatność metod i narzędzi służących do rozwiązywania prostych zadań inżynierskich typowych dla informatyki oraz wybierać i stosować właściwe metody i narzędzia między innymi do zabezpieczenia usług sieciowych	I1P_U25 I1P_U30
EU05 potrafi mówić o zagadnieniach informatycznych zrozumiałym językiem	
KOMPETENCJE SPOŁECZNE	
EU06 rozumie potrzebę i zna możliwości ciągłego dokształcania się (studia drugiego i trzeciego stopnia, studia podyplomowe i kursy), podnoszenia kompetencji zawodowych, osobistych i społecznych	I1P_K01 I1P_K04
EU07 ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole i podnoszenia odpowiedzialności za wspólnie realizowane zadania	

15. Treści programowe

Forma zajęć – wykłady

W1. Podstawowe pojęcia i definicje
W2. Odpowiedzialność Państwa za cyberbezpieczeństwo
W3. Cyberbezpieczeństwo, skala, zjawiska
W4. Działania cyberprzestępców
W5. Nadużycia w sieciach komputerowych
W6. Prawne aspekty przestępstw komputerowych
W7. Podstawy kryptografii

W8. Zaliczenie

Forma zajęć – laboratoria

L1. Wstęp, przegląd literatury
L2. Zabezpieczanie danych przy pomocy wykonywania kopii bezpieczeństwa danych systemu Windows
L3. Zabezpieczenie danych przy użyciu certyfikatów: SSL.
L4. Zabezpieczenie danych przy użyciu certyfikatów: Code Signing, ID i VPN
L5. Stosowanie podpisu elektronicznego niekwalifikowanego w wersji testowej
L6. Firewall sprzętowy i programowy- konfiguracja i zasada działania
L7. Bezpieczeństwo osobiste w Internecie
L8. Zaliczenie

16. Narzędzia/metody dydaktyczne

1. Wykład: wykorzystanie prezentacji multimedialnej, filmów szkoleniowych
2. Laboratorium: dostępne darmowe oprogramowanie z zasobów Internetu

17. Sposoby oceny (F – formująca; P – podsumowująca)

F1. Dyskusja, prelekcja

P1. Zaliczenie – forma do uzgodnienia ze studentami

18. Obciążenia pracą studenta

forma aktywności	średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem*	30+5
Nakład pracy studenta	
Przygotowanie ćwiczeń/laboratoriów	10
Przygotowanie do zaliczenia	5
SUMA	50
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	2

19. Literatura podstawowa i uzupełniająca

Literatura podstawowa:

1) Wojciechowska-Filipek S., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki organizacji, państwa*, Warszawa, CEDEWU
2) Ferguson N., Schneier B., *Kryptografia w praktyce: dwaj światowej klasy eksperci kryptografii powiedzą Ci, jak zabezpieczyć Twoją cyfrową przyszłość*, Gliwice, HELION
3) Krawiec J., *Cyberbezpieczeństwo: podejście systemowe*, Warszawa, OFICYNA WYDAWNICZA POLITECHNIKI WARSZAWSKIEJ

Literatura uzupełniająca:

1) Szymonik A., *Organizacja i funkcjonowanie systemów bezpieczeństwa*, Warszawa, DIFIN
2) Górka M., *Bezpieczeństwo dzieci i młodzieży: realny i wirtualny problem polityki bezpieczeństwa*, Warszawa, DIFIN

20. Formy oceny - szczegóły

Warunki uzyskania zaliczenia przedmiotu: zajęcia kończą się egzaminem.

Sposób weryfikacji efektów uczenia się:

Ocena stopnia osiągniętych przez studenta efektów uczenia się następuje wg poniższych kryteriów:
5.0 – zakładany efekt uczenia się został osiągnięty bez zastrzeżeń
4.5 – zakładany efekt uczenia się został osiągnięty z pojedynczymi brakami/błędami
4.0 – zakładany efekt uczenia się został osiągnięty z nielicznymi brakami/błędami
3.5 – zakładany efekt uczenia się został osiągnięty z wieloma brakami/błędami
3.0 – zakładany efekt kształcenia został osiągnięty z licznymi i istotnymi brakami/błędami (minimalnie wymagany poziom osiągnięcia efektu)
2.0 – zakładany efekt uczenia się nie został osiągnięty

21. Inne przydatne informacje o przedmiocie

1. Bezpośrednich informacji o problematyce zajęć i treściach programowych udziela Prowadzący w trakcie zajęć i podczas konsultacji
2. Zajęcia odbywać się będą w PSW w Białej Podlaskiej
3. Zajęcia odbywać się będą zgodnie z aktualnym planem zajęć
4. Konsultacje odbywać się będą zgodnie z obowiązującym terminarzem

* Zajęcia prowadzone z bezpośrednim udziałem nauczyciela akademickiego lub innej osoby prowadzącej zajęcia oraz konsultacje