KARTA PRZEDMIOTU DLA NABORU 2021/2022
FORMA: STUDIA STACJONARNE

INFORMACJE OGÓLNE

1.Nazwa przedmiotu Cyberbezpieczeństwo

2. Nazwa kierunku Informatyka

3. Poziom studiów studia pierwszego stopnia

4. Liczba punktów ECTS2

5. Liczba godzin w semestrze

semestr	w	ćw	lab/lek	prj/zp	prk
VI	15		15		

6. Język wykładowypolski

7. Wykładowca mgr inż. Zofia Lubańska

INFORMACJE SZCZEGÓŁOWE

8. Wymagania wstępne

1.Wiedza z zakresu podstaw informatyki i architektury systemów komputerowych, budowa komputera

2. Podstawy działania sieci komputerowych, systemów operacyjnych, bazy danych

9. Cele przedmiotu

C1 poznanie prawnych, organizacyjnych i technicznych aspektów przestępczości komputerowej

C2 poznanie podstawowych zasad z zakresu kryptologii

C3 znajomość struktur organizacyjnych, norm z zakresu cyberbezpieczeństwa

C4 poznanie zastosowania nowoczesnych rozwiązań teleinformatycznych z zakresu cyberbezpieczeństwa

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

Student, który zaliczył przedmiot:		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	K_W05
EU02	orientuje się w obecnym stanie i najnowszych trendach rozwojowych w informatyce	K_W20
EU03	ma elementarną wiedzę na temat cyklu życia urządzeń i systemów informatycznych	K_W21
	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	K_U25
EU05	potrafi mówić o zagadnieniach informatycznych zrozumiałym językiem	K_U29, K_U30
	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	K_K01
EU07	ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole i podnoszenia odpowiedzialności za wspólnie realizowane zadania	K_K04

11. Treści programowe

Forma zajęć – wykłady/ ćwiczenia/laboratoria/zajęcia praktyczne itp.

Wykłady

1. Podstawowe pojęcia i definicje
2. Odpowiedzialność Państwa za cyberbezpieczeństwo
3. Cyberbezpieczeństwo, skala, zjawiska
4. Działania cyberprzestępców
5. Nadużycia w sieciach komputerowych
6. Prawne aspekty przestępstw komputerowych
7. Podstawy kryptografii

Laboratoria

1. Wstęp, przegląd literatury
2. Zabezpieczanie danych przy pomocy wykonywania kopii bezpieczeństwa danych systemu Windows
3. Zabezpieczenie danych przy użyciu certyfikatów: SSL
4. Zabezpieczenie danych przy użyciu certyfikatów: CodeSigning, ID i VPN
5. Stosowanie podpisu elektronicznego niekwalifikowanego w wersji testowej
6. Firewall sprzętowy i programowy- konfiguracja i zasada działania
7. Bezpieczeństwo osobiste w Internecie

12. Narzędzia/metody dydaktyczne

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

13. Sposoby oceny (cząstkowe, końcowe)

1. Dyskusja, prelekcja
2. Zaliczenie – forma do uzgodnienia ze studentami

14. Obciążenie pracą studenta

Forma aktywności	liczba godzin
1. Zajęcia z bezpośrednim udziałem nauczyciela oraz konsultacje	35
2. Nakład pracy studenta	15
suma	50
liczba punktów ECTS	2

15. Literatura

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
3.
16. Formy oceny – szczegóły
Warunki uzyskania zaliczenia przedmiotu: zajęcia kończą się egzaminem. **<u>Sposób weryfikacji efektów uczenia się:</u>** 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
17. 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 Akademii Bialskiej im. Jana Pawła II
3. Zajęcia odbywać się będą zgodnie z aktualnym planem zajęć
4. Konsultacje odbywać się będą zgodnie z obowiązującym terminarzem