

KARTA PRZEDMIOTU DLA NABORU 2022/2023 FORMA STUDIÓW: STACJONARNA						
INFORMACJE OGÓLNE						
1. Nazwa przedmiotu Cyberbezpieczeństwo						
2. Nazwa kierunku Informatyka						
3. Poziom studiów studia pierwszego stopnia						
4. Liczba punktów ECTS 2						
5. Liczba godzin w semestrze						
semestr	w	ćw	lab/lek	prj/zp	pws	prk
VI	15		30			
6. Język wykładowy polski						
7. Wykładowca mgr inż. Andrzej Jasiński						
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 i rozumie współczesne problemy cyberbezpieczeństwa				K_W06, K_W09	
EU02	Zna i rozumie metody i narzędzia pozwalające zaprojektować i uruchomić usługi bezpieczeństwa w sieci				K_W06, K_W09	
UMIEJĘTNOŚCI						
EU04	potrafi zaprojektować, uruchomić i przetestować usługę bezpieczeństwa w sieci				K_U06, K_U10, K_U13	
EU05	potrafi dobrać odpowiedni poziom bezpieczeństwa w celu zapewnienia ochrony				K_U17, K_U18	
KOMPETENCJE SPOŁECZNE						
EU06	rozumie potrzebę i zna możliwości ciągłego dokształcania się				K_K01	
EU07	ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole i podnoszenia odpowiedzialności za wspólnie realizowane				K_K04	

zadania	
11. Treści programowe	
Forma zajęć – wykłady/laboratoria	
<p>Wykłady</p> <ol style="list-style-type: none"> 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 <p>Laboratoria</p> <ol style="list-style-type: none"> 1. Zadania związane z cyberbezpieczeństwem 2. Zabezpieczanie danych przy pomocy wykonywania kopii bezpieczeństwa danych systemu Windows 3. Zabezpieczenie danych przy użyciu certyfikatów: SSL 4. Zabezpieczenie danych przy użyciu certyfikatów: Code Signing, 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 (częstkowe, końcowe)	
1. Dyskusja, prelekcja	
2. Zaliczenie – forma do uzgodnienia ze studentami	
3. Zaliczenie pisemne	
14. Obciążenie pracą studenta	
Forma aktywności	liczba godzin
1. Zajęcia z bezpośrednim udziałem nauczyciela oraz konsultacje	45
2. Nakład pracy studenta	5
suma	50
liczba punktów ECTS	2
15. Literatura	
Literatura podstawowa:	
1. Wojciechowska-Filipek S., <i>Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki organizacji, państwa</i> , Warszawa, CEDEWU, 219	
2. Ferguson N., Schneier B., <i>Kryptografia w praktyce: dwaj światowej klasy eksperci kryptografii powiedzą Ci, jak zabezpieczyć Twoją cyfrową przyszłość</i> , Gliwice, HELION, 2004	
3. Krawiec J., <i>Cyberbezpieczeństwo: podejście systemowe</i> , Warszawa, OFICyna WYDAWNICZA POLITECHNIKI WARSZAWSKIEJ, 2019	
Literatura uzupełniająca:	
1. Szymonik A., <i>Organizacja i funkcjonowanie systemów bezpieczeństwa</i> , Warszawa, DIFIN, 2011	
2. Górka M., <i>Bezpieczeństwo dzieci i młodzieży: realny i wirtualny problem polityki bezpieczeństwa</i> , Warszawa, DIFIN, 2017	
16. 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

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 Białskiej im. Jana Pawła II
3. Zajęcia odbywać się będą zgodnie z aktualnym planem zajęć
4. Konsultacje odbywać się będą zgodnie z obowiązującym terminarzem