



IV. Opis programu studiów

3. KARTA PRZEDMIOTU

Kod przedmiotu	E-ID1T-05-s6
Nazwa przedmiotu	Cyberbezpieczeństwo
Nazwa przedmiotu w języku angielskim	Cybersecurity
Obowiązuje od roku akademickiego	2019/20

USYTUOWANIE MODUŁU W SYSTEMIE STUDIÓW

Kierunek studiów	
Poziom kształcenia	
Profil studiów	
Forma i tryb prowadzenia studiów	
Zakres	
Jednostka prowadząca przedmiot	
Koordynator przedmiotu	Dr inż. Mirosław Płaza
Zatwierdził	Dziekan Wydziału Elektrotechniki Automatyki i Informatyki Dr hab. inż. Antoni Różowicz, prof. PŚk

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów	
Status przedmiotu	
Język prowadzenia zajęć	
Usytuowanie modułu w planie studiów - semestr	
Wymagania wstępne	Sieci komputerowe, Podstawy routing i przełączania, Technologie IoT - Rozproszone Sieci Sensoryczne
Egzamin (TAK/NIE)	
Liczba punktów ECTS	

Forma prowadzenia zajęć	wykład	ćwiczenia	laboratorium	projekt	Inne
Liczba godzin w semestrze	15	0	30	0	0

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W01	Zna i rozumie współczesne problemy cyberbezpieczeństwa.	INF1_W10 INF1_W27
	W02	Dysponuje wiedzą pozwalającą zaprojektować /uruchomić usługi bezpieczeństwa w sieci teleinformatycznej.	INF1_W10 INF1_W27
	W03	Ma uporządkowaną szeroką wiedzę z zakresu architektury, organizacji i bezpieczeństwa systemów operacyjnych.	INF1_W09 INF1_W27 INF1_W28
Umiejętności	U01	Potrafi dobrać odpowiedni poziom bezpieczeństwa w celu zapewnienia ochrony przed zagrożeniami.	INF1_U31
	U02	Potrafi zaprojektować / uruchomić / przetestować usługę bezpieczeństwa w sieci teleinformatycznej.	INF1_U31 INF1_U24
	U03	Potrafi planować i przeprowadzać eksperymenty z zakresu ochrony zasobów dostępnych przez sieci teleinformatyczne.	INF1_U31 INF1_U25
Kompetencje społeczne	K01	Ma świadomość znaczenia cyberbezpieczeństwa w dzisiejszym świecie.	INF1_K07
	K02	Umie pracować i współdziałać w grupie w zakresie obejmującym tworzenie zabezpieczeń w obszarze teleinformatyki.	INF1_K03

TREŚCI PROGRAMOWE

Forma zajęć*	Treści programowe
wykład	1. Wprowadzenie do zagadnień cyberbezpieczeństwa-cyberprzestrzeń, cyberbezpieczeństwo, cyberprzestępczość.
	2. Zagrożenia, luki i ataki w cyber świecie - oprogramowanie złośliwe i zaawansowane mechanizmy ochrony. Ataki DoS, DDoS i sposoby reagowania na nie.
	3. Algorytmy szyfrowania i kontrola dostępu. Elementy kryptografii: kryptografia symetryczna i asymetryczna.
	4. Ataki dostępowe. Ataki na infrastrukturę i usługi sieciowe. Bezpieczeństwo sieci bezprzewodowych.
	5. Sieci VPN. Systemy szyfrowania, uwierzytelniania i infrastruktura klucza publicznego (PKI)
	6. Maskowanie ataków. Analiza włamań. Systemy zapobiegające wyciekom danych (DLP).
	7. Systemy IPS/IDS. Rozwiązania w chmurze z zakresu cyberbezpieczeństwa dla małych i średnich przedsiębiorstw.
	8. Polityka bezpieczeństwa systemów informatycznych. Zasady projektowania systemów zabezpieczeń i ich oceny.
laboratorium	1. Zadania związane z cyberbezpieczeństwem - identyfikacja zagrożeń.
	2. Tworzenie cyberświata - wybrane techniki komunikacji.
	3. Ochrona danych w cyberświecie - badanie integralności danych.
	4. Budowa wirtualnej maszyny.
	5. Praktyki szyfrowania danych.
	6. Wykrywanie zagrożeń i luk w zabezpieczeniach teleinformatycznych.
	7. Ataki na urządzenia mobilne i bezprzewodowe.
	8. Konfiguracja i badanie WEP/WPA2 PSK/WPA2 RADIUS
	9. Badanie ruchu FTP pomiędzy klientem a witryną zdalną.
	10. Konfiguracja VPN (Transport Mode oraz Tunnel Mode)
	11. Odzyskiwanie haseł użytkownika przy pomocy narzędzi systemowych.
	12. Zdalny dostęp - badanie i analiza problemów bezpieczeństwa.
	13. Redundancja - przełączniki oraz routery.
	14. Badanie i konfiguracja zapory firewall.
	15. List kontroli dostępu ACL – zagadnienia cyberbezpieczeństwa.

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów uczenia się					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01			X			
W02			X			
W01			X			
U01			X			
U02			X			
U03			X			
K01			X			
K02			X			

FORMA I WARUNKI ZALICZENIA

Forma zajęć*	Forma zaliczenia	Warunki zaliczenia
wykład		Uzyskanie co najmniej 50% punktów z kolokwium kończącego zajęcia wykładowe.
laboratorium		Uzyskanie co najmniej 50% punktów z kolokwium w trakcie trwania zajęć laboratoryjnych.

*) zostawić tylko realizowane formy zajęć

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS							
Lp.	Rodzaj aktywności	Obciążenie studenta					Jednostka
		W	C	L	P	S	
1.	Udział w zajęciach zgodnie z planem studiów	15		30			h
3.	Inne (konsultacje, egzamin)*	2		2			h
4.	Razem przy bezpośrednim udziale nauczyciela akademickiego	49					h
5.	Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego	1,96					ECTS
6.	Liczba godzin samodzielnej pracy studenta	26					h
7.	Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy	1,04					ECTS
8.	Nakład pracy związany z zajęciami o charakterze praktycznym	30					h
9.	Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym	1,84					ECTS
10.	Sumaryczne godzinowe obciążenie pracą studenta	75					h
11.	Punkty ECTS za moduł <i>1 punkt ECTS=25 godzin obciążenia studenta</i>	3					ECTS

* wszelkie formy weryfikacji efektów, w tym egzaminy oraz nie więcej niż 2 godziny konsultacji dla każdej formy zajęć

LITERATURA

1. Materiały zawarte na platformie NetAcad udostępniane studentom podczas zajęć dydaktycznych.

Uwaga: wykaz literatury winien uwzględniać aktualne i dostępne publikacje