Załącznik nr 9
do Zarządzenia Rektora Nr 35/19
z dnia 12 czerwca 2019 r.

IV. Opis programu studiów

3. KARTA PRZEDMIOTU

Kod przedmiotu	**E-4IZ1T-08-s7**
Nazwa przedmiotu	**Cyberbezpieczeństwo**
Nazwa przedmiotu w języku angielskim	**Cybersecurity**
Obowiązuje od roku akademickiego	**2019/20**

USYTUOWANIE MODUŁU W SYSTEMIE STUDIÓW

Kierunek studiów	Informatyka
Poziom kształcenia	I stopień
Profil studiów	Ogólnoakademicki
Forma i tryb prowadzenia studiów	Studia niestacjonarne
Zakres	Teleinformatyka
Jednostka prowadząca przedmiot	Katedra Systemów Informatycznych
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	Przedmiot specjalnościowy
Status przedmiotu	Obowiązkowy
Język prowadzenia zajęć	Polski
Usytuowanie modułu w planie studiów - semestr	Semestr VI
Wymagania wstępne	**Sieci komputerowe, Podstawy routing i przełączania, Technologie IoT - Roz-proszone Sieci Sensoryczne**
Egzamin (TAK/NIE)	Nie
Liczba punktów ECTS	3

Forma prowadzenia zajęć	**wykład**	**ćwiczenia**	**laboratorium**	**projekt**	**Inne**
Liczba godzin w semestrze	**9**	**0**	**18**	**27**	**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 za kresu 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. Tworzenie cyberświata - wybrane techniki komunikacji.
	2. Ochrona danych w cyberświecie - badanie integralności danych. Praktyki szyfrowania danych.
	3. Budowa wirtualnej maszyny.
	4. Wykrywanie zagrożeń i luk w zabezpieczeniach teleinformatycznych. Badanie ruchu FTP pomiędzy klientem a witryną zdalną.
	5. Ataki na urządzenia mobilne i bezprzewodowe. Konfiguracja i badanie WEP/WPA2 PSK/WPA2 RADIUS
	6. Konfiguracja VPN (Transport Mode oraz Tunnel Mode)
	7. Odzyskiwanie haseł użytkownika przy pomocy narzędzi systemowych. Zdalny dostęp - badanie i analiza problemów bezpieczeństwa.
	8. Redundancja - przełączniki oraz routery. Badanie i konfiguracja zapory firewall.
	9. List kontroli dostępu ACL – zagadnienia cyberbezpieczeństwa.

projekt	W ramach zadań projektowych należy wykonać system zabezpieczeń dla rozwiązań z zakresu teleinformatyki. W celach projektowych. Projekt powinien zawierać: analizę literatury, analizę oraz wybór odpowiednich technologii, docelowy projekt systemu zabezpieczeń, dokumentację projektową, instrukcję. Zadanie kończy się prezentacją zespołową opracowanego rozwiązania.

*) zostawić tylko realizowane formy zajęć

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	X		
U02			X	X		
U03			X	X		
K01			X	X		
K02			X	X		

FORMA I WARUNKI ZALICZENIA

Forma zajęć*	Forma zaliczenia	Warunki zaliczenia
wykład	zaliczenie z ocena	*Uzyskanie co najmniej 50% punktów z kolokwiów kończącego zajęcia wykładowe.*
laboratorium	zaliczenie z ocena	*Uzyskanie co najmniej 50% punktów z kolokwiów w trakcie trwania zajęć laboratoryjnych.*
projekt	zaliczenie z ocena	*Uzyskanie oceny pozytywnej z przygotowanego projektu.*

*) zostawić tylko realizowane formy zajęć

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS								
Lp.	Rodzaj aktywności	Obciążenie studenta						Jednostka
1.	Udział w zajęciach zgodnie z planem studiów	W	C	L	P	S		h
		9		18	27			
3.	Inne (konsultacje, egzamin)*	2		2	2			h
4.	**Razem przy bezpośrednim udziale nauczyciela akademickiego**	**60**						h
5.	**Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego**	**2,4**						ECTS
6.	**Liczba godzin samodzielnej pracy studenta**	**15**						h
7.	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy**	**0,6**						ECTS
8.	**Nakład pracy związany z zajęciami o charakterze praktycznym**	**45**						h

9.	**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym**	**2,2**	ECTS
10.	**Sumaryczne godzinowe obciążenie pracą studenta**	**75**	h
11.	**Punkty ECTS za moduł** *1 punkt ECTS=25 godzin obciążenia studenta*	**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