Załącznik nr 9
do Zarządzenia Rektora PŚk Nr 35/19
w brzmieniu ustalonym Zarządzeniem Nr 12/22

KARTA PRZEDMIOTU

Kod przedmiotu	studia stacjonarne:	
	studia niestacjonarne:	
Nazwa przedmiotu	**Cyberbezpieczeństwo**	
Nazwa przedmiotu w języku angielskim	**Cybersecurity**	
Obowiązuje od roku akademickiego	**2022/23**	

USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

Kierunek studiów	**Informatyka**
Poziom kształcenia	**I stopień**
Profil studiów	**ogólnoakademicki**
Forma i tryb prowadzenia studiów	**studia stacjonarne i 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. Roman Deniziak, prof. PŚk**

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów		**przedmiot specjalnościowy**
Status przedmiotu		**obowiązkowy**
Język prowadzenia zajęć		**polski**
Usytuowanie w planie studiów - semestr	studia stacjonarne	**semestr VI**
	studia niestacjonarne	**semestr VII**
Wymagania wstępne		**Sieci komputerowe, Podstawy routingu i przełączania**
Egzamin (TAK/NIE)		**TAK**
Liczba punktów ECTS		**3**

Forma prowadzenia zajęć		**wykład**	**ćwiczenia**	**laboratorium**	**projekt**	**inne**
Liczba godzin w semestrze	studia stacjonarne:	**15**		**30**		
	studia niestacjonarne:	**9**		**18**		

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty uczenia się	Odniesienie do efektów kierunkowych
Wiedza	W01	Zna i rozumie współczesne problemy cyberbezpieczeństwa.	INF1_W32
	W02	Zna i rozumie rozwiązania pozwalającą zaprojektować / uruchomić usługi bezpieczeństwa w sieci teleinformatycznej.	INF1_W32
Umiejętności	U01	Potrafi dobrać odpowiedni poziom bezpieczeństwa w celu zapewnienia ochrony przed zagrożeniami.	INF1_U32
	U02	Potrafi zaprojektować / uruchomić / przetestować usługę bezpieczeństwa w sieci teleinformatycznej.	INF1_U32
	U03	Potrafi planować i przeprowadzać eksperymenty z zakresu ochrony zasobów dostępnych przez sieci teleinformatyczne.	INF1_U32
Kompetencje społeczne	K01	Jest gotów do oceny znaczenia cyberbezpieczeństwa w dzisiejszym świecie.	INF1_K01 INF1_K02
	K02	Jest gotów do pracy i współdziałania w grupie w zakresie obejmującym tworzenie zabezpieczeń w obszarze teleinformatyki.	INF1_K01 INF1_K02

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	1. **Wprowadzenie do zagadnień cyberbezpieczeństwa** (cyberprzestrzeń, cyberprzestępczość; rodzaje podatności). 2. **Zagrożenia, luki i ataki w cyberświecie** (oprogramowanie złośliwe i zaawansowane mechanizmy ochrony; ataki DoS, DDoS i sposoby reagowania na nie). 3. **Wybrane rodzaje ataków** (ataki dostępowe; ataki na infrastrukturę i usługi sieciowe; ataki na sieci bezprzewodowe). 4. **Systemy zapobiegające kradzieżom danych.** 5. **Chmury obliczeniowe** (podstawowe rozwiązania z zakresu cyberbezpieczeństwa funkcjonujące w chmurze obliczeniowej). 6. **Projektowanie systemów bezpieczeństwa** (zasady projektowania systemów zabezpieczeń i ich oceny; polityka bezpieczeństwa systemów informatycznych). 7. **Wybrane aspekty prawne w obszarze cyberbezpieczeństwa.**
laboratorium	1. Ochrona danych w cyberświecie - badanie integralności danych. 2. Bezpieczeństwo maszyn wirtualnych. 3. Wykrywanie zagrożeń i luk w zabezpieczeniach teleinformatycznych. 4. Ataki na urządzenia stacjonarne oraz mobilne. 5. Badanie ruchu pomiędzy klientem a witryną zdalną. 6. Podstawowa konfiguracja tunelu VPN. 7. Odzyskiwanie haseł użytkownika przy pomocy narzędzi systemowych. 8. Badanie i podstawowa konfiguracja zapory firewall. 9. List kontroli dostępu w zagadnieniach 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			
W03			X			
U01			X			
U02			X			
K01			X			
K02			X			

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	egzamin	Uzyskanie co najmniej 50% punktów z egzaminu.
laboratorium	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z kolokwiów.

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS

Lp.	Rodzaj aktywności	Obciążenie studenta										Jednostka
		studia stacjonarne					studia niestacjonarne					
		W	C	L	P	S	W	C	L	P	S	
1.	Udział w zajęciach zgodnie z planem studiów	**15**		**30**			**9**		**18**			h
2.	Inne (konsultacje, egzamin)	**4**		**2**			**4**		**2**			h
3.	**Razem przy bezpośrednim udziale nauczyciela akademickiego**	**51**					**33**					h
4.	**Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego**	**2,04**					**1,32**					ECTS
5.	**Liczba godzin samodzielnej pracy studenta**	**24**					**42**					h
6.	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy**	**0,96**					**1,68**					ECTS
7.	**Nakład pracy związany z zajęciami o charakterze praktycznym**	**30**					**18**					h
8.	**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym**	**1,20**					**0,72**					ECTS
9.	**Sumaryczne obciążenie pracą studenta**	**75**					**75**					h
10.	**Punkty ECTS za moduł** *1 punkt ECTS=25 godzin obciążenia studenta*	**3**										ECTS

LITERATURA

1. Charles J. Brooks, Donald Short, Christopher Grow, **Cybersecurity Essentials**, 2018
2. Materiały platformy NetACad udostępniane studentom podczas zajęć.