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

KARTA PRZEDMIOTU

Kod przedmiotu	studia stacjonarne:	E-I2C-2001-s1
	studia niestacjonarne:	E-1IZ2C-1002-s1
Nazwa przedmiotu	**Wprowadzenie do cyberbezpieczeństwa**	
Nazwa przedmiotu w języku angielskim	**Introduction to cybersecurity**	
Obowiązuje od roku akademickiego	**2022/23**	

USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

Kierunek studiów	**Informatyka**
Poziom kształcenia	**II stopień**
Profil studiów	**Ogólnoakademicki**
Forma i tryb prowadzenia studiów	**Studia stacjonarne i niestacjonarne**
Zakres	**Cyberbezpieczeństwo**
Jednostka prowadząca przedmiot	**Katedra Systemów Informatycznych**
Koordynator przedmiotu	**Dr inż. Mirosław Płaza, mgr inż. Marcin Kozłowski**
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 I**
	studia niestacjonarne	**Semestr I**
Wymagania wstępne		**brak**
Egzamin (TAK/NIE)		**TAK**
Liczba punktów ECTS		**5**

Forma prowadzenia zajęć		**wykład**	**ćwiczenia**	**laboratorium**	**projekt**	**inne**
Liczba godzin w semestrze	studia stacjonarne:	**30**		**15**	**20**	
	studia niestacjonarne:	**18**		**9**	**12**	

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W01	Student zna i rozumie zagrożenia związane z bezpieczeństwem wykorzystywania technologii internetowych	INF2_W03
	W02	Student zna i rozumie podstawowe technologie zabezpieczeń sieci teleinformatycznych.	INF2_W02, INF2_W03, INF2_W05, INF2_W06
	W03	Student zna i rozumie struktury zarządzania bezpieczeństwem sieci.	INF2_W02, INF2_W08
Umiejętności	U01	Student potrafi konfigurować podstawowe technologie zabezpieczeń sieci.	INF2_U03, INF2_U09, INF2_U11
	U02	Student potrafi przewidywać podstawowe ataki i odpowiednio im zapobiegać.	INF2_U01, INF2_U04, INF2_U05
	U03	Student potrafi weryfikować poziom zabezpieczenia sieci.	INF2_U01, INF2_U04, INF2_U05, INF2_U09, INF2_U11
Kompetencje społeczne	K01	Student jest gotów do poznawania zagrożeń bezpieczeństwa sieci oraz technik zabezpieczania sieci.	INF2_K03 INF2_K04
	K02	Student jest gotów do współdziałania w grupie w zakresie implementacji podstawowych technologii zabezpieczeń sieci.	INF2_K03 INF2_K04

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	1. **Podstawowe zagadnienia cyberbezpieczeństwa** (polityka bezpieczeństwa, modelowanie zagrożeń, zasada wiedzy koniecznej, dane audytowe, CIA (Confidentiality, Integrity, Availability), uwierzytelnianie, autoryzacja, zależności między bezpieczeństwem, niezawodnością, dostępnością, klasyfikacja złośliwego oprogramowania). 2. **Aspekty prawne (GDRP/RODO) i ekonomiczne oraz standardy bezpieczeństwa** obowiązujące w poszczególnych dziedzinach (m.in. medycyna, bankowość, lotnictwo). 3. **Zagrożenia związane z bezpieczeństwem sieci** (rodzaje zabezpieczeń i przeciwdziałanie zagrożeniom, bezpieczeństwo telefonii komórkowej i łączności Bluetooth, bezpieczeństwo w Data Center, bezpieczeństwo w telemetrii). 4. **Bezpieczeństwo urządzeń sieciowych** (zabezpieczanie dostępu do urządzeń, przypisywanie ról administracyjnych, monitorowanie i zarządzanie urządzeniami, korzystanie z automatycznych funkcji bezpieczeństwa). 5. **Bezpieczeństwo w sieci lokalnej** (bezpieczeństwo punktów końcowych sieci, zagrożenia bezpieczeństwa warstwy 2). 6. **Wybrane techniki stosowane w rozwiązaniach bezpieczeństwa** (AAA, firewall (listy kontroli dostępu, zapory sieciowe), IPS (technologia, sygnatury, implementacje), wirtualne sieci prywatnych (elementy i operacje IPsec VPN, impementacje sieci VPN), 7. **Systemy kryptograficzne** (usługi kryptograficzne, podstawowa integralność i autentyczność, poufność, klucze publiczne). 8. **Wyzwania w zakresie cyberbezpieczeństwa** oraz charakterystyka SOC (Security Operations Center).

laboratorium	1. Konfiguracja Syslog, NTP i SSH na routerach. 2. Konfiguracja uwierzytelniania AAA na routerach. 3. Konfiguracja rozszerzonych list ACL. 4. Konfiguracja IP ACL w celu zapobiegania atakom. 5. Konfiguracja IPv6 ACL. 6. Konfiguracja Zone-Based Policy Firewall (ZPF). 7. Konfiguracja IOS Intrusion Prevention System (IPS) za pomocą CLI. 8. Konfiguracja i weryfikacja IPsec VPN Site-to-Site przy użyciu CLI. 9. Elementy konfiguracji zapory sieciowej za pomocą CLI.
projekt	Tematyka zadań projektowych z zakresu Wprowadzenia do cyberbezpieczeństwa obejmuje następujące zagadnienia: analizę literatury w zakresie dotychczas stosowanych rozwiązań dotyczących zadanego problemu inżynierskiego; analizę oraz dobranie odpowiednich technik umożliwiających skuteczną realizację zadanego problemu wraz z uzasadnieniem dokonanych wyborów; projekt opracowywanego systemu/zadania wraz z opisem zastosowanych technik oraz narzędzi; przygotowanie dokumentacji projektowej, która w sposób szczegółowy opisuje wykonany projekt wraz z założeniami projektowymi – dokumentacja przygotowywana jest samodzielnie przez zespół realizujący projekt; opis sposobu implementacji opracowanego rozwiązania wraz z instrukcją obsługi; analizę dalszych możliwości rozwoju przygotowanego rozwiązania, polityka bezpieczeństwa, modelowanie zagrożeń i ekonomia przyjętych rozwiązań, prezentacja opracowanego rozwiązania.

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów kształcenia					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01			X			
W02			X			
W03			X			
U01			X	X		
U02			X	X		
U03			X	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.
projekt	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z wykonanego projektu.

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS												
Lp.	Rodzaj aktywności	Obciążenie studenta										Jednostka
		studia stacjonarne					studia niestacjonarne					
1.	Udział w zajęciach zgodnie z planem studiów	W	C	L	P	S	W	C	L	P	S	h
		30		**15**	**20**		**18**		**9**	**12**		
2.	Inne (konsultacje, egzamin)	**4**		**2**	**2**		**4**		**2**	**2**		h

3.	**Razem przy bezpośrednim udziale nauczyciela akademickiego**	**73**	**47**	h
4.	**Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego**	**2,92**	**1,88**	ECTS
5.	**Liczba godzin samodzielnej pracy studenta**	**52**	**78**	h
6.	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy**	**2,08**	**3,12**	ECTS
7.	**Nakład pracy związany z zajęciami o charakterze praktycznym**	**35**	**21**	h
8.	**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym**	**1,4**	**0,84**	ECTS
9.	**Sumaryczne obciążenie pracą studenta**	**125**	**125**	h
10.	**Punkty ECTS za moduł** *1 punkt ECTS=25 godzin obciążenia studenta*	**5**		ECTS

LITERATURA

1. Allan Johnson, Cisco Networking Academy, **CCNA Cybersecurity Operations Companion Guide**, 2018
2. Erdal Ozkaya, **Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity**, 2019
3. Liam Smith, **Cyber Security For Beginners:: A Comprehensive And Essential Guide For Every Novice To Understand And Master Cybersecurity**, 2022