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

KARTA PRZEDMIOTU

Kod przedmiotu	studia stacjonarne:	E-ID2C-09-s2, E-ID2C-09-s3
	studia niestacjonarne:	E-2IZ2C-1013-s3
Nazwa przedmiotu	**Detekcja i monitorowanie zagrożeń**	
Nazwa przedmiotu w języku angielskim	**Detection and monitoring of threats**	
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. Małgorzata 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		**Wybieralny**
Język prowadzenia zajęć		**Polski**
Usytuowanie w planie studiów - semestr	studia stacjonarne	**Semestr II lub Semestr III**
	studia niestacjonarne	**Semestr II lub Semestr III**
Wymagania wstępne		**brak**
Egzamin (TAK/NIE)		**NIE**
Liczba punktów ECTS		**3**

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

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W01	Student zna i rozumie cele monitorowania i detekcji zagrożeń w rozwiązaniach sieciowych.	INF2_W02
	W02	Student zna i rozumie metody prowadzenia monitorowania oraz detekcji zagrożeń sieciowych.	INF2_W02, INF2_W05, INF2_W08
	W03	Student zna i rozumie architektury bezpieczeństwa sieci teleinformatycznych.	INF2_W02, INF2_W05
Umiejętności	U01	Student potrafi konfigurować narzędzia wykorzystywane do monitorowania i detekcji zagrożeń.	INF2_U02, INF2_U09, INF2_U11
	U02	Student potrafi analizować pozyskane dane dzięki monitorowaniu ruchu w sieciach teleinformatycznych.	INF2_U03, INF2_U06, INF2_U08
	U03	Student potrafi odpowiednio reagować na wykryte zagrożenia.	INF2_U01, INF2_U05, INF2_U08
Kompetencje społeczne	K01	Student jest gotów do poznawania koncepcji monitorowania i detekcji zagrożeń sieciowych.	INF2_K03 INF2_K04
	K02	Student jest gotów do zaprezentowania i omówienia w zrozumiały sposób opracowanej koncepcji oraz pracy w zespole w celu wspólnego rozwiązania postawionego zadania.	INF2_K03 INF2_K04

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	1. **Wprowadzenie do zagadnień monitorowania i wykrywania zagrożeń w sieciach teleinformatycznych** (rodzaje zagrożeń, ocena i analiza ryzyka). 2. **Organizacja i rola SOC** (ang. *Security Operations Center*). Podstawowe architektury implementowane w zakresie rozwiązań cyberbezpieczeństwa. 3. **Analiza ruchu** (wybrane narzędzia wykorzystywane w analizie i monitorowaniu ruchu sieciowego, zagadnienia IDS (Intrusion Detection System(s), SIEM (Security Information and Event Management) 4. **Incydenty w sieciach teleinformatycznych** (detekcja i sposoby reagowania na incydenty). 5. **Elementy automatyzacji zabezpieczeń sieciowych i bezpieczeństwo urządzeń końcowych sieci**. 6. **Trendy oraz perspektywy rozwoju** zagadnień związanych z detekcją i monitorowania zagrożeń w sieciach teleinformatycznych.
laboratorium	1. Metody identyfikacji ruchu sieciowego. 2. Narzędzia systemowe wykorzystywane do monitorowania ruchu sieciowego w popularnych systemach operacyjnych. 3. Identyfikacja problemów związanych z wydajnością sieci. 4. Monitorowania i wykrywania zagrożeń w ruchu FTP. 5. Wykorzystanie syslog do przechwytywania plików dziennika z urządzeń sieciowych oraz obserwacja dostępu użytkowników.

projekt	Tematyka zadań projektowych z zakresu Detekcji i monitorowania zagrożeń 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, 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	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z kolokwiów.
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**	**15**		**18**		**9**	**9**		
2.	Inne (konsultacje, egzamin)	**2**		**2**	**2**		**2**		**2**	**2**		h
3.	**Razem przy bezpośrednim udziale nauczyciela akademickiego**	**66**					**42**					h
4.	**Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego**	**2,64**					**1,68**					ECTS
5.	**Liczba godzin samodzielnej pracy studenta**	**9**					**33**					h

6.	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy**	**0,36**	**1,32**	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**	**1,2**	**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

- Richard Bejtlich, The Practice of Network Security Monitoring: Understanding Incident Detection and Response", No Starch Press, 2013
- Chris Sanders, Applied Network Security Monitoring: Collection, Detection, and Analysis, Syngress 2012