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	**Zaawansowane zagadnienia cyberbezpieczeństwa**	
Nazwa przedmiotu w języku angielskim	**Advanced cybersecurity solutions**	
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		**wybieralny**
Język prowadzenia zajęć		**polski**
Usytuowanie w planie studiów - semestr	studia stacjonarne	**semestr VII**
	studia niestacjonarne	**semestr VIII**
Wymagania wstępne		**Sieci komputerowe, Podstawy routingu i przełączania, Cyberbezpieczeństwo**
Egzamin (TAK/NIE)		**NIE**
Liczba punktów ECTS		**6**

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

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty uczenia się	Odniesienie do efektów kierunkowych
Wiedza	W01	Student zna i rozumie zaawansowane metody monitorowania bezpieczeństwa w systemach teleinformatycznych.	INF1_W32
	W02	Student zna i rozumie metody zwiększania bezpieczeństwa w zdefiniowanych cyberprzestrzeniach.	INF1_W32
	W03	Student zna i rozumie słabe punkty systemów teleinformatycznych.	INF1_W32
Umiejętności	U01	Student potrafi projektować złożone systemy teleinformatyczne z uwzględnieniem zapewnienia ochrony przed zagrożeniami.	INF1_U32
	U02	Student potrafi rozwiązywać skomplikowane problemy cyberbezpieczeństwa.	INF1_U32
	U03	Student potrafi określić zapotrzebowania na wykorzystanie technik cyberbezpieczeństwa.	INF1_U32
Kompetencje społeczne	K01	Student jest gotów do stałego uzupełniania wiedzy z obszaru cyberbezpieczeństwa.	INF1_K01 INF1_K02
	K02	Student jest gotów do oceny problemów związanych z cyberbezpieczeństwem i ich skutków dla społeczeństwa.	INF1_K01 INF1_K02

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	1. **Zagadnienia cyberbezpieczeństwa w rozwiązaniach IoT** (ocena podatności i ryzyka w systemach IoT, problemy bezpieczeństwa IoT w warstwach: device layer, communication layer oraz application layer). 2. **Zaawansowane kwestie bezpieczeństwa w systemach operacyjnych** (Windows, Linux) 3. **Sieciowe systemy bezpieczeństwa** (wdrożone na hoście, w infrastrukturze sieci teleinformatycznej lub chmurze na przykładzie rozwiązań klasy: Firewall, IPS, AMP). 4. **Zaawansowane metody ograniczania wpływu szkodliwego oprogramowania** (monitorowanie bezpieczeństwa, analiza danych wykorzystywanych w systemach monitorowania bezpieczeństwa, incydenty bezpieczeństwa). 5. Wpływ algorytmów szyfrowania i bezpiecznych protokołów komunikacyjnych oraz funkcji haszujących na bezpieczeństwo. 6. **Zaawansowane rozwiązania bezpieczeństwa dla infrastruktury chmur obliczeniowych** (bezpieczeństwo infrastruktury, bezpieczeństwo aplikacji, bezpieczne zarządzanie chmurą)
laboratorium	1. Ceberbezpieczeństwo IoT - badanie i analiza podatności aplikacji i urządzeń IoT. 2. Zaawansowane kwestie bezpieczeństwa w systemie operacyjnym Windows. 3. Zaawansowane kwestie bezpieczeństwa w systemie operacyjnym Linux. 4. Badanie zaawansowanych funkcji analizatorów sieciowych w ocenie podatności różnych protokołów sieciowych. 5. Badania możliwości ataków na wybrane typy bazy danych. 6. Szyfrowanie i deszyfrowanie danych przy użyciu wybranych metod. 7. Zaawansowane procedury obsługi incydentów związanych z bezpieczeństwem. 8. Zaawansowane techniki cyberbezpieczeństwa w obszarze chmury obliczeniowej.

projekt	Tematyka zadań projektowych obejmuje: • analizę literatury w zakresie dotychczas stosowanych rozwiązań dotyczących zadanego problemu inżynierskiego, • analiza 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 • analiza dalszych możliwości rozwoju przygotowanego rozwiązania, • prezentacja opracowanego rozwiązania.

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			
U03			X			
K01			X			
K02			X			

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	egzamin	Uzyskanie co najmniej 50% punktów z kolokwiów.
laboratorium	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z kolokwiów.
projekt	zaliczenie z oceną	Obrona przygotowanych projektów

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		**30**	**15**		**18**		**18**	**9**		
2.	Inne (konsultacje, egzamin)	**2**		**2**	**2**		**2**		**2**	**2**		h
3.	**Razem przy bezpośrednim udziale nauczyciela akademickiego**	**81**					**51**					h
4.	**Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego**	**3,24**					**2,04**					ECTS
5.	**Liczba godzin samodzielnej pracy studenta**	**69**					**99**					h
6.	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy**	**2,76**					**3,96**					ECTS
7.	**Nakład pracy związany z zajęciami o charakterze praktycznym**	**45**					**27**					h
8.	**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym**	**1,80**					**1,08**					ECTS
9.	**Sumaryczne obciążenie pracą studenta**	**150**					**150**					h
10.	**Punkty ECTS za moduł** *1 punkt ECTS=25 godzin obciążenia studenta*	**6**										ECTS

LITERATURA

1. Omar Santos, **Cisco CyberOps Associate Official Cert Guide**, 2020
2. Cisco Networking Academy, **CCNA Cybersecurity Operations Companion Guide**, 2018
3. Materiały platformy NetACad udostępniane studentom podczas zajęć.