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-01-s2, E-ID2C-01-s3
	studia niestacjonarne:	E-2IZ2C-1005-s3
Nazwa przedmiotu	**Bezpieczeństwo aplikacji internetowych**	
Nazwa przedmiotu w języku angielskim	**Security of internet applications**	
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. Karol Wieczorek, mgr inż. Mateusz Pawełkiewicz**
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		**Wprowadzenie do cyberbezpieczeństwa**
Egzamin (TAK/NIE)		**NIE**
Liczba punktów ECTS		**3**

Forma prowadzenia zajęć		**wykład**	**ćwiczenia**	**laborato-rium**	**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 zagrożenia związane z podatnością aplikacji internetowych na ataki oraz zasady projektowania ich w sposób bezpieczny.	INF2_W02, INF2_W03
Umiejętności	U01	Student potrafi analizować aplikacje webowe pod kątem podatności na typowe ataki.	INF2_U01, INF2_U02, INF2_U05, INF2_U07, INF2_U09, INF2_U10, INF2_U11
Kompetencje społeczne	K01	Student umie pracować w zespole i rozwiązywać problemy projektowe.	INF2_K02

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	1. **Wprowadzenie do podstawowych podatności aplikacji internetowych na ataki** (Sql Injection, Session Hijack, XSS, CSRF, XSRF). 2. **Zasady projektowania bezpiecznych aplikacji internetowych - front end** (aplikacje client-side, server-side, JWT, OAuth2 - komunikacja z systemami zewnętrznymi, zabezpieczenia komunikacji REST). 3. **Zasady projektowania bezpiecznych aplikacji internetowych - backend** (uwierzytelnianie i autoryzacja użytkowników, utrzymywanie sesji HTTP, szyfrowanie, OAuth2 - komunikacja z zewnętrznymi systemami). 4. **Zabezpieczenia architektur rozproszonych** (bezpieczeństwo systemów opartych na mikroserwisach, uwierzytelnianie żądań, Circuit Breakers).
laboratorium	1. Metody ataku na aplikacje internetowe 2. Wyszukiwanie i eliminowanie podatności na ataki wybranego systemu internetowego
projekt	Zadanie projektowe polegające na przygotowaniu aplikacji internetowej wraz z zestawem testów penetracyjnych

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów kształcenia					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01			X			
U01					X	X
K01				X	X	

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z kolokwium zaliczeniowego.
laboratorium	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów za wykonane zadania laboratoryjne
projekt	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów za wykonane zadanie projektowe oraz sprawozdanie.

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

1. M. Bentkowski, A. Czyż i inni, „Bezpieczeństwo aplikacji webowych”
2. Źródła internetowe