Politechnika Świętokrzyska

WYDZIAŁ ELEKTROTECHNIKI, AUTOMATYKI I INFORMATYKI

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-2003-s1
	studia niestacjonarne:	E-1IZ2C-1004-s1
Nazwa przedmiotu	**Programowanie defensywne**	
Nazwa przedmiotu w języku angielskim	**Defensive Programming**	
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. Arkadiusz Chrobot**
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 uczenia się	Odniesienie do efektów kierunkowych
Wiedza	W01	Student zna i rozumie w stopniu rozszerzonym zagrożenie jakim dla bezpieczeństwa są defekty w oprogramowaniu.	INF2_W02
	W02	Student zna i rozumie standardy i praktyki wykrywania, naprawiania i unikania defektów powodujących powstanie podatności w oprogramowaniu.	INF2_W03
	W03	Student zna i rozumie standardy tworzenia bezpiecznego oprogramowania.	INF2_W03
	W04	Student zna i rozumie zasady tworzenia modelu zagrożeń dla oprogramowania.	INF2_W02
Umiejętności	U01	Student potrafi opracować model zagrożeń dla oprogramowania.	INF2_U01, INF2_U05, INF2_U06
	U02	Student potrafi zastosować zasady tworzenia bezpiecznego kodu w procesie tworzenia oprogramowania.	INF2_U02, INF2_U09, INF2_U10, INF2_U11
Kompetencje społeczne	K01	Student jest gotów ciągle aktualizować swoją wiedzę i poszerzać umiejętności tworzenia bezpiecznego oprogramowania.	INF2_K03, INF2_K04

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	1. **Defekty w oprogramowaniu związane z bezpieczeństwem** (przegląd najczęściej spotykanych podatności, model zagrożeń dla oprogramowania). 2. **Wykrywanie podatności** (przegląd kodu, narzędzia analizy statycznej, testy jednostkowe). 3. **Usuwanie podatności i zapobieganie im** (programowanie defensywne i ofensywne, standardy i zasady tworzenia bezpiecznego oprogramowania)
laboratorium	1. **Tworzenie modelu zagrożeń dla aplikacji** (określanie i ocena ryzyk). 2. **Badanie podatności** (sprawdzanie konsekwencji istnienia podatności w kodzie programu). 3. **Wykrywanie i usuwanie podatności** (metody i narzędzia odnajdywania i naprawiania defektów bezpieczeństwa). **4.** **Techniki bezpiecznego tworzenia oprogramowania** (programowanie defensywne i ofensywne, standardy tworzenia bezpiecznego oprogramowania).
projekt	W ramach projektu studenci pracują w zespołach co najwyżej trzyosobowych. Pojedyncze zadanie projektowe składa się z dwóch części. W pierwszej studenci tworzą zgodnie ze standardami i praktykami zabezpieczeń oprogramowanie realizujące zadane usługi. W drugiej współpracują z innym, przydzielonym im zespołem, szukając w opracowanym przez niego kodzie aplikacji podatności, jednocześnie analizując i naprawiając defekty znalezione w swoim oprogramowaniu przez ten inny zespół. Technologia i języki programowania użyte do realizacji zadania mogą być dowolne, ale muszą być uzgodnione z innymi zespołami, aby możliwa była opisana wcześniej współpraca.

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów uczenia się					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01		X		X		X
W02		X		X		X
W03		X		X		X
W04		X		X		X
U01				X		X
U02				X		X
K01				X		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 za realizację zadań laboratoryjnych.
projekt	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów za wykonany projekt.

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	**0**	**15**	**20**	**0**	**18**	**0**	**9**	**12**	**0**	
2.	Inne (konsultacje, egzamin)	**2**	**0**	**0**	**0**	**0**	**2**	**0**	**0**	**0**	**0**	h
3.	**Razem przy bezpośrednim udziale nauczyciela akademickiego**	67					41					h
4.	**Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego**	2,68					1,64					ECTS
5.	**Liczba godzin samodzielnej pracy studenta**	58					84					h
6.	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy**	2,32					3,36					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**	1,40					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. „SEI CERT Coding Standards”, https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards (dostęp: 2022-09-15).
2. David A. Wheeler, „Secure Programming HOWTO”, 2015 (https://dwheeler.com/secure-programs/Secure-Programs-HOWTO.pdf dostęp:2022-09-15).