Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2023/2024

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma sudiów: niestacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Cyberbezpieczeństwo

1 Informacje o przedmiocie

Nazwa przedmiotu	Bezpieczeństwo systemów informatycznych
Nazwa przedmiotu w języku angielskim	Computer systems security
Kod przedmiotu	WIiT I oIIN D5 23/24
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	3.00
Semestry	2

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
2	9	0	0	9	0	9

3 Cele przedmiotu

Cel 1 Poznanie zagadnień związanych z bezpieczeństwem systemów komputerowych

Cel 2 Opanowanie umiejętności projektowania i tworzenia bezpiecznych systemów

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 Znajomość i umiejętność obsługi systemów operacyjnych

2 Znajomość podstaw sieci komputerowych

3 Znajomość języka angielskiego w stopniu umożliwiającym studiowanie literatury i uczestnictwo w zajęciach

5 Efekty kształcenia

EK1 Umiejętności Student potrafi skonfigurować bezpieczny system operacyjny

EK2 Umiejętności Student potrafi tworzyć bezpieczne aplikacje

EK3 Wiedza Student zna techniki ataków

EK4 Wiedza Student zna metody obrony przed atakami

6 Treści programowe

Projekt		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
P1	Wprowadzenie	1
P2	Realizacja projektu związanego z bezpieczeństwem	8

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Wprowadzenie do bezpieczeństwa systemów komputerowych	1
W2	Kryptografia	2
W3	Bezpieczeństwo aplikacji	2
W4	Bezpieczeństwo systemów operacyjnych	1
W5	Bezpieczeństwo baz danych	1
W6	Bezpieczeństwo chmur i IoT	1
W7	Bezpieczeństwo urządzeń mobilnych	1

Laboratorium komputerowe		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
K1	Techniki ataków na aplikacje	4
K2	Łamanie haseł w systemach operacyjnych	2
K3	Testy penetracyjne	1
K4	IDS/IPS	2

7 Narzędzia dydaktyczne

N1 Wykłady (w przypadku realizacji zajęć w trybie zdalnym z wykorzystaniem stosownych narzędzi teleinformatycznych)

N2 Ćwiczenia laboratoryjne (w przypadku realizacji zajęć w trybie zdalnym z wykorzystaniem stosownych narzędzi teleinformatycznych)

N3 Dyskusja

N4 Konsultacje

N5 MS Teams

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	27
Konsultacje przedmiotowe	15
Egzaminy i zaliczenia w sesji	0
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	16
Opracowanie wyników	16
Przygotowanie raportu, projektu, prezentacji, dyskusji	16
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**90**
Sumaryczna liczba punktów ECTS dla przedmiotu	3.00

9 Sposoby oceny

Ocena formująca

F1 Sprawozdanie z ćwiczenia laboratoryjnego

F2 Test

F3 Projekt zespołowy

Ocena podsumowująca

P1 Średnia ważona ocen formujących

P2 Zaliczenie pisemne

Warunki zaliczenia przedmiotu

W1 Zaliczenie wszystkich ćwiczeń laboratoryjnych

W2 Pozytywna ocena z projektu

W3 Spełnienie warunku obecności na zajęciach

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Student nie spełnia warunków określonych dla oceny 3.0.
Na ocenę 3.0	Uzyskanie co najmniej 51% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Na ocenę 3.5	Uzyskanie co najmniej 61% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Na ocenę 4.0	Uzyskanie co najmniej 71% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Na ocenę 4.5	Uzyskanie co najmniej 81% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Na ocenę 5.0	Uzyskanie co najmniej 91% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie spełnia warunków określonych dla oceny 3.0.
Na ocenę 3.0	Uzyskanie co najmniej 51% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Na ocenę 3.5	Uzyskanie co najmniej 61% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Na ocenę 4.0	Uzyskanie co najmniej 71% punktów w ramach sposobów weryfikacji nabytych kompetencji.

Na ocenę 4.5	Uzyskanie co najmniej 81% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Na ocenę 5.0	. Uzyskanie co najmniej 91% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Efekt kształcenia 3	
Na ocenę 2.0	Student nie spełnia warunków określonych dla oceny 3.0.
Na ocenę 3.0	Uzyskanie co najmniej 51% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Na ocenę 3.5	Uzyskanie co najmniej 61% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Na ocenę 4.0	Uzyskanie co najmniej 71% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Na ocenę 4.5	Uzyskanie co najmniej 81% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Na ocenę 5.0	Uzyskanie co najmniej 91% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Efekt kształcenia 4	
Na ocenę 2.0	Student nie spełnia warunków określonych dla oceny 3.0.
Na ocenę 3.0	Uzyskanie co najmniej 51% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Na ocenę 3.5	Uzyskanie co najmniej 61% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Na ocenę 4.0	Uzyskanie co najmniej 71% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Na ocenę 4.5	Uzyskanie co najmniej 81% punktów w ramach sposobów weryfikacji nabytych kompetencji.
Na ocenę 5.0	Uzyskanie co najmniej 91% punktów w ramach sposobów weryfikacji nabytych kompetencji.

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1	I2_W08 I2_U07 I2_U09 I2_U12	Cel 1	P1 P2 W1 W2	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK2	I2_W08 I2_U07 I2_U09 I2_U12	Cel 2	W3 W4	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK3	I2_W01	Cel 1 Cel 2	P1 P2 W5 W6	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK4	I2_W02	Cel 2	P1 P2 W4 W5 W6 W7	N1 N2 N3 N4	F1 F2 F3 P1 P2

11 Wykaz literatury

Literatura podstawowa

[1] William Stallings, Lawrie Brown — *Bezpieczeństwo systemów informatycznych. Zasady i praktyka.*, , 2019, Helion

[2] Tajinder Kalsi — *Bezpieczeństwo systemu Linux w praktyce. Receptury.*, , 2019, Helion

[3] Prakhar Prasad — *Testy penetracyjne nowoczesnych serwisów. Kompendium inżynierów bezpieczeństwa*, , 2017, Helion

[4] — *Źródła internetowe (np. Sekurak, Hacking, OWASP)*, , 2019,

Literatura uzupełniająca

[1] Prashant Verma, Akshay Dixit — *Bezpieczeństwo urządzeń mobilnych. Receptury*, , 2017, Helion

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr Agnieszka Jakóbik (kontakt: agnieszka.jakobik@pk.edu.pl)

Osoby prowadzące przedmiot

2 dr inż. Dariusz Żelasko (kontakt: dariusz.zelasko@pk.edu.pl)

13 Zatwierdzenie karty przedmiotu do realizacji

(miejscowość, data) (odpowiedzialny za przedmiot) (dziekan)

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

.....