Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2021/2022

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka | Profil: Ogólnoakademicki

Forma sudiów: stacjonarne | 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 oIIS D5 21/22
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	4.00
Semestry	1

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
1	15	0	15	0	0	15

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

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

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	4
W5	Bezpieczeństwo baz danych	2
W6	Bezpieczeństwo chmur i IoT	2
W7	Bezpieczeństwo urządzeń mobilnych	2

Laboratorium		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
L1	Wprowadzenie	1
L2	Techniki ataków na aplikacje	6
L3	Łamanie haseł w systemach operacyjnych	2
L4	Testy penetracyjne	2
L5	IDS/IPS	4

Projekt		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
P1	Wprowadzenie	1
P2	Realizacja projektu związanego z bezpieczeństwem	14

7 Narzędzia dydaktyczne

N1 Wykłady

N2 Ćwiczenia laboratoryjne

N3 Dyskusja

N4 Konsultacje

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	45
Konsultacje przedmiotowe	31
Egzaminy i zaliczenia w sesji	4
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	20
Opracowanie wyników	10
Przygotowanie raportu, projektu, prezentacji, dyskusji	10
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**120**
Sumaryczna liczba punktów ECTS dla przedmiotu	4.00

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 Regularnie uczęszczanie na zajęcia laboratoryjne

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Student nie potrafi przeprowadzić konfiguracji.
Na ocenę 3.0	Student potrafi wykonać częściową konfiguracje, często popełniając błędy.
Na ocenę 3.5	Student potrafi konfigurować podstawowe usługi, błędy popełnia rzadko.
Na ocenę 4.0	Student potrafi konfigurować zaawansowane metody bezpieczeństwa, ma odpowiednia wiedzę, zaawansowana konfiguracja nie zawsze działa poprawnie.
Na ocenę 4.5	Student radzi sobie z konfiguracją zaawansowanych metod bezpieczeństwa, ma szeroki zakres wiedzy pozwalający mu zrozumieć konfigurowane metody.
Na ocenę 5.0	Student radzi sobie z konfiguracją każdej podstawowej i zaawansowanej funkcji bezpieczeństwa.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie zna pojęcia bezpiecznej aplikacji
Na ocenę 3.0	Student potrafi wykazać podstawowe problemy związane z bezpieczeństwem aplikacji
Na ocenę 3.5	Student potrafi w podstawowy sposób zabezpieczyć aplikacje. Zabezpieczenia rzadko działają poprawnie.
Na ocenę 4.0	Student potrafi w podstawowy sposób zabezpieczyć aplikacje. Zabezpieczenia działają w większości przypadków.
Na ocenę 4.5	Student potrafi w zaawansowany sposób zabezpieczyć aplikacje. Czasem pojawiają się błędy.
Na ocenę 5.0	Student potrafi w zaawansowany sposób zabezpieczyć aplikacje, nie popełnia błędów, posiada szeroką wiedze w tematyce bezpieczeństwa
Efekt kształcenia 3	
Na ocenę 2.0	Student nie potrafi wymienić podstawowych technik ataków
Na ocenę 3.0	Student potrafi opisać podstawowe techniki ataków

Na ocenę 3.5	Student potrafi szczegółowo opisać techniki ataków, nie potrafi ich zastosować
Na ocenę 4.0	Student potrafi przeprowadzać podstawowe ataki
Na ocenę 4.5	Student potrafi przeprowadzać zaawansowane ataki
Na ocenę 5.0	Student posiada szeroką wiedzę w zakresie bezpieczeństwa, zna na wysokim poziomie techniki ataków, umie je stosować
Efekt kształcenia 4	
Na ocenę 2.0	Student nie zna metod obrony przed podstawowymi atakami
Na ocenę 3.0	Student umie opisać metody obrony przed podstawowymi atakami
Na ocenę 3.5	Student umie opisać metody obrony przed zaawansowanymi atakami
Na ocenę 4.0	Student potrafi skonfigurować podstawowe mechanizmy obrony
Na ocenę 4.5	Student potrafi skonfigurować zaawansowane mechanizmy obrony
Na ocenę 5.0	Student posiada szeroką wiedzę w zakresie ochrony, zna na wysokim poziomie techniki obrony przed atakami, umie je stosować

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	Cel 1	W1 W2 L1 L2 P1 P2	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK2	I2_W08	Cel 2	W3 W4 L3 L4	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK3	I2_W01	Cel 1 Cel 2	W5 W6 L4 L5 P1 P2	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK4	I2_W02	Cel 2	W4 W5 W6 W7 L3 L4 P1 P2	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

1 mgr inż. Dariusz Żelasko (kontakt: dzelasko@pk.edu.pl)

13 Zatwierdzenie karty przedmiotu do realizacji

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

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .