

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 studiów: stacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Teleinformatyka

1 INFORMACJE O PRZEDMIOCIE

NAZWA PRZEDMIOTU	Bezpieczeństwo aplikacyjne i systemowe
NAZWA PRZEDMIOTU W JĘZYKU ANGIELSKIM	Application and system security
KOD PRZEDMIOTU	WiT I oIIS D12 21/22
KATEGORIA PRZEDMIOTU	Przedmioty specjalnościowe
LICZBA PUNKTÓW ECTS	2.00
SEMESTRY	3

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁAD	ĆWICZENIA	LABORATORIUM	LABORATORIUM KOMPUTERO- WE	SEMINARIUM	PROJEKT
3	30	0	0	0	0	15

3 CELE PRZEDMIOTU

Cel 1 Poznanie zagadnień związanych z bezpieczeństwem systemów komputerowych

Cel 2 Opanowanie umiejętności projektowania i tworzenia bezpiecznych systemów oraz aplikacji

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

PROJEKT		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
P1	Projekt związany z bezpieczeństwem systemu operacyjnego	7
P2	Projekt związany z bezpieczeństwem aplikacji	7
P3	Podsumowanie projektów	1

WYKŁAD		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W1	Wprowadzenie do bezpieczeństwa systemów komputerowych	2
W2	Kryptografia	2
W3	Hasła i funkcje skrótu	2
W4	Bezpieczeństwo aplikacji	6
W5	Bezpieczeństwo systemów operacyjnych	6
W6	Bezpieczeństwo baz danych	4
W7	Bezpieczeństwo chmur i IoT	4
W8	Bezpieczeństwo urządzeń mobilnych	4

7 NARZĘDZIA DYDAKTYCZNE

N1 Wykłady

N2 Ćwiczenia projektowe

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	5
Egzaminy i zaliczenia w sesji	5
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	5
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	0
SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA	60
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	2.00

9 SPOSOBY OCENY

OCENA FORMUJĄCA

F1 Projekt zespołowy

F2 Test

OCENA PODSUMOWUJĄCA

P1 Projekt

P2 Egzamin pisemny

P3 Średnia ważona ocen formujących

WARUNKI ZALICZENIA PRZEDMIOTU
W1 Zaliczenie projektu

W2 Regularne uczęszczanie na zajęcia

W3 Pozytywne zdanie egzaminu

KRYTERIA OCENY

EFEKT KSZTAŁCENIA 1	
NA OCENĘ 2.0	Student nie potrafi przeprowadzić konfiguracji.
NA OCENĘ 3.0	Student potrafi wykonać częściową konfigurację, 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 odpowiednią 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 szeroka wiedzę 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 szeroka wiedze 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 szeroka wiedze w zakresie ochrony, zna na wysokim poziomie techniki obrony przed atakami, umie je stosować.

10 MACIERZ REALIZACJI PRZEDMIOTU

EFEKT KSZTAŁCENIA	ODNIESIENIE DANEGO EFEKTU DO SZCZEGÓLOWYCH EFEKTÓW ZDEFINIOWANYCH DLA PROGRAMU	CELE PRZEDMIOTU	TREŚCI PROGRAMOWE	NARZĘDZIA DYDAKTYCZNE	SPOSOBY OCENY
EK1	I2_W02 I2_W06 I2_U06	Cel 1	P2 P3 W1 W2 W3 W4	N1 N2 N3 N4	F1 F2 P1 P2 P3
EK2	I2_W06 I2_U06	Cel 2	P2 W1 W5 W6 W7 W8	N1 N2 N3 N4	F1 F2 P1 P2 P3
EK3	I2_W02 I2_W03 I2_W05	Cel 1 Cel 2	P1 P2 W4 W5 W6 W7 W8	N1 N2 N3 N4	F1 F2 P1 P2 P3
EK4	I2_W02 I2_W06 I2_U11	Cel 2	P1 P2 P3 W4 W5 W6 W7 W8	N1 N2 N3 N4	F1 F2 P1 P2 P3

11 WYKAZ LITERATURY

LITERATURA PODSTAWOWA

- [1] | **William Stallings, Lawrie Brown** — *Bezpieczeństwo systemów informatycznych. Zasady i praktyka*, Gliwice, 2019, Helion
- [2] | **Tajinder Kalsi** — *Bezpieczeństwo systemu Linux w praktyce. Receptury*, Gliwice, 2019, Helion

- [3] **Prakhar Prasad** — *Testy penetracyjne nowoczesnych serwisów. Kompendium inżynierów bezpieczeństwa*, Gliwice, 2017, Helion
- [4] — *Źródła internetowe (np. Sekurak, Hacking, OWASP)*, , 2020,

LITERATURA UZUPEŁNIAJĄCA

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

12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

OSOBA ODPOWIEDZIALNA ZA KARTĘ

dr inż. Daniel Grzonka (kontakt: daniel.grzonka@pk.edu.pl)

OSOBY PROWADZĄCE PRZEDMIOT

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

13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejsowość, data)

(odpowiedzialny za przedmiot)

(dziekan)

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....