

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2022/2023

Wydział Inżynierii Elektrycznej i Komputerowej

Kierunek studiów: Infotronika

Profil: Ogólnoakademicki

Forma studiów: stacjonarne

Kod kierunku: It-E-3

Stopień studiów: II

Specjalności: bez specjalności

1 INFORMACJE O PRZEDMIOCIE

NAZWA PRZEDMIOTU	Informatyczne systemy tolerujące uszkodzenia
NAZWA PRZEDMIOTU W JĘZYKU ANGIELSKIM	
KOD PRZEDMIOTU	WIEiK INFOTRON oIIS PW3 22/23
KATEGORIA PRZEDMIOTU	Przedmioty wybieralne
LICZBA PUNKTÓW ECTS	3.00
SEMESTRY	3

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁADY	ĆWICZENIA	LABORATORIA	LABORATORIA KOMPUTERO- WE	PROJEKTY	
3	15	0	0	15	10	0

3 CELE PRZEDMIOTU

Cel 1 Przedstawienie modeli i wymiarów wiarygodności. Zapoznanie z zagrożeniami systemów informatycznych i cechy systemów FT. Poznanie technik tolerowania uszkodzeń (FT). Systemy krytyczne.

Cel 2 Zapoznanie z technikami i zasadami bezpieczeństwa: komputerowego i oprogramowania i systemów.

Cel 3 Poznanie problemów zarządzania (w tym: zarządzanie bezpieczeństwem IT, oceny ryzyka, środki/plany/procedury, zasoby ludzkie, audyt bezpieczeństwa, aspekty prawne i etyczne)i algorytmów kryptograficznych

4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

- 1 Znajomość organizacji systemów komputerowych (architektury, systemów operacyjnych i baz danych). Znajomość zagadnień Internetu rzeczy, chmur obliczeniowych i systemów wbudowanych.
- 2 Umiejętność programowania w językach niskopoziomym i obiektowym.
- 3 Podstawowa wiedza z inżynierii oprogramowania i inżynierii elektrycznej.

5 EFEKTY KSZTAŁCENIA

EK1 Kompetencje społeczne Student potrafi pracować indywidualnie i w zespole projektowym, umie oszacować czas potrzebny na realizację zleconego zadania.

EK2 Umiejętności Student potrafi wykorzystać w praktyce systemy tolerujące uszkodzenia. Potrafi również samodzielnie zaprojektować i zaimplementować aplikację z asercjami i wyjątkami.

EK3 Wiedza Student zna problemy tolerowania uszkodzeń w systemach: operacyjnych i systemach zarządzania bazami danych.

EK4 Wiedza Student ma wiedzę w zakresie technik i zasad bezpieczeństwa komputerowego.

6 TREŚCI PROGRAMOWE

PROJEKTY		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
P1	Projekt i implementacja aplikacji tolerującej uszkodzenia z wykorzystaniem zasad bezpieczeństwa systemów komputerowych.	2
P2	Implementacje algorytmów FT w programowaniu aplikacji numerycznych, morfologicznych i semantycznych. Również wykorzystanie algorytmów FT w działaniu systemów operacyjnych i systemów baz danych.	4
P3	Modelowanie systemów FT za pomocą BPMN i CMNN.	4

WYKŁADY		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W1	Przedstawienie koncepcji bezpieczeństwa komputerowego. Zagrożenia, ataki i aktywa. Funkcjonalne wymagania bezpieczeństwa. Podstawowe zasady projektowania bezpieczeństwa. Techniki i zasady bezpieczeństwa.	3

WYKŁADY		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W2	System infotroniczny/mechatroniczny jako złożony system informatyczny. Redundacje sprzętowe i programowe dla zapewnienia odporności na uszkodzenia takich systemów. Zagrożenia systemów w kontekście poufności, integralności i dostępności informacji, ogólna analiza zagrożeń i ryzyka, przykładowe uszkodzenia. Modele wiarygodności systemów informatycznych. Systemy krytyczne.	2
W4	Problematyka oprogramowania systemów FT (systemów operacyjnych i baz danych). Plany samotestowania, samodiagnozy i odporności na błędy. Bezpieczeństwo oprogramowania i systemów: przepełnienie bufora, bezpieczeństwo systemów operacyjnych i oprogramowania. Bezpieczeństwo chmur i Internetu rzeczy.	2
W5	Zarządzanie bezpieczeństwem IT i ocena ryzyka. Środki, plany i procedury. SIEM i audyt bezpieczeństwa	2
W6	Systemy informatyczne tolerujące uszkodzenia. Przegląd, wady i zalety tego typu systemów. Przykłady.	2
W7	BPMN (Business Process Model and Notation) i CMMN (Case Management Model and Notation) w projektowaniu systemów krytycznych.	4

LABORATORIA KOMPUTEROWE		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
K1	Realizacja ćwiczeń dotyczących luk i ataków. Implementacja programu z ukrytymi lukami i opracowanie strategii ich wykorzystania.	2
K2	Laboratorium eksploracyjne z wykorzystaniem zasad bezpieczeństwa, analizy i oceny systemów tolerujących uszkodzenia.	6
K3	Implementacje w aplikacjach punktów kontrolnych, logów i odtwarzanie stanu.	2
K4	Projektowanie w BPMN i CMNN; wykrywanie anomalii systemowych.	5

7 NARZĘDZIA DYDAKTYCZNE

N1 wykłady

N2 Ćwiczenia laboratoryjne

N3 Ćwiczenia projektowe

N4 Konsultacje i dyskusje

8 OBCIĄŻENIE PRACĄ STUDENTA

FORMA AKTYWNOŚCI	ŚREDNIA LICZBA GODZIN NA ZREALIZOWANIE AKTYWNOŚCI
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	40
Konsultacje przedmiotowe	4
Egzaminy i zaliczenia w sesji	2
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	15
Opracowanie wyników	10
Przygotowanie raportu, projektu, prezentacji, dyskusji	10
SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA	81
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	3.00

9 SPOSOBY OCENY

OCENA FORMUJĄCA

F1 Ocena z projektu zespołowego

F2 Ocena ze sprawozdań z ćwiczeń laboratoryjnych

F3 Ocena z kolokwium

OCENA PODSUMOWUJĄCA

P1 średnia ważona ocen formujących

WARUNKI ZALICZENIA PRZEDMIOTU

W1 Warunkiem uzyskania zaliczenia jest uczestnictwo w zajęciach, zaliczenie sprawozdań i projektów oraz uzyskanie pozytywnych ocen.

KRYTERIA OCENY

EFEKT KSZTAŁCENIA 1	
NA OCENĘ 2.0	Student nie potrafi zrealizować prostego zdania.
NA OCENĘ 3.0	Student potrafi pracować indywidualnie i w zespole.
NA OCENĘ 3.5	Student potrafi zrealizować proste zadania.

NA OCENĘ 4.0	Student umie oszacować czas potrzebny na realizację zleconego zadania.
NA OCENĘ 4.5	Student potrafi pracować w zespole, wykorzystując swoją wiedzę i dzieląc się nią z osobami w zespole.
NA OCENĘ 5.0	Student potrafi wykorzystać swoją wiedzę, przekazać ją słabszym osobom w grupie. Potrafi zorganizować harmonogram pracy dla zespołu projektowego.
EFEKT KSZTAŁCENIA 2	
NA OCENĘ 2.0	Student NIE zna koncepcje asercji i obsługi wyjątków.
NA OCENĘ 3.0	Student zna koncepcje asercji i obsługi wyjątków.
NA OCENĘ 3.5	+ Ma podstawową wiedzę w zakresie systemów tolerujących uszkodzenia.
NA OCENĘ 4.0	Student potrafi programować asercje i wyjątki w językach niskopoziomowych i obiektowych.
NA OCENĘ 4.5	+Umie zastosować systemy tolerujące uszkodzenia.
NA OCENĘ 5.0	Student potrafi optymalizować programy z obsługą asercji i wyjątków, także w programach mobilnych. Zna i bardzo dobrze potrafi wykorzystać w praktyce systemy tolerujące uszkodzenia.
EFEKT KSZTAŁCENIA 3	
NA OCENĘ 2.0	Brak wiedzy w w zakresie problemów tolerowania uszkodzeń w systemach informatycznych.
NA OCENĘ 3.0	Student ma wiedzę w zakresie problemów tolerowania uszkodzeń w systemach operacyjnych i systemach zarządzania bazami danych.
NA OCENĘ 3.5	+Posiada podstawową wiedzę w zakresie technik FT oraz zna zagrożenia w bazodanowych i sieciowych konfiguracjach systemu komputerowego
NA OCENĘ 4.0	Student potrafi zalgorytmizować problemy operacyjne systemów informatycznych: synchronizacji procesów i szeregowania zadań.
NA OCENĘ 4.5	+ Potrafi instalować i programować bezpieczne protokoły sieciowe i dzienniki powtórzeń baz danych i chmur obliczeniowych.
NA OCENĘ 5.0	Student potrafi zoptymalizować wielokryterialnie rozwiązania problemów równoczesnego szeregowania zadań i synchronizacji procesów. Student potrafi zarządzać i stroić systemy zarządzania baz danych i systemy sieciowe pod względem efektywności i bezpieczeństwa ich działania.
EFEKT KSZTAŁCENIA 4	
NA OCENĘ 2.0	Student nie ma wiedzy w zakresie technik i zasad bezpieczeństwa komputerowego.
NA OCENĘ 3.0	Student zna i rozumie koncepcję bezpieczeństwa komputerowego.
NA OCENĘ 3.5	+Potrafi scharakteryzować, wskazać wady i zalety dostępnych technik bezpieczeństwa komputerowego.

NA OCENĘ 4.0	+Student posiada wiedzę w zakresie technik i zasad bezpieczeństwa komputerowego.
NA OCENĘ 4.5	+Student zna zasady bezpieczeństwa oprogramowania i systemów.
NA OCENĘ 5.0	+Posiada dużą wiedzę w zakresie bezpieczeństwa chmur i Internetu rzeczy.

10 MACIERZ REALIZACJI PRZEDMIOTU

EFEKT KSZTAŁCENIA	ODNIESIENIE DANEGO EFEKTU DO SZCZEGÓŁOWYCH EFEKTÓW ZDEFINIOWANYCH DLA PROGRAMU	CELE PRZEDMIOTU	TREŚCI PROGRAMOWE	NARZĘDZIA DYDAKTYCZNE	SPOSOBY OCENY
EK1	K_U12 K_K02	Cel 2 Cel 3	P1 P2 P3 W1 W5 W7 K4	N3 N4	F1 P1
EK2	K_U04	Cel 1 Cel 2	P1 P2 W2 W5 K2 K3	N1 N2 N3	F1 F2 P1
EK3	K_U01	Cel 2 Cel 3	P1 P3 W1 W4 W5 W6 K1 K2 K4	N1 N2 N3 N4	F1 F2 P1
EK4	K_W04 K_U01 K_U04	Cel 2 Cel 3	P1 P2 P3 W1 W4 W5 K1 K2 K3 K4	N1 N2 N3 N4	F1 F2 P1

11 WYKAZ LITERATURY

LITERATURA PODSTAWOWA

- [1] | **P.A. Lee, T. Anderson** — *Fault Tolerance. Principles and Practice*, , 1990, Springer
- [2] | **Josef Pieprzyk, Thomas Hardjono, Jennifer Seberry**, — *Teoria bezpieczeństwa systemów komputerowych*, Warszawa, 2007, Helion
- [3] | **Drejewicz Szymon** — *Zrozumieć BPMN. Modelowanie procesów biznesowych*,, Warszawa, 2012, Helion

LITERATURA UZUPEŁNIAJĄCA

- [1] | **Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse** — *Bezpieczeństwo aplikacji mobilnych*, Warszawa, 2012, Helion
- [2] | **Prashant Verma, Akshay Dixit** — *Bezpieczeństwo aplikacji mobilnych. Receptury*,, Warszawa, 2017, Helion

LITERATURA DODATKOWA

[1 | Marek Ogiela — *Bezpieczeństwo systemów komputerowych*, Kraków, 2002, AGH

12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH**OSOBA ODPOWIEDZIALNA ZA KARTĘ**

mgr inż. Anna Suchenia (kontakt: asuchenia@pk.edu.pl)

OSOBY PROWADZĄCE PRZEDMIOT

1 mgr inż. Anna Suchenia (kontakt: asuchenia@pk.edu.pl)

2 dr inż. Karol Suchenia (kontakt: karol.suchenia@pk.edu.pl)

13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejscowość, data)

(odpowiedzialny za przedmiot)

(dziekan)

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....
.....