Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2021/2022

Wydział Inżynierii Elektrycznej i Komputerowej

Kierunek studiów: Infotronika

Profil: Ogólnoakademicki

Forma sudiów: 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 21/22
Kategoria przedmiotu	Przedmioty wybieralne
Liczba punktów ECTS	4.00
Semestry	3

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykłady	Ćwiczenia	Laboratoria	Laboratoria komputerowe	Projekty	
3	15	0	0	15	15	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 niskopoziomowym i obiektowym.

3 Podstawowa wiedza z inżynierii oprogramowania i inżynierii elektrycznej.

5 Efekty kształcenia

EK1 Kompetencje społeczne Student potrafi pracować indywidualnie i 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

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

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

Projekty		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
P1	Projekt i implementacja aplikacji tolerującej uszkodzenia z wykorzystaniem zasad bezpieczeństwa systemów komputerowych.	5
P2	Implementacje algorytmów FT w programowaniu aplikacji numerycznych, morfologicznych i semantycznych. Również wykorzystanie algorytmów FT w działaniu systemów operacyjnych i systemów baz danych.	5
P3	Modelowanie systemów FT za pomocą BPMN i CMNN.	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	45
Konsultacje przedmiotowe	19
Egzaminy i zaliczenia w sesji	6
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	30
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 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 3.0	Student zna koncepcje asercji i obsługi wyjątków. Ma podstawową wiedzę w zakresie systemów tolerujących uszkodzenia.
Na ocenę 4.0	Student potrafi programować asercje i wyjątki w językach niskopoziomowych i obiektowych. 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 3.0	Student ma wiedzę w zakresie problemów tolerowania uszkodzeń w systemach operacyjnych i systemach zarządzania bazami danych. 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. 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	.
Na ocenę 3.0	Student zna i rozumie koncepcję bezpieczeństwa komputerowego.
Na ocenę 4.0	Student posiada wiedzę w zakresie technik i zasad bezpieczeństwa komputerowego.
Na ocenę 5.0	Student zna zasady bezpieczeństwo oprogramowania i systemów. Posiada 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_U11 K_U12	Cel 2 Cel 3	W1 P1 P2 P3	N3 N4	F1 P1
EK2	K_W04 K_U02	Cel 1 Cel 2	K2 K3 W2 W5 P1 P2	N1 N2 N3	F1 F2 P1
EK3	K_U02 K_U05	Cel 2 Cel 3	K1 K2 K4 W1 W4 W5 W6 P1 P3	N1 N2 N3 N4	F1 F2 P1
EK4	K_U02 K_U04	Cel 2 Cel 3	K1 K2 K3 K4 W1 W4 W5 P1 P2 P3	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 — *Bezpieczństwo aplikacji moblinych. 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 dr hab. inż. prof. PK Mieczysław Drabowski (kontakt: drabowski@pk.edu.pl)

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

3 dr inż. Sławomir Bąk (kontakt: sbak@pk.edu.pl)

13 Zatwierdzenie karty przedmiotu do realizacji

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

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .

. . . . . .

. . . . . .