Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2020/2021

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	Bezpieczeństwo systemów informatycznych
Nazwa przedmiotu w języku angielskim	
Kod przedmiotu	WIEiK INFOTRON oIIS PW3 20/21
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 Cel przedmiotu 1 Przedstawienie zagrożeń systemów informatycznych i cechy systemów bezpiecznych

Cel 2 Cel przedmiotu 2 Przedstawienie modeli wiarygodności, wymiarów wiarygodności.

Cel 3 Cel przedmiotu 3 Analiza i synteza systemów o podwyższonym stopniu dostępności, niezawodności, bezpieczeństwa i zabezpieczenia.

Cel 4 Cel przedmiotu 4 Przedstawienie elementów problematyki kryptosystemów.

Cel 5 Cel przedmiotu 5 Przedstawienie bezpieczeństwa baz danych i sieci komputerowych.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 Wymaganie 1 1.Znajomość organizacji systemów komputerowych (architektury, systemów operacyjnych i baz danych).

2 Wymaganie 2 2.Umiejętność programowania w językach niskopoziomowym i obiektowym.

3 Wymaganie 3 3.Znajomość zagadnień Internetu rzeczy, chmur obliczeniowych i systemów wbudowanych.

5 Efekty kształcenia

EK1 Umiejętności Efekt kształcenia 1 Potrafi zaprojektować system wiarygodny. Potrafi wykorzystać narzędzia programistyczne: eBPMN, BPMN Modeler.

EK2 Umiejętności Efekt kształcenia 2 Potrafi skonstruować oprogramowanie bezpieczne. Potrafi posługiwać się platformami programistycznymi C/C++, Java.

EK3 Wiedza Efekt kształcenia 3 Zna problemy bezpieczeństwa systemów informatycznych, w tym systemów operacyjnych.

EK4 Wiedza Efekt kształcenia 4 Ma wiedzę dotyczącą bezpieczeństwa infrastruktury informatycznej, baz danych i chmur obliczeniowych oraz sieci komputerowych i Internetu rzeczy.

6 Treści programowe

Wykłady		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Treści programowe 1 System infotroniczny/mechatroniczny jako złożony system informatyczny. Redundacje sprzętowe i programowe dla zwiększania poziomu bezpieczeństwa takich systemów. Zagrożenia systemów w kontekście poufności, integralności i dostępności informacji, ogólna analiza zagrożeń i ryzyka, przykładowe ataki. Modele bezpieczeństwa i klasy bezpieczeństwa systemów informatycznych.	4
W2	Treści programowe 2 Problematyka bezpiecznego programowania. Plany samotestowania, samodiagnozy i odporności na błędy.	4
W3	Treści programowe 3 Bezpieczeństwo systemów operacyjnych i sieci komputerowych.	3
W4	Treści programowe 4 Bezpieczeństwo systemów baz danych.	2
W5	Treści programowe 5 BPMN (Business Process Model and Notation) i CMMN (Case Management Model and Notation) w projektowaniu systemów bezpiecznych.	2

Projekty		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
P1	Treści programowe 1 Implementacje algorytmów bezpiecznego działania systemów operacyjnych i systemów baz danych.	6
P2	Treści programowe 2 Implementacje algorytmów bezpiecznego programowania aplikacji numerycznych, morfologicznych i semantycznych.	5
P3	Treści programowe 3 Modelowanie systemów bezpiecznych za pomocą BPMN i CMNN.	4

Laboratoria komputerowe		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
K1	Treści programowe 1 Implementacje asercji w programach w językach niskopoziomowych.	4
K2	Treści programowe 2 Implementacje wyjątków w programach w językach obiektowych.	4
K3	Treści programowe 3 Implementacje w aplikacjach punktów kontrolnych, logów i odtwarzanie stanu.	4
K4	Treści programowe 4 Ćwiczenia w projektowanie w BPMN i CMNN; wykrywanie anomalii systemowych.	3

7 Narzędzia dydaktyczne

N1 Narzędzie 1 wykłady

N2 Narzędzie 2 dyskusje

N3 Narzędzie 3 konsultacje

N4 Narzędzie 4 prezentacje multimedialne

N5 Narzędzie 5 ćwiczenia laboratoryjne

N6 Narzędzie 6 ćwiczenia projektowe

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	20
Opracowanie wyników	15
Przygotowanie raportu, projektu, prezentacji, dyskusji	15
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 1 sprawozdania z ćwiczeń laboratoryjnych

F2 Ocena 2 projekt zespołowy

F3 Ocena 3 dokumentacja projektowa

F4 Ocena 4 aktywność na ćwiczeniach

Ocena podsumowująca

P1 Ocena 1 Średnia ważona ocen formujących F1, F2, F3, F4.

Warunki zaliczenia przedmiotu

W1 Ocena 1 Warunkiem uzyskania zaliczenia jest uczestnictwo na zajeciach, oddanie sprawozdań i projektów oraz uzyskanie pozytywnej oceny podsumowującej.

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 3.0	Student zna pojęcie wiarygodności i potrafi podać jej wymiary.

Na ocenę 4.0	Student potrafi wskazać przykłady redundancji występujących w poszczególnych warstwach systemu dla jego ochrony i bezpieczeństwa.
Na ocenę 5.0	Student potrafi projektować systemy komputerowe o zwiększonym poziomie wiarygodności
Efekt kształcenia 2	
Na ocenę 3.0	Student zna koncepcje asercji i obsługi wyjątków.
Na ocenę 4.0	Student potrafi programować asercje i wyjątki w językach niskopoziomowych i obiektowych.
Na ocenę 5.0	Student potrafi optymalizować programy z obsługą asercji i wyjątków, także w programach mobilnych.
Efekt kształcenia 3	
Na ocenę 3.0	Student zna kolizje zasobowe występujące w systemach i zna metody ich przeciwdziałaniu.
Na ocenę 4.0	Student potrafi zalgorytmizować problemy operacyjne systemów informatycznych: synchronizacji procesów i szeregowania zadań.
Na ocenę 5.0	Student potrafi optymalizować wielokryterialnie rozwiązania problemów równoczesnego szeregowania zadań i synchronizacji procesów.
Efekt kształcenia 4	
Na ocenę 3.0	Student rozumie znaczenie bezpieczeństwa danych oraz zna zagrożenia w bazodanowych i sieciowych konfiguracjach systemu komputerowego.
Na ocenę 4.0	Student potrafi instalować i programować bezpieczne protokoły sieciowe i dzienniki powtórzeń baz danych i chmur obliczeniowych.
Na ocenę 5.0	Student potrafi zarządzać i stroić systemy zarządzania baz danych i systemy sieciowe pod względem efektywności i bezpieczeństwa ich działania, w tym 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		Cel 1	W1 W5 P1 K1	N1 N3 N5	F1 F2 F3 F4 P1
EK2		Cel 2 Cel 3	W2 W3	N1 N3 N5	F1 F2 F3 F4 P1

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK3		Cel 3 Cel 4	W3 W4 W5 P1 P3 K2 K4	N1 N3 N4 N5	F1 F2 F3 F4 P1
EK4		Cel 3 Cel 4 Cel 5	W4 W5 P2 P3 K2 K3 K4	N3 N5 N6	F1 F2 F3 F4 P1

11 Wykaz literatury

Literatura podstawowa

[1] **1.Josef Pieprzyk, Thomas Hardjono, Jennifer Seberry** — *Teoria bezpieczeństwa systemów komputerowych*, Warszawa, 2007, Helion

[2] **2.Marek Ogiela** — *Bezpieczeństwo systemów komputerowych,*, Kraków, 2002, AGH

[3] **3.William Stalling** — *Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów.*, Warszawa, 2015, Helion

[4] **4.William Stalling** — *Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji*, Warszawa, 2016, Heloin

Literatura uzupełniająca

[1] **5.Simson Garfinkel, Gene Spafforg** — *Bezpieczeństwo w Unixie i Internecie*, Warszawa, 2007, Wydawnictwo RM

[2] **6.Drejewicz Szymon** — *Zrozumieć BPMN. Modelowanie procesów biznesowych,*, Warszawa, 2012, Wydawnictwo Helion

[3] **7. Piotrowski Marek** — *, Procesy biznesowe w praktyce. Projektowanie, testowanie i optymalizacja.*, Warszawa, 2016, Wydawnictwo One Press

Literatura dodatkowa

[1] **1.Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse** — *Bezpieczeństwo aplikacji mobilnych,*, Warszawa, 2018, Helion

[2] **2.Prashant Verma, Akshay Dixit** — *Bezpieczństwo aplikacji moblinych. Receptury,*, Warszawa, 2017, Helion

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr hab.inż. Mieczysław Drabowski (kontakt: `gpedrak@pk.edu.pl`)

Osoby prowadzące przedmiot

1 dr hab. inż. prof. PK Mieczysław Drabowski (kontakt: drabowski@pk.edu.pl)

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

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

13 Zatwierdzenie karty przedmiotu do realizacji

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

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .

. . . . . .

. . . . . .