

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2019/2020

Wydział Inżynierii Elektrycznej i Komputerowej

Kierunek studiów: Infotronika

Profil: Ogólnoakademicki

Forma studiów: stacjonarne

Kod kierunku: ITron

Stopień studiów: II

Specjalności: bez specjalności

1 INFORMACJE O PRZEDMIOCIE

NAZWA PRZEDMIOTU	Bezpieczeństwo systemów informatycznych
NAZWA PRZEDMIOTU W JĘZYKU ANGIELSKIM	Security of computing systems
KOD PRZEDMIOTU	WIEiK INFOTRON oIIS PW3 19/20
KATEGORIA PRZEDMIOTU	Przedmioty wybieralne
LICZBA PUNKTÓW ECTS	4.00
SEMESTRY	3

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁADY	ĆWICZENIA	LABORATORIA	LABORATORIA KOMPUTERO- WE	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 BŁOKÓW 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 zajęciach, 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	K_W03 K_U02	Cel 1	W1 W5 P1 K1	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
EK2	K_W03 K_W05 K_U04	Cel 2 Cel 3	W2 W3	N1 N3 N5	F1 F2 F3 F4 P1
EK3	K_W02 K_U01 K_U03 K_U11 K_K03	Cel 3 Cel 4	W3 W4 W5 P1 P3 K2 K4	N1 N3 N4 N5	F1 F2 F3 F4 P1
EK4	K_W02 K_W03 K_W05 K_U01 K_U08 K_K02	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, Helion

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** — *Bezpieczeństwo aplikacji mobilnych. 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)

.....
.....
.....