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	Bezpieczeństwo systemów informatycznych
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 Zapoznanie z zasadami (metodami) projektowania i administrowania systemów bezpieczeństwa.

Cel 2 Poznanie zagadnień określania zagrożeń systemów komputerowych i sieci, oceny względnego ryzyka tych zagrożeń.

Cel 3 Zapoznanie z zasadami bezpieczeństwa i ich wdrożenie, elementy kryptografii.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

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

2 Umiejętność programowania w językach niskopoziomowym i obiektowym.

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

5 Efekty kształcenia

EK1 Wiedza Zna problemy i zasady bezpieczeństwa systemów informatycznych, w tym systemów operacyjnych.

EK2 Wiedza Ma wiedzę dotyczącą bezpieczeństwa infrastruktury informatycznej, baz danych i chmur obliczeniowych oraz sieci komputerowych i Internetu rzeczy.

EK3 Kompetencje społeczne Student potra wykorzystać swoją wiedzę, przekazać ją słabszym osobom w grupie. Potra zorganizować harmonogram pracy dla zespołu projektowego.

EK4 Umiejętności Absolwent potrafi zaprojektować system wiarygodny. Potrafi wykorzystać narzędzia programistyczne: eBPMN, BPMN Modeler. Potrafi skonstruować oprogramowanie bezpieczne. Potrafi posługiwać się platformami programistycznymi C/C++, Java.

6 Treści programowe

Wykłady		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Moduł 1: Zasady bezpieczeństwa i ich wdrożenie. Podstawowe wymagania bezpieczeństwa dotyczące poufności, nienaruszalności i dostępności. Rodzaje zagrożeń bezpieczeństwa i ataków.	3
W2	Moduł 2: Podstawowe zasady projektowania bezpieczeństwa. Modele bezpieczeństwa i klasy bezpieczeństwa systemów informatycznych. Projektowanie systemów bezpiecznych z użyciem BPMN i CMMN. Bezpieczeństwo oprogramowania i infrastruktury.	4
W3	Moduł 3: Elementy kryptograficzne. Podstawy działania algorytmów szyfrowania danych, mechanizm podpisu cyfrowego i pojęcie kopert cyfrowych. Narzędzia kryptograficzne.	4
W4	Moduł 4: Praca administratora bezpieczeństwa. Bezpieczeństwo systemów operacyjnych i sieci komputerowych. Bezpieczeństwo systemów baz danych. Zapewnienie bezpiecznej pracy sieci.	4

Laboratoria komputerowe		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
K1	Laboratorium eksploracyjne z wykorzystaniem zasad bezpieczeństwa.	6

Laboratoria komputerowe		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
K2	Zagadnienia bezpieczeństwa oprogramowania i programowania defensywnego. Implementacja aplikacji z wykorzystaniem zasad bezpieczeństwa.	2
K3	Bezpieczeństwo systemów operacyjnych (planowanie, hartowanie, dbałość o bezpieczeństwo, bezpieczeństwo wirtualizacji).	2
K4	Ćwiczenia w projektowanie w BPMN i CMNN; wykrywanie anomalii systemowych.	5

Projekty		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
P1	Wprowadzenie do tematyki. Zapoznanie z zasadami i tematami projektów systemów i aplikacji bezpiecznych.	6
P2	Projekt i implementacja systemu pozwalającego na zaspokojenie wymagań bezpieczeństwa komputerowego, z wykorzystaniem standardów w tej dziedzinie. Implementacja z użyciem algorytmów bezpiecznego programowania aplikacji numerycznych, morfologicznych i semantycznych.	5
P3	Modelowanie systemów bezpiecznych za pomocą BPMN i CMNN.	4

7 Narzędzia dydaktyczne

N1 Wykłady połączone z dyskusją

N2 Prezentacje multimedialne

N3 Ćwiczenia laboratoryjne

N4 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	30
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	**131**
Sumaryczna liczba punktów ECTS dla przedmiotu	4.00

9 Sposoby oceny

Ocena formująca

F1 Sprawozdania z ćwiczeń laboratoryjnych

F2 Projekt zespołowy

F3 Kolokwium

Ocena podsumowująca

P1 Średnia ważona ocen formujących F1, F2, F3.

Warunki zaliczenia przedmiotu

W1 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 ma podstawowa wiedzę w zakresie problemów i zasad bezpieczeństwa systemów informatycznych, w tym systemów operacyjnych.

Na ocenę 5.0	Student ma dużą wiedzę w zakresie kryptografii, zasad bezpieczeństwa i ich wdrożenia. Potrafi korzystać z bezpiecznego oprogramowania i infrastruktury. Zna i rozumie zasady utrzymania bezpieczeństwa systemu i potrafi wskazać, dlaczego ich przestrzeganie ma kluczowe znaczenie.
Efekt kształcenia 2	
Na ocenę 3.0	Student rozumie znaczenie bezpieczeństwa danych oraz zna zagrożenia w bazodanowych i sieciowych konfiguracjach systemu komputerowego.
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.
Efekt kształcenia 3	
Na ocenę 3.0	Student potra pracować indywidualnie i w zespole.
Na ocenę 5.0	Student potra wykorzystać swoją wiedzę, przekazać ją słabszym osobom w grupie. Potra zorganizować harmonogram pracy dla zespołu projektowego.
Efekt kształcenia 4	
Na ocenę 3.0	Student potrafi wykorzystać narzędzia programistyczne: eBPMN, BPMN Modeler. Umie skonstruować proste oprogramowanie bezpieczne.
Na ocenę 5.0	Student potrafi zaprojektować złożony system wiarygodny. Potrafi w sposób biegły wykorzystać narzędzia programistyczne: eBPMN, BPMN Modeler. Potrafi skonstruować oprogramowanie bezpieczne.

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_W04 K_U04	Cel 1 Cel 2 Cel 3	W1 W2 W3 W4 K1 K2 K3 K4 P1 P3	N1 N2 N3	F1 F2 F3 P1
EK2	K_W02 K_W08	Cel 1 Cel 2 Cel 3	W2 W3 W4 K1 K2 K3 K4 P2 P3	N1 N2 N3 N4	F1 F2 F3 P1
EK3	K_U04 K_U11 K_U12 K_K03	Cel 1 Cel 2 Cel 3	W2 W4 K1 P1 P2 P3	N1 N2 N3 N4	F1 F2 P1
EK4	K_U01 K_U04 K_U10 K_K02	Cel 1 Cel 2 Cel 3	W3 W4 K1 P1 P2 P3	N1 N2 N3 N4	F2 P1

11 Wykaz literatury

Literatura podstawowa

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

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

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

Literatura uzupełniająca

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

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

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

Literatura dodatkowa

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

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

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 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)

.....

.....

.....