Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2023/2024

Wydział Inżynierii Elektrycznej i Komputerowej

Kierunek studiów: Informatyka w Inżynierii Komputerowej — Profil: Ogólnoakademicki

Forma sudiów: stacjonarne — Kod kierunku: IwIK

Stopień studiów: I

Specjalności: bez specjalności

1 Informacje o przedmiocie

Nazwa przedmiotu	Bezpieczeństwo systemów komputerowych
Nazwa przedmiotu w języku angielskim	
Kod przedmiotu	WIEiK INFOR_W_INZ_KOMP oIS PS10 23/24
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	5.00
Semestry	6

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykłady	Ćwiczenia	Laboratoria	Laboratoria komputerowe	Projekty	
6	20	0	0	30	15	0

3 Cele przedmiotu

Cel 1 Dostarczenie aktualnego przeglądu postępów w bezpieczeństwie systemów komputerowych.

Cel 2 Przedstawienie bezpieczeństwa: systemów operacyjnych, baz danych, sieci komputerowych

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 niskopoziomowych i obiektowych.

5 Efekty kształcenia

EK1 Wiedza Student zna zagrożenia i problemy bezpieczeństwa systemów informatycznych. Ma wiedzę w zakresie cechy bezpiecznych systemów. Posiada wiedzę w zakresie bezpieczeństwa chmur i Internetu rzeczy.

EK2 Wiedza Student ma wiedzę dotyczącą bezpieczeństwa infrastruktury informatycznej, w tym bezpiecznych baz danych i sieci komputerowych.

EK3 Umiejętności Student potrafi skonturować bezpieczne programowanie wykorzystując platformy programistyczne.

EK4 Kompetencje społeczne Student jest gotowy do podejmowania wyzwań zawodowych, zarówno indywidualnych, jak i zespołowych. Wykazuje aktywność w grupie, przyjmując w niej różne role (np. współwykonawcy, wykonawcy projektu).

6 Treści programowe

Wykłady		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Koncepcje bezpieczeństwa komputerowego. Zagrożenia, ataki i aktywa. Podstawowe zasady projektowania bezpieczeństwa (w tym BPMN, CMMN i DMN). Strategia bezpieczeństwa komputerowego. Standardy bezpieczeństwa.	4
W2	Zagrożenia systemów w kontekście poufności, integralności i dostępności. Ogólna analiza zagrożeń i ryzyka, przykładowe ataki. Modele bezpieczeństwa i klasy bezpieczeństwa systemów komputerowych.	4
W3	Bezpieczeństwo systemów operacyjnych. Wprowadzenie do tematyki oraz planowanie bezpieczeństwa systemu operacyjnego. Hartowanie systemu i dbałość o bezpieczeństwo. Bezpieczeństwo systemu Linux i UNIX. Bezpieczeństwo systemu Windows.	6
W4	Bezpieczeństwo baz i centrów danych. Zapotrzebowanie na bezpieczeństwo baz danych. Systemy zarządzania bazami danych. Ataki wstrzykiwania w sql. Kontrolowanie dostępu, wnioskowanie, szyfrowanie.	2
W5	Bezpieczeństwo sieci komputerowych. Bezpieczeństwo: systemów rozproszonych, e-commerce, protokoły bezpiecznej transmisji internetowej IPSec.	2
W6	Bezpieczeństwo chmur i Internetu rzeczy. Koncepcje bezpieczeństwa chmury i Internetu rzeczy. Podejście do bezpieczeństwa.	2

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.	6
K2	Projektowanie bezpiecznych systemów komputerowych w BPMN i CMNN; wykrywanie anomalii systemowych.	6
K3	Bezpieczeństwo systemów operacyjnych (planowanie, hartowanie, dbałość o bezpieczeństwo, bezpieczeństwo wirtualizacji).	8
K4	Laboratorium eksploracyjne z wykorzystaniem zasad bezpieczeństwa, analizy i oceny systemów bezpiecznych.	10

Projekty		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
P1	Wprowadzenie do tematyki. Zapoznanie z zasadami i tematami projektów systemów i aplikacji bezpiecznych.	3
P2	Projekt i implementacja systemu pozwalającego na zaspokojenie wymagań bezpieczeństwa komputerowego, z wykorzystaniem standardów w tej dziedzinie oraz algorytmów bezpiecznego programowania.	8
P3	Modelowanie systemów bezpiecznych za pomocą BPMN i CMNN.	4

7 Narzędzia dydaktyczne

N1 Wykłady, prezentacje multimedialne

N2 Laboratoria komputerowe

N3 Ćwiczenia projektowe, dyskusje i konsultacje

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	65
Konsultacje przedmiotowe	15
Egzaminy i zaliczenia w sesji	4
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	20
Opracowanie wyników	20
Przygotowanie raportu, projektu, prezentacji, dyskusji	8
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**132**
Sumaryczna liczba punktów ECTS dla przedmiotu	5.00

9 Sposoby oceny

Ocena formująca

F1 Sprawozdanie z ćwiczenia laboratoryjnego

F2 Projekt zespołowy oraz dokumentacja projektowa

F3 Kolokwium

Ocena podsumowująca

P1 Średnia ważona ocen formujących F1, F2 i F3

Warunki zaliczenia przedmiotu

W1 Warunkiem uzyskania zaliczenia jest uczestnictwo na zajęciach, oddanie sprawozdań i projektów, pozytywna ocena z kolokwium oraz uzyskanie pozytywnej oceny podsumowującej.

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Brak podstawowej wiedzy w zakresie zagrożeń i problemów bezpieczeństwa systemów informatycznych
Na ocenę 3.0	+Student zna i rozumie zagadnienie bezpieczeństwa systemów informatycznych.

Na ocenę 3.5	+Student zna i rozumie zagadnienie bezpieczeństwa systemów informatycznych. Potrafi wskazać zagrożenia i problemy z tym związane.
Na ocenę 4.0	+Student ma wiedze w zakresie cech bezpiecznych systemów komputerowych.
Na ocenę 4.5	+Zna i rozumie szczegóły związane z planowaniem bezpiecznego systemu.
Na ocenę 5.0	+Student zna i rozumie podejście do bezpieczeństwa systemów operacyjnych oraz bezpieczeństwa chmury i Internetu rzeczy. Posiada wiedze w zakresie specyficznych aspektów zabezpieczania systemów Linux, Unix i Windows. Potrafi zdefiniować obliczenia chmurowe.
Efekt kształcenia 2	
Na ocenę 2.0	Brak podstawowej wiedzy w zakresie bezpieczeństwa infrastruktury informatycznej.
Na ocenę 3.0	Student rozumie znaczenie bezpieczeństwa danych.
Na ocenę 3.5	+ Student 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.
Na ocenę 4.5	Student potrafi zarządzać bezpieczeństwem sieci oraz zarządzać bazami danych,
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 2.0	Brak umiejętności w programowaniu bezpiecznych aplikacji.
Na ocenę 3.0	Student potrafi napisać bezpieczny kod.
Na ocenę 3.5	+ Poprawnie umie implementować algorytmy oraz zapobiegać szkodliwym działaniom.
Na ocenę 4.0	Student potrafi programować asercje oraz wyjątki w językach niskopoziomowych i obiektowych.
Na ocenę 4.5	+Ma umiejętność wskazywania podobieństw i różnic między atakami wstrzykiwania poleceń a atakami wstrzykiwania SQL.
Na ocenę 5.0	Student potrafi optymalizować programy z obsługą asercji oraz wyjątków także w aplikacjach mobilnych.
Efekt kształcenia 4	
Na ocenę 2.0	Student nie potrafi współpracować i nie wykonuje zadań.
Na ocenę 3.0	Student potrafi współpracować w zespole wykonując dobrze powierzone mu zadania.

Na ocenę 3.5	Student potrafi pracować w zespole i dobrze organizować swój czas na realizację powierzonego mu zadania.
Na ocenę 4.0	+ posiada i dzieli się swoją wiedzą i doświadczeniem z innymi osobami w zespole.
Na ocenę 4.5	Student potrafi współpracować w zespole pełniąc w nim różne role (np. współwykonawcy, wykonawcy projektu).
Na ocenę 5.0	Jest gotowy do podejmowania wzywań zawodowych i potrafi być odpowiedzialny za grupę, potrafi również pełnić rolę kierownika projektu.

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_W10 K_W12	Cel 1 Cel 2	W1 W2 W3 W4 W5 W6 K2 K3 P2	N1 N2 N3	F1 F2 F3
EK2	K_W10 K_W12	Cel 1 Cel 2	W1 W2 W3 W4 W5 W6 K1 K2 K3 K4 P1 P2 P3	N1 N2 N3	F1 F2 F3
EK3	K_W17 K_U19	Cel 1 Cel 2	W1 W3 W4 W5 W6 K1 K2 K3 K4 P1 P2 P3	N1 N2 N3	F1 F2 F3
EK4	K_U02 K_K03 K_K05	Cel 1	P1 P2 P3	N3	F1 F2 P1

11 Wykaz literatury

Literatura podstawowa

[1] Hardjono T., Seberry J., Pieprzyk J. — *Teoria bezpieczeństwa systemów komputerowych*, Warszawa, 2007, Helion

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

[3] Drejewicz Sz. — *Zrozumieć BPMN. Modelowanie procesów biznesowych*, Warszawa, 2012, Helion

Literatura uzupełniająca

[1] Lawrie Brown , William Stallings — *Bezpieczeństwo systemów informatycznych. Zasady i praktyka*, , 2019, Helion

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: anna.suchenia@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)

. . . . . .

. . . . . .