Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2023/2024

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 23/24
Kategoria przedmiotu	Przedmioty wybieralne
Liczba punktów ECTS	3.00
Semestry	3

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykłady	Ćwiczenia	Laboratoria	Laboratoria komputerowe	Projekty	
3	15	0	0	15	10	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. Posiada wiedzę w zakresie cech bezpiecznych systemów, 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 (C/C++, Java, Python).

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.	3
W2	Zagrożenia systemów w kontekście poufności, integralności i dostępności. Ogólna analiza zagrożeń i ryzyka, przykładowe ataki. Modele bezpieczeństwa i klasy bezpieczeństwa systemów komputerowych.Problematyka bezpiecznego programowania	3
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.	3
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

Projekty		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
P1	Wprowadzenie do tematyki. Zapoznanie z zasadami i tematami projektów systemów i aplikacji bezpiecznych.	2
P2	Projekt i implementacja systemu pozwalającego na zaspokojenie wymagań bezpieczeństwa komputerowego, z wykorzystaniem standardów w tej dziedzinie oraz algorytmów bezpiecznego programowania.	4
P3	Modelowanie systemów bezpiecznych za pomocą BPMN i CMNN.	4

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.	3
K2	Projektowanie bezpiecznych systemów komputerowych w BPMN i CMNN; wykrywanie anomalii systemowych.	3
K3	Bezpieczeństwo systemów operacyjnych (planowanie, hartowanie, dbałość o bezpieczeństwo, bezpieczeństwo wirtualizacji).	4
K4	Laboratorium eksploracyjne z wykorzystaniem zasad bezpieczeństwa, analizy i oceny systemów bezpiecznych.	5

7 Narzędzia dydaktyczne

N1 Wykłady, prezentacje multimedialne

N2 Ćwiczenia laboratoryjne

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	40
Konsultacje przedmiotowe	6
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	10
Opracowanie wyników	10
Przygotowanie raportu, projektu, prezentacji, dyskusji	10
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**80**
Sumaryczna liczba punktów ECTS dla przedmiotu	3.00

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 zagrożenia i problemów bezpieczeństwa systemów informatycznych.
Na ocenę 3.0	Student zna i rozumie zagadnienie bezpieczeństwa systemów informatycznych.

Na ocenę 3.5	+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 wiedzy w zakresie bezpieczeństwa infrastruktury informatycznej.
Na ocenę 3.0	Student rozumie znaczenie bezpieczeństwa danych oraz zna zagrożenia w bazodanowych i sieciowych konfiguracjach systemu komputerowego.
Na ocenę 3.5	Student zna zasady dotyczące bezpieczeństwa sieci komputerowych oraz Internetu rzeczy.
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 systemów baz 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 zakresie implementowania prostych 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 pracować w zespole.
Na ocenę 3.0	Student potrafi współpracować w zespole wykonując dobrze powierzone mu zadania.

Na ocenę 3.5	Student potrafi dobrze zarządzać i organizować swój czas. Chętnie bierze udział w dyskusjach w ramach zespołu.
Na ocenę 4.0	Student wykazuje aktywność w grupie, stara się szukać rozwiązań proponując swoje pomysły.
Na ocenę 4.5	Student posiada dużą wiedzę i umiejętnie dzieli się nią ze swoim zespołem.
Na ocenę 5.0	Student potrafi współpracować w zespole pełniąc w nim różne role. Jest gotowy do podejmowania wzywań zawodowych i potrafi być odpowiedzialny za grupę.

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_U01	Cel 1 Cel 2	W1 W2 W3 W4 W5 W6 P2 K2 K3	N1 N2 N3	F1 F2 F3
EK2	K_U01	Cel 1 Cel 2	W1 W2 W3 W4 W5 W6 P1 P2 P3 K1 K2 K3 K4	N1 N2 N3	F1 F2 F3
EK3	K_W02	Cel 1 Cel 2	W1 W3 W4 W5 W6 P1 P2 P3 K1 K2 K3 K4	N1 N2 N3	F1 F2 F3
EK4	K_U12 K_K02	Cel 1	P1 P2 P3	N3	F1 F2 P1

11 Wykaz literatury

Literatura podstawowa

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

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

Literatura uzupełniająca

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

. . . . . .

. . . . . .