

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2022/2023

Wydział Inżynierii Elektrycznej i Komputerowej

Kierunek studiów: Informatyka w Inżynierii Komputerowej

Profil: Ogólnoakademicki

Forma studiów: niestacjonarne

Kod kierunku: IwIK

Stopień studiów: I

Specjalności: bez specjalności

1 INFORMACJE O PRZEDMIOCIE

NAZWA PRZEDMIOTU	Bezpieczeństwo systemów komputerowych
NAZWA PRZEDMIOTU W JĘZYKU ANGIELSKIM	Security of computer systems
KOD PRZEDMIOTU	WIEiK INFOR_W_INZ_KOMP oIN PS15 22/23
KATEGORIA PRZEDMIOTU	Przedmioty specjalnościowe
LICZBA PUNKTÓW ECTS	5.00
SEMESTRY	7

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁADY	ĆWICZENIA	LABORATORIA	LABORATORIA KOMPUTERO- WE	PROJEKTY	
7	15	0	0	0	25	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 skonstruować 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

PROJEKTY		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
P1	Wprowadzenie do tematyki. Zapoznanie z zasadami i tematami projektów systemów i aplikacji bezpiecznych.	4
P2	Projekt i implementacja systemu pozwalającego na zaspokojenie wymagań bezpieczeństwa komputerowego, z wykorzystaniem standardów w tej dziedzinie oraz algorytmów bezpiecznego programowania.	15
P3	Modelowanie systemów bezpiecznych za pomocą BPMN i CMNN.	6

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, CMNN 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.	2
W3	Problematyka bezpiecznego programowania. Plany samotestowania, samodiagnozy i odporności na błędy.	2

WYKŁADY		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W4	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.	2
W5	Bezpieczeństwo baz i centrów danych. Zapotrzebowanie na bezpieczeństwo baz danych. Systemy zarządzania bazami danych. Ataki wstrzykiwania w sql. Kontrolowanie dostępu, wnioskowanie, szyfrowanie.	2
W6	Bezpieczeństwo sieci komputerowych. Bezpieczeństwo: systemów rozproszonych, e-commerce, protokoły bezpiecznej transmisji internetowej IPSec.	2
W7	Bezpieczeństwo chmur i Internetu rzeczy. Koncepcje bezpieczeństwa chmury i Internetu rzeczy. Podejście do bezpieczeństwa.	2

7 NARZĘDZIA DYDAKTYCZNE

N1 Wykłady, prezentacje multimedialne

N2 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	20
Egzaminy i zaliczenia w sesji	8
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	20
SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA	128
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	5.00

9 SPOSOBY OCENY

OCENA FORMUJĄCA

F1 Projekt zespołowy oraz dokumentacja projektowa

OCENA PODSUMOWUJĄCA

P1 Egzamin pisemny/ustny

P2 Średnia ważona ocen formujących i egzaminu

WARUNKI ZALICZENIA PRZEDMIOTU

W1 Pozytywna ocena podsumowująca

KRYTERIA OCENY

EFEKT KSZTAŁCENIA 1	
NA OCENĘ 2.0	Brak 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	+ Potrafi wskazać zagrożenia i problemy z tym związane.
NA OCENĘ 4.0	Student ma wiedzę 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 wiedzę 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 i rozumie zasady działania bezpiecznego 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 systemami baz danych pod względem ich bezpieczeństwa oraz prawidłowego działania.
NA OCENĘ 5.0	Student potrafi 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	Student nie umie implementować 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 współpracuje w zespole.
NA OCENĘ 3.0	Student potrafi współpracować w zespole wykonując dobrze powierzone mu zadania.
NA OCENĘ 3.5	Student potrafi organizować i zarządzać czasem potrzebnym na wykonanie powierzonego zadania.
NA OCENĘ 4.0	Student chętnie dzieli się swoimi przemyśleniami, szuka rozwiązań i współpracuje w zespole.
NA OCENĘ 4.5	Student potrafi współpracować w zespole pełniąc w nim różne role.
NA OCENĘ 5.0	Student posiada bardzo dużą wiedzę i dzieli się nią w zespole. 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_W12 K_W23	Cel 1 Cel 2	P1 P2 W1 W2 W3 W4 W5 W6 W7	N1 N2	F1 P1
EK2	K_W12 K_W23	Cel 1 Cel 2	P1 P2 P3 W4 W5 W6 W7	N1 N2	F1 P1

EFEKT KSZTAŁCENIA	ODNIESIENIE DANEGO EFEKTU DO SZCZEGÓŁOWYCH EFEKTÓW ZDEFINIOWANYCH DLA PROGRAMU	CELE PRZEDMIOTU	TREŚCI PROGRAMOWE	NARZĘDZIA DYDAKTYCZNE	SPOSOBY OCENY
EK3	K_W12 K_U02 K_U11	Cel 1 Cel 2	P1 P2 P3 W1 W4 W5 W6 W7	N1 N2	F1 P1
EK4	K_U02 K_U04 K_K05	Cel 1	P1 P2 P3	N2	F1 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

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. Mieczysław Drabowski (kontakt: mieczyslaw.drabowski@pk.edu.pl)

2 mgr inż. Anna Suchenia (kontakt: anna.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)

.....

.....