Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2021/2022

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma sudiów: stacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Teleinformatyka,Cyberbezpieczeństwo

1 Informacje o przedmiocie

Nazwa przedmiotu	Bezpieczeństwo chmur obliczeniowych
Nazwa przedmiotu w języku angielskim	Computational Cloud security
Kod przedmiotu	WIiT I oIIS D15 21/22
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	2.00
Semestry	2

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
2	30	0	15	0	0	0

3 Cele przedmiotu

Cel 1 Cel przedmiotu 1 Zapoznanie studentów z podstawowymi pojęciami i metodami bezpieczeństwa systemów Chmurowych

Cel 2 Cel przedmiotu 2 Zapoznanie studentów z podstawowymi algorytmami zabezpieczania systemów Chmurowych

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 Wymaganie 1 Zaliczenie przedmiotów: algebra, matematyka dyskretna

5 Efekty kształcenia

EK1 Kompetencje społeczne Efekt kształcenia 1 Student posiada umiejętności pracy w grupie, umiejętności komunikacji z nauczycielem, oraz organizacji pracy w grupie. Student posiada umiejętności komunikacji ze srodowiskiem pozauczelnianym w celu popularyzacji wiedzy uzyskanej w ramach nauki oraz przedstawiania wyników swoich badań w sposób zrozumiały i czytelny.

EK2 Umiejętności Efekt kształcenia 2 Student potra zrealizować podstawowe metody z zakresu zabezpieczania systemów Chmurowych

EK3 Wiedza Efekt kształcenia 3 Student zna podstawowe pojęcia z zakresu bezpieczeństwa systemów Chmurowych

EK4 Umiejętności Efekt kształcenia 4 Student potra przeprowadzic analize zagrożeń bezpieczeństwa systemów Chmurowych

6 Treści programowe

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Wstęp do systemów chmurowych, charakterystyka i własności	2
W2	Łańcuch zaufania w Chmurach, Cloud Controls Matrix	2
W3	Bezpieczeństwo infrastruktury systemów chmurowych	2
W4	Bezpieczeństwo danych i ich przechowywania	2
W5	Tożsamości oraz zarządzania dostępem w Chmurze	2
W6	Bezpieczeństwo w modelu SaaS	2
W7	Bezpieczeństwo w modelu PaaS	2
W8	Bezpieczeństwo w modelu PaaS	2
W9	Zagadnienia prywatności w systemach chmurowych	2
W10	Metody wykrywania zagrożeń oraz ataków na systemy Chmurowe	2
W11	Automatyzacja strategii obronnych w systemach chmurowych	2
W12	Prezentacja praktycznych przykładów wykrywania zagrożeń oraz ataków na systemy Chmurowych w oparciu o analizę metodami sztucznej inteligencji	2
W13	Prezentacja praktycznych przykładów automatyzacja strategii obronnych w systemach chmurowych z wykorzystaniem teorii gier	2

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W14	Międzynarodowe standardy i normy dotyczące zapewniania bezpieczeństwa systemów chmurowych, organy certyfikujące systemy CHmurowe	2
W15	Podsumowanie	2

Laboratorium		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
L1	Wprowadzenie do środowiska CloudSIM. Konfigurowanie projektów, podstawowe definicje. Pierwsza symulacja systemu chmurowego	2
L2	Algorytmy udostępniania tajnego. Implementacja i wdrożenie protokołu Blakleya z 3 przecinającymi się płaszczyznami. Implementacja i wdrożenie protokołu Shamira z 5 tajnymi udziałami	2
L3	Symulacja ataku DDoS. Symulacja, objaśnienie i porównanie metod równoważenia obciążenia: First Fit, Best Fit and Worst Fit.	2
L4	Szyfrowanie oparte na atrybutach: polityka szyfrowania ABE, kluczowe zasady ABE, prezentacja i użycie narzędzi. Szyfrowanie homomorficzne: przykład i implementacja oparta na RSA	2
L5	Struktura Blockchain zapewniająca integralność danych w Edge i Fog Computing	2
L6	Bezpieczeństwo warstwy drugiej sieci. Narzędzia: AAA (Authentication, Authorization, Accounting), RADIUS, TACACS, ARP inspection, Port Security i IP Source Guard	2
L7	Analiza dokumentów bezpieczeństwa pod kątem bezpiecznego i zgodnego z prawem przetwarzania danych w środowiskach chmurowych: ISO 27001, SOC 1, SOC 2,SOC 3, raporty CERT, GDPR	3

7 Narzędzia dydaktyczne

N1 Ćwiczenia laboratoryjne

N2 Dyskusja

N3 Wykłady

N4 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	45
Konsultacje przedmiotowe	5
Egzaminy i zaliczenia w sesji	0
Zaliczenia	2
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	4
Opracowanie wyników	2
Przygotowanie raportu, projektu, prezentacji, dyskusji	2
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**60**
Sumaryczna liczba punktów ECTS dla przedmiotu	2.00

9 Sposoby oceny

Ocena formująca

F1 Ćwiczenie praktyczne

F2 Odpowiedź ustna

F3 Sprawozdanie z ćwiczenia laboratoryjnego

Ocena podsumowująca

P1 Średnia ważona ocen formujących

P2 Test

Warunki zaliczenia przedmiotu

W1 Zaliczenie ćwiczeń mogą uzyskać studenci, którzy regularnie uczęszczali na ćwiczenia

W2 Ocena końcowa jest średnią z ocen P1-P2.

Ocena aktywności bez udziału nauczyciela

B1 Podstawą oceny aktywności bez udziału nauczyciela jest ocena przygotowanego przez studenta sprawozdania z laboratorium

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Student nie potrafi samodzielnie, bądź w grupie wykonać zadań praktycznych. Nie wykonuje poleceń nauczyciela, nie potrafi wykonać poleceń uzgodnionych z grupa.
Na ocenę 3.0	Student potrafi samodzielnie wykonać zadania praktyczne. Student wykonuje polecenia nauczyciela, uczęszcza na zajęcia, potrafi wykonać polecenia uzgodnione z grupą.
Na ocenę 3.5	Student potrafi samodzielnie wykonać zadania praktyczne. Student wykonuje polecenia nauczyciela, uczęszcza na zajęcia, potrafi wykonać polecenia uzgodnione z grupą. Student jest aktywny na zajęciach, bierze udział w dyskusjach grupowych.
Na ocenę 4.0	Student potrafi samodzielnie wykonać zadania praktyczne. Student wykonuje polecenia nauczyciela, uczęszcza na zajęcia, potrafi wykonać polecenia uzgodnione z grupą. Student jest aktywny na zajęciach, bierze udział w dyskusjach grupowych. Student potrafi pracować w małej grupie.
Na ocenę 4.5	Student potrafi samodzielnie wykonać zadania praktyczne. Student wykonuje polecenia nauczyciela, uczęszcza na zajęcia, potrafi wykonać polecenia uzgodnione z grupą. Student jest aktywny na zajęciach, bierze udział w dyskusjach grupowych. Student potrafi kierowac praca małej grupy.
Na ocenę 5.0	Student potrafi samodzielnie wykonać zadania praktyczne. Student wykonuje polecenia nauczyciela, uczęszcza na zajęcia, potrafi wykonać polecenia uzgodnione z grupą. Student jest aktywny na zajęciach, bierze udział w dyskusjach grupowych. Student potrafi kierowac praca małej grupy, potrafi w sposób zrozumiały przedstawiać wyniki jej pracy oraz rozwiązywać w sposób kreatywny powstałe podczas pracy problemy.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie potrafi zasymulować prostego środowiska chmurowego. Student nie potrafi wyjaśnić zagrożeń dotyczących bezpieczeństwa wspomnianych na laboratoriach i wykładach. Student nie potrafi ani użyć ani zaimplementować narzędzi służących do zapewnienia bezpieczeństwa wspomnianych na laboratoriach.
Na ocenę 3.0	Student potrafi zasymulować proste środowisko chmurowe. Student potrafi wyjaśnić zagrożenia dotyczące bezpieczeństwa wspomniane na laboratoriach i wykładach. Student nie potrafi użyć zaawansowanych technik bezpieczeństwa (blockchain, load balancing, ABE, secret sharing, switch security), ale jest w stanie efektywnie użyć podstawowych (haszowanie, szyfrowanie).
Na ocenę 3.5	Student potrafi zasymulować proste środowisko chmurowe. Student potrafi wyjaśnić zagrożenia dotyczące bezpieczeństwa wspomniane na laboratoriach i wykładach. Student nie potrafi użyć zaawansowanych technik bezpieczeństwa (blockchain, load balancing, ABE, secret sharing, switch security), ale jest w stanie efektywnie użyć podstawowych (haszowanie, szyfrowanie). Student potrafi także zaimplementować podstawowe algorytmy dotyczące bezpieczeństwa wspomniane na laboratoriach

Na ocenę 4.0	Student potrafi zasymulować środowisko chmurowe. Student potrafi wyjaśnić zagrożenia dotyczące bezpieczeństwa wspomniane na laboratoriach i wykładach. Student potrafi użyć zaawansowanych technik bezpieczeństwa (blockchain, load balancing, ABE, secret sharing, switch security) oraz podstawowych (haszowanie, szyfrowanie). Student potrafi także zaimplementować podstawowe algorytmy dotyczące bezpieczeństwa wspomniane na laboratoriach.
Na ocenę 4.5	Student potrafi zasymulować środowisko chmurowe. Student potrafi wyjaśnić zagrożenia dotyczące bezpieczeństwa wspomniane na laboratoriach i wykładach. Student potrafi użyć zaawansowanych technik bezpieczeństwa (blockchain, load balancing, ABE, secret sharing, switch security) oraz podstawowych (haszowanie, szyfrowanie). Student potrafi także zaimplementować wszystkie algorytmy dotyczące bezpieczeństwa wspomniane na laboratoriach. Student potrafi dobrać właściwe metody obrony stosownie do ataków wspomnianych na laboratoriach.
Na ocenę 5.0	Student potrafi zasymulować środowisko chmurowe. Student potrafi wyjaśnić zagrożenia dotyczące bezpieczeństwa wspomniane na laboratoriach i wykładach. Student potrafi użyć zaawansowanych technik bezpieczeństwa (blockchain, load balancing, ABE, secret sharing, switch security) oraz podstawowych (haszowanie, szyfrowanie). Student potrafi także zaimplementować wszystkie algorytmy dotyczące bezpieczeństwa wspomniane na laboratoriach. Student potrafi dobrać właściwe metody obrony stosownie do ataków wspomnianych na laboratoriach. Student bardzo dobrze rozumie scenariusze zagrożeń. Potrafi wykonać prosty atak w kontrolowanym środowisku i zademonstrować strategię obrony przed nim.
Efekt kształcenia 3	
Na ocenę 2.0	Student nie zna ogólnych zasad dotyczących zagrożeń bezpieczeństwa oraz zabezpieczania oraz nie potrafi scharakteryzować środowisk chmurowych w kontekście bezpieczeństwa infrastruktury, danych, oraz użytkowników. Student nie potrafi wymienić ani jednego przykładu z ww zagadnień.
Na ocenę 3.0	Student zna ogólne zasady dotyczących zagrożeń bezpieczeństwa oraz zabezpieczania oraz potrafi scharakteryzować środowiska chmurowych w kontekście bezpieczeństwa infrastruktury, danych, oraz użytkowników. Student potrafi wymienić po jednym przykładzie z ww zagadnień,
Na ocenę 3.5	Student zna ogólne zasady dotyczących zagrożeń bezpieczeństwa oraz zabezpieczania oraz potrafi scharakteryzować środowiska chmurowych w kontekście bezpieczeństwa infrastruktury, danych, oraz użytkowników. Potra podać różne przykłady dla każdego wymienionego zagadnienia.
Na ocenę 4.0	Student zna szczegółowo zasady dotyczących zagrożeń bezpieczeństwa oraz zabezpieczania systemów Chmurowych w zależności od modelu Chmury oraz potrafi scharakteryzować środowiska chmurowe w kontekście bezpieczeństwa infrastruktury, danych, oraz użytkowników. Potra podać różne przykłady dla każdego wymienionego zagadnienia.
Na ocenę 4.5	Student zna szczegółowo zasady dotyczących zagrożeń bezpieczeństwa oraz zabezpieczania systemów Chmurowych w zależności od modelu Chmury oraz potrafi scharakteryzować środowiska chmurowe w kontekście bezpieczeństwa infrastruktury, danych, oraz użytkowników. Potra podać oraz rozumie matematyczne podstawy wybranych metod zabezpieczania oraz ich automatyzacji .

Na ocenę 5.0	Student zna szczegółowo zasady dotyczących zagrożeń bezpieczeństwa oraz zabezpieczania systemów Chmurowych w zależności od modelu Chmury, typu zabezpieczanej instrastruktury, typu przesyłanych danych. Student potrafi obszernie scharakteryzować środowiska chmurowe w kontekście zagrożeń bezpieczeństwa .Potra podać oraz rozumie matematyczne podstawy wybranych metod zabezpieczania oraz ich automatyzacji . Student potrafi dobrać metody zabezpieczania ww środowisk do konkretnych przykładów środowisk.
Efekt kształcenia 4	
Na ocenę 2.0	Student nie potrafi zasymulować prostego środowiska chmurowego. Student nie potrafi wyjaśnić zasad ataków na systemy Chmurowe, omawianych na laboratoriach i wykładach. Student nie potrafi ani użyć ani zaimplementować narzędzi służących analizy systemów pod kątem wystąpienia ataków.
Na ocenę 3.0	Student potrafi zasymulować proste środowisko chmurowe. Student potrafi wyjaśnić mechanizmy ataków.
Na ocenę 3.5	Student potrafi zasymulować proste środowisko chmurowe. Student potrafi wyjaśnić mechanizmy ataków. Student potrafi także zaimplementować podstawowe algorytmy ochrony przed atakami na bezpieczeństwo systemó Chmurowych.
Na ocenę 4.0	Student potrafi zasymulować proste środowisko chmurowe. Student potrafi wyjaśnić mechanizmy ataków. Student potrafi także zaimplementować zaawansowane algorytmy ochrony przed atakami na bezpieczeństwo systemó Chmurowych.
Na ocenę 4.5	Student potrafi zasymulować proste środowisko chmurowe. Student potrafi wyjaśnić mechanizmy ataków. Student potrafi także zaimplementować zaawansowane algorytmy ochrony przed atakami na bezpieczeństwo systemó Chmurowych. Student potrafi prawidłowo dobrac metody ochrony do konkretnego środowiska Chmurowego.
Na ocenę 5.0	Student potrafi zasymulować proste środowisko chmurowe. Student potrafi wyjaśnić mechanizmy ataków. Student potrafi także zaimplementować zaawansowane algorytmy ochrony przed atakami na bezpieczeństwo systemó Chmurowych. Student potrafi prawidłowo dobrac metody ochrony do konkretnego środowiska Chmurowego. Syudent potrafi przeprowadzic analizę wybranego ataku na bezpieczeństwo systemu Chmurowego.

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1	I2_K01 I2_K04	Cel 1 Cel 2	W1 W2 W12 W14 W15	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK2	I2_U07 I2_U08	Cel 1 Cel 2	W1 W2 W3 W4 W5 W6 W7 W8 W9 W10 W11 W12 W13 W14 W15	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK3	I2_W01 I2_W02	Cel 1 Cel 2	W1 W2 W3 W4 W5 W6 W7 W8 W9 W10 W11 W12 W13 W14 W15	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK4	I2_U11 I2_U12	Cel 1 Cel 2	W1 W2 W3 W4 W5 W6 W7 W8 W9 W10 W11 W12 W13 W14 W15	N1 N2 N3 N4	F1 F2 F3 P1 P2

11 Wykaz literatury

Literatura podstawowa

[1] Imad M. Abbadi — *CLOUD MANAGEMENT AND SECURITY*, -, 0, -

[2] Tim Mather, Subra Kumaraswamy, and Shahed Latif — *Cloud Security and Privacy*, -, 0, -

[3] Cloud Security Alliance — *Cloud Controls Matrix*, -, 0, -

Literatura uzupełniająca

[1] THE OFFICIAL SITE OF CLOUD SIM — *CLOUD SIM*, -, 0, -

[2] www.cloudsim.com — *CLOUDSIM PLUS - A modern, full-featured, highly extensible and easier-to-use Java 8+ Framework for Modeling and Simulation of Cloud Computing Infrastructures and Services*, -, 0, -

[3] John Bethencourt, Amit Sahai, and Brent Waters. — *CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION*, -, 0, -

[4] Saily Satish Ghodke. — *LOAD BALANCING AND VIRTUAL MACHINE ALLOCATION IN CLOUD-BASED DATA CENTERS*, -, 0, -

[5] Shreshth Tuli, Redowan Mahmud, Shikhar Tuli, and Rajkumar Buyya — *FOGBUS: A BLOCKCHAIN-BASED LIGHTWEIGHT FRAMEWORK FOR EDGE AND FOG COMPUTING*, -, 0, -

[6] CISCO — *CISCO CONFIGURATION GUIDE*, -, 0, -

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr Agnieszka Jakóbik (kontakt: akrok@pk.edu.pl)

Osoby prowadzące przedmiot

1 Dr Agnieszka Jakóbik (kontakt: ajakobik@pk.edu.pl)

2 mgre Jacek Tchórzewski (kontakt: jacek.tchorzewski@pk.edu.pl)

13 Zatwierdzenie karty przedmiotu do realizacji

(miejscowość, data) (odpowiedzialny za przedmiot) (dziekan)

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .

. . . . . .