KARTA PRZEDMIOTU DLA NABORU 2020-2021

INFORMACJE OGÓLNE

1. **Nazwa przedmiotu kształcenia**
   BEZPIECZEŃSTWO W CHMURZE
2. **Nazwa jednostki prowadzącej moduł** Zakład Informatyki
3. **Grupa treści kształcenia** treści kształcenia kierunkowego
4. **Typ przedmiotu** obowiązkowy
5. **Poziom studiów** studia pierwszego stopnia
6. **Liczba punktów ECTS** 5
7. **Poziom przedmiotu** zaawansowany
8. **Rok studiów, semestr** IV rok, semestr VII
9. **Liczba godzin w semestrze** laboratoria 15h, wykłady 30 h
10. **Język wykładowy:** polski
11. **Wykładowca (wykładowcy)**
    Marcin Klimek, dr inż. m.klimek@dydaktyka.pswbp.pl

INFORMACJE SZCZEGÓŁOWE

12. Wymagania wstępne

1. Posiadanie podstawowej wiedzy na temat bezpieczeństwa danych, kryptologii i sieci komputerowych.
2. Posiadanie podstawowej wiedzy z zakresu administracji systemami komputerowymi.

13. Cele przedmiotu

C1. nabycie umiejętności tworzenia bezpiecznych rozwiązań chmurowych

C2. zapoznanie z aktualnymi trendami dotyczącymi zabezpieczeń systemów i aplikacji w chmurze

C3. Zapoznanie z ryzykami związanymi z umieszczaniem danych w chmurze obliczeniowej

14. Efekty uczenia się w zakresie wiedzy, umiejętności i kompetencji społecznych

Student, który zaliczył przedmiot potrafi:	odniesienie do kierunkowych efektów uczenia się
WIEDZA	
EU01 zna normy i standardy tworzenia bezpiecznych rozwiązań chmurowych	I1P_W05 I1P _W20 I1P_W21 I1P_W26
EU02 zna aktualne metody oraz trendy w sposobach zabezpieczeń rozwiązań chmurowych	
EU03 zna zagrożenia występujące przy stosowaniu rozwiązań chmurowych	
UMIEJĘTNOŚCI	
EU04 umie zastosować istniejące rozwiązania i produkty do ochrony danych i systemów w chmurze	I1P _U06 I1P_U14 I1P_U17 I1P_U25 I1P_U29 I1P_U30
EU05 umie przeprowadzić podstawową konfigurację popularnych platform chmurowych	
EU06 potrafi przeprowadzić ocenę bezpieczeństwa i niezawodności aplikacji lub systemu informatycznego w chmurze	
KOMPETENCJE SPOŁECZNE	
EU07 rozumie znaczenie i potrzebę śledzenia bieżącej wiedzy z zakresu bezpieczeństwa rozwiązań chmurowych	I1P_K01

15. Treści programowe

Forma zajęć – wykłady

Standardowe zasady i pojęcia znajdujące zastosowanie w środowisku w chmurze. Normy i standardy rozwiązań chmurowych.
Infrastruktura bezpiecznych rozwiązań chmurowych. Strategie ochrony danych.
Techniki dotyczące zabezpieczania popularnych platform środowisk w chmurze, takich jak Amazon Web Services, Microsoft Azure i IBM Cloud.
Najlepsze praktyki dotyczące bezpieczeństwa środowisk w chmurze. Najlepsze wzorce dla aplikacji w

chmurze.
Niezawodność chmur obliczeniowych. Kwestie dotyczące prywatności i bezpieczeństwa danych, aspekty prawne związane z lokalizacją danych.
Sposoby zarządzania dostawcami środowiska w chmurze, przechowującymi, przetwarzającymi dane lub zapewniającymi kontrolę administracyjną.
Tożsamość i zarządzanie zasobami IAM (ang. Identity and Access Management) w chmurze. Autentykacja.
Sposoby zarządzania różnego rodzaju zagrożeniami. Monitorowanie i audyt bezpieczeństwa.

Forma zajęć – laboratoria

Analiza możliwości ataku na system / aplikację umieszczoną w chmurze na przykładach.
Przykładowe ataki na systemy w chmurze.
Konfiguracja zabezpieczeń w popularnych platformach chmurowych tj. w Amazon Web Services, Microsoft Azure i IBM Cloud. Autentykacja, kontrola dostępu itp.
Analiza ryzyka systemów informatycznych w chmurze.
Projekt bezpieczeństwa wskazanego systemu w chmurze obliczeniowej: studenci przygotowują analizę bezpieczeństwa i niezawodności wskazanego systemu informatycznego umieszczonego w chmurze obliczeniowej oraz opracowują plan jego poprawy.

16. Narzędzia/metody dydaktyczne

1. Podczas laboratoriów praca indywidualna studentów. Studenci samodzielnie rozwiązują zadany problem praktyczny, dobierając odpowiednie narzędzia .
2. Laboratoria w części odbywają się przy tablicy: studenci np. analizują różne strategie dotyczące bezpieczeństwa danych chmurze.
3. Wykład prowadzony z wykorzystaniem projektora multimedialnego. Wykłady przygotowane w formie prezentacji PowerPoint.
4. Treści prezentowane na wykładzie są wzbogacone o pokazy praktycznych rozwiązań odnoszących się do prezentowanych zagadnień.

17. Sposoby oceny (F – formująca; P – podsumowująca)

F1. Kolokwium przy komputerze ze znajomości Amazon Web Services, Microsoft Azure i IBM Cloud.
F2. Kartkówki na laboratoriach
F3. Ocena realizacji projektu zaliczeniowego. Projekt wykonywany w zespołach 2-3 osobowych.
F4. Ocena ciągła pracy indywidualnej podczas laboratoriów.
P1. Egzamin w formie pisemnej sprawdzający wiedzę z wykładów i laboratoriów

18. Obciążenia pracą studenta

forma aktywności	średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem*	30+15
Przygotowanie się do zajęć	20
Przygotowanie projektu zaliczeniowego	40
Przygotowanie do egzaminu	20
SUMA	125
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	5

19. Literatura podstawowa i uzupełniająca

Literatura podstawowa:

1) Mateos A.: Rosenberg J.: Chmura obliczeniowa. Rozwiązania dla biznesu. Helion, Gliwice, 2011.
2) Białas A.: BEZPIECZEŃSTWO INFORMACJI I USŁUG W NOWOCZESNEJ INSTYTUCJI I FIRMIE, WNT 2017.
3) Dotson Ch.: Bezpieczeństwo w chmurze: Przewodnik po projektowaniu i wdrażaniu zabezpieczeń, PWN 2020.
4) Franklin Curtis, Chee Brian: Securing the Cloud, Taylor and Francis, 2019.

Literatura uzupełniająca:

1) Fryźlewicz Z., Nikończuk D.: Windows Azure : wprowadzenie do programowania w chmurze. Gliwice : Wydawnictwo Helion, 2012.
2) Chu-Carroll Mark C.: Google App Engine : kod w chmurze, Gliwice : Wydawnictwo Helion, 2012.
3) Erl Thomas: Cloud Computing Design Patterns, Pearson, 2019.

20. Formy oceny – szczegóły

Warunki uzyskania zaliczenia przedmiotu: zajęcia kończą się zaliczeniem z oceną.

Sposób weryfikacji efektów uczenia się:

Ocena stopnia osiągniętych przez studenta efektów uczenia się następuje wg poniższych kryteriów:

5.0 – zakładany efekt uczenia się został osiągnięty bez zastrzeżeń

4.5 – zakładany efekt uczenia się został osiągnięty z pojedynczymi brakami/błędami

4.0 – zakładany efekt uczenia się został osiągnięty z nielicznymi brakami/błędami

3.5 – zakładany efekt uczenia się został osiągnięty z wieloma brakami/błędami

3.0 – zakładany efekt kształcenia został osiągnięty z licznymi i istotnymi brakami/błędami (minimalnie wymagany poziom osiągnięcia efektu)

2.0 – zakładany efekt uczenia się nie został osiągnięty

21. Inne przydatne informacje o przedmiocie
1. Bezpośrednich informacji o problematyce zajęć i treściach programowych udziela prowadzący w trakcie zajęć i podczas konsultacji
2. Zajęcia odbywać się będą w PSW w Białej Podlaskiej
3. Zajęcia odbywać się będą zgodnie z aktualnym planem zajęć
4. Konsultacje odbywać się będą zgodnie z obowiązującym terminarzem

* Zajęcia prowadzone z bezpośrednim udziałem nauczyciela akademickiego lub innej osoby prowadzącej zajęcia oraz konsultacje