

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

KARTA OPISU PRZEDMIOTU

| | | | |
|------------------------|-----------|--|------------------|
| Wydział | | Informatyki | |
| Kierunek | | Informatyka | |
| Specjalność | | Cyberbezpieczeństwo | |
| Semestr | VI | Program studiów, dla którego obowiązuje sylabus | 2024/2025 |
| Stopień studiów | I | | |

| | | | | |
|----------------------|--|------|----------------|----------------|
| Nazwa przedmiotu | Bezpieczeństwo chmury i systemów rozproszonych | | | |
| Kod przedmiotu | BCISR | | | |
| Łączna liczba godzin | 30 | Tryb | stacjonarny | niestacjonarny |
| Profil kształcenia | Ogólnoakademicki (A) | | Praktyczny (P) | |
| Forma zajęć | laboratorium | | | |
| Język przedmiotu | polski | | | |
| Liczba punktów ECTS | 2 | | | |

| Prowadzący zajęcia | |
|---------------------------------|---------------------|
| Forma prowadzonych zajęć | Laboratorium |
| Wymiar zajęć | 30 h |
| Stopień (tytuł) naukowy | |
| Imię | |
| Nazwisko | |

| | |
|------------------------------------|---|
| Wymagania wstępne | Podstawowa wiedza z zakresu informatyki i technologii informacyjnych, umiejętność obsługi systemów operacyjnych Windows i Linux, znajomość podstaw programowania i algorytmiki oraz podstawowych zasad działania sieci komputerowych. |
| Założenia i cele przedmiotu | Przedmiot skupia się na bezpieczeństwie środowisk chmurowych i rozproszonych, omawiając modele usług (IaaS, PaaS, SaaS), zagrożenia specyficzne dla chmury, mechanizmy zabezpieczające dane i aplikacje, a także wymagania prawne i compliance (np. RODO). Studenci nauczą się konfigurować zabezpieczenia w wybranych platformach chmurowych, zarządzać tożsamością i dostępem oraz stosować konteneryzację dla poprawy bezpieczeństwa i skalowalności systemów rozproszonych. |
| Metody dydaktyczne | <ol style="list-style-type: none"> 1. Prezentacje multimedialne. 2. Pokazy przykładowych rozwiązań problemów. 3. Rozwiązywanie zadań praktycznych. |

| Efekty uczenia się (odniesienie do charakterystyk poziomów Polskiej Ramy Kwalifikacji) | | Odniesienie do efektów dla kierunku | Odniesienie do efektów uczenia się wg Polskiej Ramy Kwalifikacji |
|---|---|--|---|
| WIEDZA – absolwent zna i | W01. Koncepcje, modele i usługi chmurowe oraz ich wpływ na projektowanie i bezpieczeństwo | K_W16 | P6S_WG P6S_WK |

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

| | | | |
|--|---|--|---|
| rozumie: | <p>systemów informatycznych.</p> <p>W02. Metody zabezpieczania danych w chmurze oraz sposoby kontroli dostępu i ochrony komunikacji w środowiskach rozproszonych.</p> <p>W03. Społeczne i regulacyjne aspekty bezpieczeństwa w chmurze, w tym kwestie prywatności, zgodności z RODO i innymi przepisami.</p> <p>W04. Zasady monitorowania, diagnozowania i optymalizacji aplikacji działających w chmurze, uwzględniając aspekty bezpieczeństwa i dostępności.</p> <p>W05. Technologie konteneryzacji (Docker) i narzędzia orkiestracji (Kubernetes) oraz ich wpływ na bezpieczeństwo, skalowalność i zarządzanie zasobami w środowiskach rozproszonych.</p> | <p>K_W19</p> <p>K_W23</p> <p>K_W26</p> | P6S_WG_INŻ |
| UMIEJĘTNOŚCI – absolwent potrafi: | <p>U01. Pozyskiwać i interpretować informacje z dokumentacji, raportów oraz literatury branżowej, aby stosować najnowsze praktyki bezpieczeństwa w chmurze i systemach rozproszonych.</p> <p>U02. Wdrażać, konfigurować oraz zarządzać aplikacjami i zasobami w chmurach obliczeniowych, uwzględniając aspekty bezpieczeństwa i zgodności z regulacjami.</p> <p>U03. Stosować mechanizmy szyfrowania danych w spoczynku i w transzycie oraz zarządzać kontrolą dostępu w środowisku chmurowym i systemach rozproszonych.</p> <p>U04. Tworzyć i konfigurować kontenery oraz korzystać z narzędzi orkiestracji (Kubernetes) w celu zapewnienia skalowalności i bezpieczeństwa usług w środowisku rozproszonym.</p> <p>U05. Wykorzystywać metody analityczne i modele do oceny ryzyka, planowania zabezpieczeń i projektowania architektur bezpieczeństwa w chmurze.</p> | <p>K_U01</p> <p>K_U02</p> <p>K_U03</p> <p>K_U04</p> <p>K_U06</p> <p>K_U12</p> <p>K_U18</p> <p>K_U24</p> <p>K_U25</p> | <p>P6S_UW</p> <p>P6S_UW_INŻ</p> <p>P6S_UO</p> <p>P6S_KK</p> <p>P6S_UK</p> |
| KOMPETENCJE SPOŁECZNE – absolwent jest gotów do | <p>K01. Pracy w zespole, przyjmując w nim różne role.</p> <p>K02. Krytycznej oceny możliwości urządzeń sieciowych i systemów i dostępnych na rynku IT.</p> <p>K03. Ciągłego samokształcenia się w celu dostosowywania się do dynamicznie zmieniających się technologii.</p> | <p>K_K04</p> <p>K_K05</p> <p>K_K06</p> | <p>P6S_UO</p> <p>P6S_KR</p> <p>P6S_KK</p> |

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

| Lp. | Tematyka zajęć | Liczba godzin |
|-----------------------------------|--|---------------|
| Forma zajęć – laboratorium | | |
| 1 | Wprowadzenie do chmury obliczeniowej. Modele usług (IaaS, PaaS, SaaS), modele wdrożenia (publiczna, prywatna, hybrydowa). | 4 |
| 2 | Zagrożenia i wyzwania bezpieczeństwa w chmurze. Charakterystyka zagrożeń, odpowiedzialność dostawcy i klienta. | 6 |
| 3 | Mechanizmy zabezpieczające w chmurze. Szyfrowanie danych w spoczynku i w tranzycie, zarządzanie tożsamością i dostępem (IAM). | 6 |
| 4 | Bezpieczeństwo systemów rozproszonych. Synchronizacja danych, integralność, dostępność w środowiskach rozproszonych. | 6 |
| 5 | Compliance i regulacje prawne. RODO, zgodność z przepisami, audyty bezpieczeństwa w chmurze. | 4 |
| 6 | Praktyczne ćwiczenia z wykorzystaniem usług chmurowych. Konfiguracja zabezpieczeń w AWS/Azure/GCP, scenariusze awaryjne. Zaliczenie. | 4 |

| | | |
|---|--|---|
| Forma i warunki zaliczenia przedmiotu | Wykonanie projektów. Częstkowe prezentacje, zdawanie raportów, obrona projektów. | |
| Metody weryfikacji efektów uczenia się | | Nr efektu uczenia się z sylabusu |
| | Ocena projektów i częściowych prezentacji. | W01-W05, U01-U05, K01-K03 |

| | |
|---------------------------------|---|
| Literatura podstawowa | <ol style="list-style-type: none"> 1. M. Kief, <i>Infrastruktura jako kod. Dynamiczne systemy w epoce chmury</i>, APN Promise 2021. 2. S. Kane, K. Matthias, <i>Docker. Praktyczne zastosowania</i>, Helion, Gliwice 2019. 3. B. Burns, J. Beda, K. Hightower, <i>Kubernetes. Tworzenie niezawodnych systemów rozproszonych</i>, Helion, Gliwice 2020. 4. S. A. Tanebaum, M. Steen, <i>Systemy rozproszone Zasady i paradygmaty</i>, WNT, Warszawa 2006. 5. R. Kurose, <i>Sieci komputerowe. Ujęcie całościowe</i>, Helion, Gliwice 2017. 6. W. Kabaciński, M. Żal, <i>Sieci telekomunikacyjne</i>, Warszawa 2008. 7. D. E. Comer, <i>Sieci komputerowe i intersieci</i>, Helion, Gliwice 2012. 8. W. Stallings, <i>Kryptografia i bezpieczeństwo sieci komputerowych: matematyka szyfrów i techniki kryptologii</i>, Helion, Gliwice 2012. 9. E. Cole, R. Krutz, J. Conle, <i>Bezpieczeństwo sieci: biblia</i>, Helion, Gliwice 2005. |
| Literatura uzupełniająca | <ol style="list-style-type: none"> 1. C. Dotson, <i>Bezpieczeństwo w chmurze</i>, Helion, Gliwice 2020. 2. M. Krief, <i>DevOps w praktyce. Wdrażanie narzędzi Terraform, Azure DevOps, Kubernetes i Jenkins</i>, Helion, Gliwice 2023. |

AKADEMIA TECHNICZNO-INFORMATYCZNA W NAUKACH STOSOWANYCH

| Nakład pracy studenta | |
|---|---------------|
| | Liczba godzin |
| Zajęcia dydaktyczne | 30 |
| Przygotowanie się do zajęć | 5 |
| Studiowanie literatury | 5 |
| Udział w konsultacjach | 2 |
| Przygotowanie projektu / eseju / prezentacji itp. | 18 |
| Przygotowanie się do egzaminu / zaliczenia | - |
| Inne | - |
| ŁĄCZNY nakład pracy studenta w godz. | 60 |
| Liczba punktów ECTS | 2 |