

WROCŁAWSKA WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ

KARTA OPISU PRZEDMIOTU

| | | | |
|------------------------|-----------|--|------------------|
| Wydział | | Informatyki | |
| Kierunek | | Informatyka | |
| Specjalność | | Bezpieczeństwo systemów komputerowych | |
| Semestr | VI | Program studiów, dla którego obowiązuje sylabus | 2023/2024 |
| Stopień studiów | I | | |

| | | | | |
|----------------------|----------------------|------|----------------|----------------|
| Nazwa przedmiotu | Walidacja sieci | | | |
| Kod przedmiotu | WS | | | |
| Łączna liczba godzin | 18 | 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 | 18 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 ma za zadanie zapoznanie studentów z procesami walidacji i testowania sieci w celu oceny ich bezpieczeństwa, wydajności i zgodności z założeniami. Obejmuje planowanie procesu walidacji, wykorzystanie specjalistycznych narzędzi (Wireshark, Nmap, Metasploit), przeprowadzanie audytów bezpieczeństwa, analizę oraz interpretację wyników testów, a także formułowanie rekomendacji i planów naprawczych. |
| 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 rozumie: | W01.Cele oraz metody walidacji i testowania sieci. W02.Narzędzia do testowania sieci takie jak Wireshark, Nmap, Metasploit. | K_W16 | P6S_WG P6S_WG_INŻ |

WROCŁAWSKA WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ

| | | | |
|--|--|--|---|
| | <p>W03. Zasady przeprowadzania audytów bezpieczeństwa sieci, identyfikacji podatności i raportowania wyników.</p> <p>W04. Metody analizy i interpretacji wyników testów, w tym ocenę ryzyka i priorytetyzację działań.</p> <p>W05. Sposoby tworzenia rekomendacji i planów naprawczych po przeprowadzonej walidacji sieci.</p> | | |
| UMIEJĘTNOŚCI – absolwent potrafi: | <p>U01. Zaplanować i przeprowadzić proces walidacji sieci z uwzględnieniem wyznaczonych celów.</p> <p>U02. Wykorzystać narzędzia takie jak Wireshark, Nmap, Metasploit do testowania i diagnozowania sieci.</p> <p>U03. Przeprowadzić audyt bezpieczeństwa sieci, zidentyfikować podatności oraz sporządzić dokumentację i raport końcowy.</p> <p>U04. Analizować wyniki testów, oceniać ryzyko oraz wskazywać priorytety działań korygujących.</p> <p>U05. Przygotować rekomendacje oraz opracować plan działań naprawczych, a następnie nadzorować ich realizację.</p> | <p>K_U01 K_U02 K_U03 K_U04 K_U08 K_U09 K_U13 K_U17 K_U18</p> | <p>P6S_UW P6S_UW_INŻ P6S_UO P6S_KK 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 K_K05 K_K06</p> | <p>P6S_UO P6S_KR P6S_KK</p> |

| Lp. | Tematyka zajęć | Liczba godzin |
|-----------------------------------|---|---------------|
| Forma zajęć – laboratorium | | |
| 1 | Metody walidacji i testowania sieci. Cele walidacji; rodzaje testów; planowanie procesu walidacji. | 2 |
| 2 | Narzędzia do testowania sieci. Wykorzystanie narzędzi takich jak Wireshark, Nmap, Metasploit. | 4 |
| 3 | Audyt bezpieczeństwa sieci. Przeprowadzanie audytów; identyfikacja podatności; raportowanie. | 4 |
| 4 | Analiza i interpretacja wyników testów. Ocena ryzyka; priorytetyzacja działań naprawczych. | 4 |
| 5 | Tworzenie rekomendacji i planów naprawczych. Opracowanie strategii poprawy bezpieczeństwa na podstawie wyników walidacji. Zaliczenie. | 4 |

WROCŁAWSKA WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ

| | | |
|---|--|---|
| 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. R. Kurose, <i>Sieci komputerowe. Ujęcie całościowe</i>, Helion, Gliwice 2017. 2. W. Kabaciński, M. Żal, <i>Sieci telekomunikacyjne</i>, Warszawa 2008. 3. D. E. Comer, <i>Sieci komputerowe i intersieci</i>, Helion, Gliwice 2012. 4. W. Stallings, <i>Kryptografia i bezpieczeństwo sieci komputerowych: matematyka szyfrów i techniki kryptologii</i>, Helion, Gliwice 2012. 5. E. Cole, R. Krutz, J. Conle, <i>Bezpieczeństwo sieci: biblia</i>, Helion, Gliwice 2005. |
| Literatura uzupełniająca | <ol style="list-style-type: none"> 1. S. A. Tanenbaum, M. Steen, <i>Systemy rozproszone Zasady i paradygmaty</i>, WNT, Warszawa 2006. 2. B. Dunsmore, T. Skandier, <i>Cisco, technologie telekomunikacyjne</i>, MIKOM, Warszawa 2008. |

| Nakład pracy studenta | |
|---|---------------|
| | Liczba godzin |
| Zajęcia dydaktyczne | 18 |
| Przygotowanie się do zajęć | 9 |
| Studiowanie literatury | 9 |
| Udział w konsultacjach | 2 |
| Przygotowanie projektu / eseju / prezentacji itp. | 22 |
| Przygotowanie się do egzaminu / zaliczenia | - |
| Inne | - |
| ŁĄCZNY nakład pracy studenta w godz. | 60 |
| Liczba punktów ECTS | 2 |