|  |  |  |
| --- | --- | --- |
| Akademia_logo (4) | **Wydział** | Techniczny |
| **Kierunek** | Informatyka |
| **Poziom studiów** | drugiego stopnia |
| **Forma studiów** | stacjonarna/niestacjonarna |
| **Profil studiów** | praktyczny |
| **Pozycja w planie studiów (lub kod przedmiotu)** | C.4.1 |

**KARTA ZAJĘĆ**

**1. Informacje ogólne**

|  |  |
| --- | --- |
| Nazwa zajęć | Etyczny haker |
| Punkty ECTS | 4 |
| Rodzaj zajęć | ~~obowiązkowe~~/obieralne |
| Moduł/specjalizacja | Cyberbezpieczeństwo |
| Język, w którym prowadzone są zajęcia | Polski/Angielski |
| Rok studiów | 1 |
| Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia | dr inż. Łukasz Lemieszewski, mgr inż. Robert Suchocki |

**2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze**

|  |  |  |  |
| --- | --- | --- | --- |
| **Forma zajęć** | **Liczba godzin****Stacjonarne/niestacjonarne** | **Rok studiów/semestr** | **Punkty ECTS** (zgodnie z programem studiów) |
| **wykład** | **15/10** | **1/2;** | **4** |
| **laboratoria** | **30/18** | **1/2;** |
| **projekt** | **15/10** | **1/2;** |

**3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć**

|  |
| --- |
| Student przedmiotu Zarządzanie bezpieczeństwem w systemach sieciowych posiada wiedzę, umiejętności i kompetencje społeczne, które nabył podczas realizacji przedmiotu wprowadzenie do sieci komputerowych, routing i przełączanie w sieciach LAN i WAN, cyberbezpieczeństwo |

**4. Cele kształcenia**

|  |
| --- |
| C1 - Zrozumienie zasad etycznego hakowania i odpowiedzialnego ujawniania luk w zabezpieczeniach. Poznanie kodeksów postępowania dla etycznych hakerówC2 - Rozwijanie umiejętności technicznych w zakresie testów penetracyjnych. Poznanie metod skanowania i analizy luk w zabezpieczeniach. Zapoznanie się z narzędziami do testów penetracyjnych. Rozwijanie umiejętności przeprowadzania testów penetracyjnych w sposób etyczny i odpowiedzialnyC3 - Kształtowanie umiejętności komunikacji i współpracy z organizacjami. Nauczenie się tworzenia raportów z wyników testów penetracyjnych. Rozwijanie umiejętności prezentacji wyników testów penetracyjnych dla decydentów |

**5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych**

|  |  |  |
| --- | --- | --- |
| **Symbol efektu uczenia się** | **Opis efektu uczenia się** | **Odniesienie do efektu kierunkowego** |
| **WIEDZA** |
| W\_01 | Student ma elementarną wiedzę z zakresu podstaw informatyki obejmującą bezpieczeństwo danych i systemów komputerowych oraz bezpieczeństwo aplikacji. | K\_W03 |
| W\_02 | Student orientuje się w obecnym stanie oraz trendach rozwojowych bezpieczeństwa systemów i sieci teleinformatycznych | K\_W08 |
| **UMIEJĘTNOŚCI** |
| U\_01 | Student potrafi ocenić ryzyko i bezpieczeństwo baz danych, aplikacji internetowych, systemów i sieci komputerowych, stosując techniki oraz narzędzia sprzętowe i programowe. | K\_U04K\_U05 |
| U\_02 | Student potrafi zaplanować i przeprowadzić symulację oraz przeprowadzić eksperyment pomiarowy z zakresu bezpieczeństwa systemów; potrafi przedstawić otrzymane wyniki w formie liczbowej oraz dokonać ich interpretacji i wyciągnąć właściwe wnioski | K\_U11 |
| **KOMPETENCJE SPOŁECZNE** |
| K\_01 | Student prawidłowo identyfikuje i rozstrzyga dylematy Cyberbezpieczeństwa. | K\_K02 |

**6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć** (zgodnie z programem studiów):

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści wykładów**  | **Liczba godzin na studiach** |
| **stacjonarnych** | **stacjonarnych** |
| W1 | Wprowadzenie do etycznego hakowania i testów penetracyjnych | 2 | 2 |
| W2 | Planowanie i określanie zakresu oceny testów penetracyjnych | 2 | 1 |
| W3 | Gromadzenie informacji i skanowanie luk w zabezpieczeniach | 2 | 2 |
| W4 | Ataki socjotechniczne | 2 | 1 |
| W5 | Wykorzystanie podatności sieci przewodowych i bezprzewodowych | 2 | 1 |
| W6 | Wykorzystywanie luk w zabezpieczeniach aplikacji | 2 | 1 |
| W7 | Bezpieczeństwo chmury, urządzeń mobilnych i IoT. Wykonywanie technik poeksploatacyjnych | 2 | 1 |
| W8 | Raportowanie i komunikacja. Narzędzia do testów penetracyjnych  | 1 | 1 |
|  | **Razem liczba godzin wykładów**  | **15** | **10** |

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści laboratoriów** | **Liczba godzin na studiach** |
| **stacjonarnych** | **stacjonarnych** |
| L1 | 1.1.3 Laboratorium - Badanie karier w dziedzinie pentestingu 1.2.6 Laboratorium - Porównanie metodologii pentestingu1.3.6 Laboratorium - Wdrażanie gotowej maszyny wirtualnej Kali Linux 1.3.7 Laboratorium - Badanie systemu Kali Linux  | 2 | 1 |
| L2 | 2.1.9 Laboratorium - Wymagania zgodności i lokalne ograniczenia2.2.10 Laboratorium - Tworzenie umowy pentestingowej2.2.9 Laboratorium - Zakres i planowanie przed zaangażowaniem2.3.3 Laboratorium - Osobisty kodeks postępowania | 2 | 1 |
| L3 | 3.1.12 Laboratorium - Gromadzenie informacji o pracownikach3.1.14 Laboratorium - Znajdowanie informacji z certyfikatów SSL | 2 | 1 |
| L4 | 3.1.18 Laboratorium - Uzyskiwanie informacji o organizacji3.1.19 Laboratorium - Wyszukiwanie zaawansowane | 2 | 1 |
| L5 | 3.1.20 Laboratorium - Wyszukiwanie Shodan3.1.4 Laboratorium - Korzystanie z narzędzi OSINT | 2 | 1 |
| L6 | 3.1.9 Laboratorium - Wyszukiwanie DNS3.2.11 Laboratorium - Podsłuchiwanie sieci za pomocą Wireshark  | 2 | 1 |
| L7 | 3.2.6 Laboratorium - Enumeracja za pomocą Nmap 3.2.9 Laboratorium - Tworzenie pakietów za pomocą Scapy  | 2 | 1 |
| L8 | 3.3.6 Laboratorium - Skanowanie podatności za pomocą Kali Tools 3.4.3 Laboratorium - Badanie źródeł informacji o podatnościach  | 2 | 1 |
| L9 | 4.4.7 Laboratorium - Poznaj zestaw narzędzi do inżynierii społecznej4.4.8 Laboratorium - Korzystanie z Browser Exploitation Framework (BeEF) | 2 | 1 |
| L10 | 5.1.16 Laboratorium - Ataki na ścieżce przy użyciu Ettercap5.1.4 Laboratorium - Skanowanie w poszukiwaniu luk w zabezpieczeniach SMB przy użyciu enum4linux | 2 | 1 |
| L11 | 6.1.7 Laboratorium - Skanowanie podatności sieci Web 6.1.8 Laboratorium - Korzystanie ze skanera podatności GVM  | 2 | 1 |
| L12 | 6.12.13 Laboratorium - Korzystanie z przewodnika OWASP Web Security Testing Guide - ILM.docx6.4.7 Laboratorium - Ataki iniekcyjne - ILM.docx | 2 | 1 |
| L13 | 6.5.8 Laboratorium - Korzystanie z narzędzi haseł 6.7.8 Laboratorium - Cross Site Scripting  | 2 | 1 |
| L14 | 9.1.9 Laboratorium - Przeglądanie raportów z testów penetracyjnych9.2.7 Laboratorium - rekomendowanie środków zaradczych na podstawie wyników | 2 | 1 |
| L15 | 10.1.19 Laboratorium - Analiza kodu exploita 10.1.20 Laboratorium - Analiza kodu automatyzacji  | 2 | 1 |
|  | **Razem liczba godzin laboratoriów** | **30** | **18** |

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści wykładów**  | **Liczba godzin na studiach** |
| **stacjonarnych** | **stacjonarnych** |
| W1 | Planowanie testów penetracyjnych. Zakres planowania testów. | 2 | 2 |
| W2 | Rozpoznanie środowiska testowanego. | 2 | 1 |
| W3 | Faza Ataku na sieci przewodowe. | 2 | 2 |
| W4 | Faza ataku na sieci bezprzewodowe | 2 | 1 |
| W5 | Tworzenie raportów - podsumowanie techniczne pentestu. | 2 | 1 |
| W6 | Zestawienie wykrytch podatosci i luk w zabezpieczeniach. | 2 | 1 |
| W7 | Zestawienie wykrytch podatosci i luk w zabezpieczeniach. | 2 | 1 |
| W8 | Prezentacja projektu. | 1 | 1 |
|  | **Razem liczba godzin wykładów**  | **15** | **10** |

**7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć**

|  |  |  |
| --- | --- | --- |
| **Forma zajęć** | **Metody dydaktyczne (wybór z listy)** | **Środki dydaktyczne** |
| Wykład | M1, M2 - wykład informacyjny jako prelekcja z objaśnieniami połączone z dyskusją oraz możliwością prezentacji prac własnych zrealizowanych jako prezentacje z przeglądu literatury | projektor, dostęp do Internetu,prezentacja multimedialna |
| Laboratoria | M5 - ćwiczenia doskonalące umiejętność pozyskiwania informacji ze źródeł internetowych i doskonalących obsługę narzędzi informatycznych  | Komputer z środowiskiem GNS3 oraz dostępem do Internetu, Urządzenia sieciowe zgodnie ze specyfikacją CCNA Security |
| Projekt | M5 - ćwiczenia doskonalące umiejętność pozyskiwania informacji ze źródeł internetowych i doskonalących obsługę narzędzi informatycznych oraz obrona projektu końcowego. | Komputer z środowiskiem GNS3 oraz dostępem do Internetu, Urządzenia sieciowe zgodnie ze specyfikacją CCNA Security |

**8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta**

**8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć**

|  |  |  |
| --- | --- | --- |
| **Forma zajęć** | **Ocena formująca (F)** **–** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)** | **Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)** |
| Wykład | F1 - sprawdzian pisemny (kolokwium cząstkowe testy z pytaniami wielokrotnego wyboru i pytaniami otwartymi)  | P1 – egzamin pisemny w formie pytań testowych |
| Laboratoria | F2 – obserwacja/aktywność (przygotowanie do zajęć, ocena ćwiczeń wykonywanych podczas zajęć), F5 - ćwiczenia praktyczne (ćwiczenia z wykorzystaniem sprzętu i oprogramowania fachowego) | P2 – kolokwium praktyczne  |
| Projekt | F3 – dokumentacja projektu F4 – wystąpienie – analiza projektu | P4 – praca pisemna - projekt |

**8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x”)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Symbol efektu** | Wykład | Laboratoria | Projekt |
| F1 | F2 | F5 | F3 | F4 | P4 |
| W\_01 | x |  |  | x | x | x |
| W\_02 | x |  |  | x | x | x |
| U\_01 |  | x | x | x | x | x |
| U\_02 |  | x | x | x | x | x |
| K\_01 | x | x | x | x | x | x |

# 9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Z każdej formy prowadzonych zajęć uzyskaną ilość punktów przelicza się na wartość procentową. Ocena końcowa jest zgoda w progami oceniania zamieszczonymi w tabeli 1.
2. *Tab. 1. Progi ocenia procentowego*

|  |  |
| --- | --- |
| **Wynik procentowy** | **Ocena** |
| 0-50 % | niedostateczny (2.0) |
| 51-60 %. | dostateczny (3.0) |
| 61-70 % | dostateczny plus (3.5) |
| 71-80 % | dobry (4.0) |
| 81-90 % | dobry plus (4.5) |
| 91-100 % | bardzo dobry (5.0) |

 |

10. Forma zaliczenia zajęć

|  |
| --- |
| egzamin z oceną |

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

|  |  |
| --- | --- |
| **Forma aktywności studenta** | **Liczba godzin** |
| **na studiach stacjonarnych** | **na studiach niestacjonarnych** |
| **Godziny kontaktowe studenta (w ramach zajęć):** |
| liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia | **45** | **28** |
| **Praca własna studenta (indywidualna praca studenta związana z zajęciami):** |
| Zapoznanie z literaturą | 10 | 12 |
| Przygotowanie sprawozdań | 15 | 20 |
| Przygotowanie projektu | 15 | 20 |
| Przygotowanie do egzaminu | 15 | 20 |
| **suma godzin:** | **100** | **100** |
| **liczba pkt ECTS przypisana do zajęć:** (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta) | **4** | **4** |

12. Literatura zajęć

|  |
| --- |
| **Literatura obowiązkowa:**1. Materiały kursu CISCO pt. **Ethical hacker** , dostępny po zalogowaniu na platformie skillsforall.com, 2023.2. Diogenes, Yuri; Ozkaya, Erdal, **Cyberbezpieczeństwo : strategie ataku i obrony : jak osiągnąć najwyższy możliwy stan zabezpieczeń systemu informatycznego,** Helion 20233. Praca zbiorowa pod redakcją M. Sajdak, **Wprowadzenie do bezpieczeństwa IT, tom 1**, Securitum Szkolenia, 2023. |
| **Literatura zalecana / fakultatywna:**1. DiMaggio, Jon, **Wiersz poleceń Linuksa : rozwijanie umiejętności efektywnej pracy,** Helion 20231. Dominic Chell, Shaun Colley, Tyrone Erasmus, Ollie Whitehouse, **Bezpieczeństwo aplikacji mobilnych. Podręcznik hakera**, Helion 2023.3. Vickie Li ; przekład: Lech Lachowski, **Bug bounty bootcamp : przewodnik po tropieniu i zgłaszaniu luk w zabezpieczeniach** , Gliwice, Helion, 2022.4. Praca zbiorowa pod redakcją M. Sajdak, **Bezpieczeństwo aplikacji webowych**, Securitum Szkolenia, 2019. |

13. Informacje dodatkowe

|  |  |
| --- | --- |
| imię i nazwisko sporządzającego | dr inż. Łukasz Lemieszewski, , mgr inż. Robert Suchocki |
| dane kontaktowe (e-mail) | llemieszewski@ajp.edu.pl |
| data sporządzenia / aktualizacji | 10.06.2024 r.  |
| podpis |  |

|  |  |  |
| --- | --- | --- |
| Akademia_logo (4) | **Wydział** | Techniczny |
| **Kierunek** | Informatyka |
| **Poziom studiów** | drugiego stopnia |
| **Forma studiów** | stacjonarna/niestacjonarna |
| **Profil studiów** | praktyczny |
| **Pozycja w planie studiów (lub kod przedmiotu)** | C.4.2 |

**KARTA ZAJĘĆ/MODUŁU**

**1. Informacje ogólne**

|  |  |
| --- | --- |
| Nazwa zajęć | Bezpieczeństwo aplikacji webowych |
| Punkty ECTS | 3 |
| Rodzaj zajęć | ~~obowiązkowe~~/obieralne |
| Moduł/specjalizacja | Cyberbezpieczeństwo |
| Język, w którym prowadzone są zajęcia | Polski/Angielski |
| Rok studiów | 1 |
| Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia | mgr inż. Grzegorz Remiszewski |

**2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze**

|  |  |  |  |
| --- | --- | --- | --- |
| **Forma zajęć** | **Liczba godzin****Stacjonarne/niestacjonarne** | **Rok studiów/semestr** | **Punkty ECTS** (zgodnie z programem studiów) |
| **wykład** | **15/10** | **1/2;** | **3** |
| **laboratoria** | **30/18** | **1/2;** |

**3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć**

|  |
| --- |
| Student przedmiotu Zarządzanie bezpieczeństwem w systemach sieciowych posiada wiedzę, umiejętności i kompetencje społeczne, które nabył podczas realizacji przedmiotu wprowadzenie do sieci komputerowych, routing i przełączanie w sieciach LAN i WAN, aspekty cyberbezpieczeństwa. |

**4. Cele kształcenia**

|  |
| --- |
| C1 – Identyfikacja typów zagrożeń dla aplikacji webowych.C2 - Rozwijanie umiejętności praktycznych w zakresie zabezpieczania aplikacji webowych. C3 - Kształtowanie umiejętności analizy i oceny bezpieczeństwa aplikacji webowych.C4 - Korzystanie z narzędzi bezpieczeństwa i ocena zgodności ze standardami. |

**5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych**

|  |  |  |
| --- | --- | --- |
| **Symbol efektu uczenia się** | **Opis efektu uczenia się** | **Odniesienie do efektu kierunkowego** |
| **WIEDZA** |
| W\_01 | Student ma elementarną wiedzę z zakresu podstaw informatyki obejmującą bezpieczeństwo systemów komputerowych w szczególności bezpieczeństwo ich aplikacji. | K\_W03 |
| W\_02 | Student orientuje się w obecnym stanie oraz trendach rozwojowych bezpieczeństwa aplikacji webowych | K\_W06K\_W07 |
| **UMIEJĘTNOŚCI** |
| U\_01 | Student potrafi ocenić ryzyko i bezpieczeństwo baz danych, aplikacji internetowych, systemów i sieci komputerowych, stosując techniki oraz narzędzia sprzętowe i programowe. | K\_U04 |
| U\_02 | Student potrafi zaplanować i przeprowadzić symulację oraz przeprowadzić eksperyment pomiarowy z zakresu bezpieczeństwa systemów; potrafi przedstawić otrzymane wyniki w formie liczbowej oraz dokonać ich interpretacji i wyciągnąć właściwe wnioski | K\_U11 |
| **KOMPETENCJE SPOŁECZNE** |
| K\_01 | Student prawidłowo identyfikuje i rozstrzyga dylematy Cyberbezpieczeństwa. | K\_K01K\_K02 |

**6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć** (zgodnie z programem studiów):

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści wykładów**  | **Liczba godzin na studiach** |
| **stacjonarnych** | **niestacjonarnych** |
| W1 | Zajęcia organizacyjne – omówienie karty przedmiotu (cele i Efekty uczenia się, treści programowe, formy i warunki zaliczenia). Wprowadzenie do przedmiotu bezpieczeństwo aplikacji webowych. | 1 | 1 |
| W2 | Prawne aspekty ochrony danych osobowych. | 2 | 1 |
| W3 | Wprowadzenie do etycznego hakowania i testów penetracyjnych. | 2 | 2 |
| W4 | Wykorzystywanie luk w zabezpieczeniach sieci. | 2 | 1 |
| W5 | Bezpieczeństwo chmury, urządzeń mobilnych i IoT. | 2 | 1 |
| W6 | Wykorzystywanie luk w zabezpieczeniach aplikacji. | 2 | 1 |
| W7 | Wykonywanie technik poeksploatacyjnych. | 2 | 1 |
| W8 | Środowisko pracy aplikacji. Zaliczenie wykładu. | 2 | 2 |
|  | **Razem liczba godzin wykładów**  | **15** | **10** |

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści laboratoriów** | **Liczba godzin na studiach** |
| **stacjonarnych** | **niestacjonarnych** |
| L1 | Omówienie zakresu zajęć laboratoryjnych.  | 2 | 1 |
| L2 | Wprowadzenie do środowiska Damn Vulnerable Web Application (DVWA). | 2 | 1 |
| L3 | Analiza zagrożeń Stored Cross Site Scripting (XSS) oraz SQL Injection w środowisku DVWA. | 2 | 1 |
| L4 | Analiza zagrożeń File Upload oraz Insecure CAPTCHA w środowisku DVWA. | 2 | 1 |
| L5 | Analiza zagrożeń Brute Force oraz Command Injection w środowisku DVWA. | 2 | 1 |
| L6 | Testy penetracyjne . | 2 | 1 |
| L7 | Zarządzanie dostępem i ryzykiem. Plan DLP. | 2 | 1 |
| L8 | Wirtualizacji i konteneryzacja aplikacji  | 2 | 1 |
| L9 | Niebezpieczeństwa deserializacji | 2 | 1 |
| L10 | Podatność Path Traversal | 2 | 1 |
| L11 | OSINT (ang. Open-Source INTelligence) | 2 | 1 |
| L12 | Same-Origin Policy i Cross-Origin Resource Sharing (CORS). | 2 | 1 |
| L13 | Podatność Server-Side Template Injection (SSTI). | 2 | 1 |
| L14 | Zabezpieczenia Hosta.  | 2 | 1 |
| L15 | Omówienie sprawozdań, zaliczenia. Wystawienie ocen. | 2 | 1 |
|  | **Razem liczba godzin laboratoriów** | **30** | **18** |

**7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć**

|  |  |  |
| --- | --- | --- |
| **Forma zajęć** | **Metody dydaktyczne (wybór z listy)** | **Środki dydaktyczne** |
| Wykład | M1, M2 - wykład informacyjny jako prelekcja z objaśnieniami połączone z dyskusją oraz możliwością prezentacji prac własnych zrealizowanych jako prezentacje z przeglądu literatury | projektor, dostęp do Internetu,prezentacja multimedialna |
| Laboratoria | M5 - ćwiczenia doskonalące umiejętność pozyskiwania informacji ze źródeł internetowych i doskonalących obsługę narzędzi informatycznych oraz analiza sprawozdań przedstawionych przez studentów | Komputer z oprogramowaniem IDE dla aplikacji WEB oraz dostępem do Internetu. |

**8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta**

**8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć**

|  |  |  |
| --- | --- | --- |
| **Forma zajęć** | **Ocena formująca (F)** **–** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)** | **Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)** |
| Wykład | F1 - sprawdzian pisemny (kolokwium cząstkowe testy z pytaniami wielokrotnego wyboru i pytaniami otwartymi)  | P1 – zaliczenie z oceną pisemne |
| Laboratoria | F2 – obserwacja/aktywność (przygotowanie do zajęć, ocena ćwiczeń wykonywanych podczas zajęć), F5 - ćwiczenia praktyczne (ćwiczenia z wykorzystaniem sprzętu i oprogramowania fachowego) | P2 – kolokwium praktyczne  |

**8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x”)**

|  |  |  |
| --- | --- | --- |
| **Symbol efektu** | Wykład | Laboratoria |
| F1 | F2 | F5 |
| W\_01 | x |  |  |
| W\_02 | x |  |  |
| U\_01 |  | x | x |
| U\_02 |  | x | x |
| K\_01 | x | x | x |

# 9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Z każdej formy prowadzonych zajęć uzyskaną ilość punktów przelicza się na wartość procentową. Ocena końcowa jest zgoda w progami oceniania zamieszczonymi w tabeli 1.
2. *Tab. 1. Progi ocenia procentowego*

|  |  |
| --- | --- |
| **Wynik procentowy** | **Ocena** |
| 0-50 % | niedostateczny (2.0) |
| 51-60 %. | dostateczny (3.0) |
| 61-70 % | dostateczny plus (3.5) |
| 71-80 % | dobry (4.0) |
| 81-90 % | dobry plus (4.5) |
| 91-100 % | bardzo dobry (5.0) |

 |

10. Forma zaliczenia zajęć

|  |
| --- |
| zaliczenie z oceną |

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

|  |  |
| --- | --- |
| **Forma aktywności studenta** | **Liczba godzin** |
| **na studiach stacjonarnych** | **na studiach niestacjonarnych** |
| **Godziny kontaktowe studenta (w ramach zajęć):** |
| liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia | **45** | **28** |
| **Praca własna studenta (indywidualna praca studenta związana z zajęciami):** |
| Zapoznanie z literaturą | 5 | 10 |
| Przygotowanie sprawozdań | 10 | 17 |
| Przygotowanie do zaliczenia | 15 | 20 |
| **suma godzin:** | **75** | **75** |
| **liczba pkt ECTS przypisana do zajęć:** (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta) | **3** | **3** |

12. Literatura zajęć

|  |
| --- |
| **Literatura obowiązkowa:**1. Praca zbiorowa pod redakcją M. Sajdak, **Bezpieczeństwo aplikacji webowych**, Securitum Szkolenia, 2019.
2. Materiały kursu CISCO pt. **CyberOps,** dostępny po zalogowaniu na platformie netacad.com, 2020.
3. Stallings W., Brown L., **Bezpieczeństwo systemów informatycznych.** **Zasady i praktyka, Tom I i II,** Helion, Gliwice 2019.
 |
| **Literatura zalecana / fakultatywna:**1. Dominic Chell, Shaun Colley, Tyrone Erasmus, Ollie Whitehouse, **Bezpieczeństwo aplikacji mobilnych. Podręcznik hakera**, Helion 2023.2. O. Santos, Cisco **Cyberops Associate Cbrops 200-201 Official Cert Guide**, CISCO, 2020.3. Vickie Li ; przekład: Lech Lachowski, **Bug bounty bootcamp : przewodnik po tropieniu i zgłaszaniu luk w zabezpieczeniach** , Gliwice, Helion, 2023. |

13. Informacje dodatkowe

|  |  |
| --- | --- |
| imię i nazwisko sporządzającego | mgr inż. Grzegorz Remiszewski |
| data sporządzenia / aktualizacji | 10.06.2024 r.  |
| dane kontaktowe (e-mail) | g.remiszewski@ajp.edu.pl |
| podpis |  |

|  |  |  |
| --- | --- | --- |
| Akademia_logo (4) | **Wydział** | Techniczny |
| **Kierunek** | Informatyka |
| **Poziom studiów** | drugiego stopnia |
| **Forma studiów** | stacjonarna/niestacjonarna |
| **Profil studiów** | praktyczny |
| **Pozycja w planie studiów (lub kod przedmiotu)** | C.4.3 |

**KARTA ZAJĘĆ**

**1. Informacje ogólne**

|  |  |
| --- | --- |
| Nazwa zajęć | Zapewnienie bezpieczeństwa systemów informatycznych i sieci komputerowych |
| Punkty ECTS | 3 |
| Rodzaj zajęć | ~~obowiązkowe~~/obieralne |
| Moduł/specjalizacja | Cyberbezpieczeństwo |
| Język, w którym prowadzone są zajęcia | Polski/Angielski |
| Rok studiów | 1 |
| Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia | dr inż. Łukasz Lemieszewski, mgr Mariusz Kowalski |

**2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze**

|  |  |  |  |
| --- | --- | --- | --- |
| **Forma zajęć** | **Liczba godzin****Stacjonarne/niestacjonarne** | **Rok studiów/semestr** | **Punkty ECTS** (zgodnie z programem studiów) |
| **wykład** | **15/10** | **1/2;** | **3** |
| **laboratoria** | **30/18** | **1/2;** |

**3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć**

|  |
| --- |
| Student przedmiotu Zarządzanie bezpieczeństwem w systemach sieciowych posiada wiedzę, umiejętności i kompetencje społeczne, które nabył podczas realizacji przedmiotu operacje cyberbezpieczeństwa. |

**4. Cele kształcenia**

|  |
| --- |
| C1 - kształtowanie umiejętności miękkich niezbędnych do pracy w obszarze bezpieczeństwa ITC2 - rozwijanie umiejętności praktycznych w zakresie konfiguracji i administrowania systemami bezpieczeństwaC3 - Student potrafi diagnozować, eliminować i przewidywać zagrożenia bezpieczeństwa systemów i sieci komputerowych. |

**5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych**

|  |  |  |
| --- | --- | --- |
| **Symbol efektu uczenia się** | **Opis efektu uczenia się** | **Odniesienie do efektu kierunkowego** |
| **WIEDZA** |
| W\_01 | Student ma elementarną wiedzę z zakresu rozwiązywania problemów i zapewnienia bezpieczeństwa bezpieczeństwo danych i systemów komputerowych bezpieczeństwo aplikacji. | K\_W01K\_W07 |
| W\_02 | Student orientuje się w obecnym stanie oraz trendach rozwojowych systemów i sieci teleinformatycznych  | K\_W09 |
| **UMIEJĘTNOŚCI** |
| U\_01 | Student potrafi ocenić ryzyko i bezpieczeństwo baz danych, aplikacji internetowych, systemów i sieci komputerowych, stosując techniki oraz narzędzia sprzętowe i programowe. | K\_U03K\_U05 |
| U\_02 | Student potrafi zaplanować i przeprowadzić symulację oraz przeprowadzić eksperyment pomiarowy z zakresu bezpieczeństwa systemów; potrafi przedstawić otrzymane wyniki w formie liczbowej oraz dokonać ich interpretacji i wyciągnąć właściwe wnioski | K\_U18 |
| **KOMPETENCJE SPOŁECZNE** |
| K\_01 | Student prawidłowo identyfikuje i rozstrzyga dylematy wpłyu na środowisko i związaną z tym odpowiedzialność za podejmowane decyzje w zakresie bezpieczeństwa systemów informatycznych i sieci komputerowych | K\_K02 |

**6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć** (zgodnie z programem studiów):

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści wykładów**  | **Liczba godzin na studiach** |
| **stacjonarnych** | **stacjonarnych** |
| W1 | Zrozumienie obrony. Kontrola dostępu.  | 2 | 2 |
| W2 | Analiza zagrożeń. | 2 | 1 |
| W3 | Wybrane zagadnienia kryptografii. | 2 | 2 |
| W4 | Ochrona punktów końcowych. | 2 | 1 |
| W5 | Ocena podatności punktu końcowego. | 2 | 1 |
| W6 | Ocena alertów. Praca z danymi technologie i protokoły  | 2 | 1 |
| W7 | Dane bezpieczeństwa sieci | 2 | 1 |
| W8 | Cyfrowa analiza śledcza i analiza incydentów oraz reagowanie. | 1 | 1 |
|  | **Razem liczba godzin wykładów**  | **15** | **10** |

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści laboratoriów** | **Liczba godzin na studiach** |
| **stacjonarnych** | **stacjonarnych** |
| L1 | 14.1.11 Laboratorium - Anatomia złośliwego oprogramowania14.2.8 Laboratorium - Inżynieria społeczna | 2 | 1 |
| L2 | 15.0.3 Ćwiczenie - Co się dzieje?17.1.7 Laboratorium - Badanie ruchu DNS | 2 | 1 |
| L3 | 17.2.6 Laboratorium - Atakowanie bazy danych mySQL17.2.7 Laboratorium - Czytanie logów serwera | 2 | 1 |
| L4 | 21.0.3 Ćwiczenie - Tworzenie kodów21.1.6 Laboratorium – Haszowanie odwrotne | 2 | 1 |
| L5 | 21.2.10 Laboratorium - Szyfrowanie i deszyfrowanie danych przy użyciu OpenSSL | 2 | 1 |
| L6 | 21.2.11 Laboratorium - Szyfrowanie i deszyfrowanie danych przy użyciu narzędzia hakerskiego | 2 | 1 |
| L7 | 21.2.12 Laboratorium - Badanie protokołów Telnet i SSH w Wireshark21.4.7 Laboratorium - Magazyny urzędów certyfikacji | 2 | 1 |
| L8 | 26.1.7 Laboratorium - Snort i reguły zapory | 2 | 1 |
| L9 | 27.1.5 Laboratorium - Konwersja danych do uniwersalnego formatu27.2.10 Laboratorium - Wyodrębnianie pliku wykonywalnego z PCAP | 2 | 1 |
| L10 | 27.2.12 Laboratorium - Interpretacja danych HTTP i DNS w celu wyizolowania aktora-zagrożenia | 2 | 1 |
| L11 | 27.2.14 Laboratorium - Izolowanie skompromitowanego hosta przy użyciu 5-tuple | 2 | 1 |
| L12 | 27.2.15 Laboratorium - Badanie złośliwego oprogramowania | 2 | 1 |
| L13 | 27.2.16 Laboratorium - Badanie ataku na hosta Windows | 2 | 1 |
| L14 | 27.2.9 Laboratorium - Samouczek dotyczący wyrażeń regularnych | 2 | 1 |
| L15 | 28.4.13 Laboratorium - Obsługa incydentów. | 2 | 1 |
|  | **Razem liczba godzin laboratoriów** | **30** | **18** |

**7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć**

|  |  |  |
| --- | --- | --- |
| **Forma zajęć** | **Metody dydaktyczne (wybór z listy)** | **Środki dydaktyczne** |
| Wykład | M1, M2 - wykład informacyjny jako prelekcja z objaśnieniami połączone z dyskusją oraz możliwością prezentacji prac własnych zrealizowanych jako prezentacje z przeglądu literatury | projektor, dostęp do Internetu,prezentacja multimedialna |
| Laboratoria | M5 - ćwiczenia doskonalące umiejętność pozyskiwania informacji ze źródeł internetowych i doskonalących obsługę narzędzi informatycznych oraz analiza sprawozdań przedstawionych przez studentów | Komputer z oprogramowaniem IDE dla aplikacji WEB oraz dostępem do Internetu. |

**8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta**

**8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć**

|  |  |  |
| --- | --- | --- |
| **Forma zajęć** | **Ocena formująca (F)** **–** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)** | **Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)** |
| Wykład | F1 - sprawdzian pisemny (kolokwium cząstkowe testy z pytaniami wielokrotnego wyboru i pytaniami otwartymi)  | P1 – egzamin pisemny w formie pytań testowych |
| Laboratoria | F2 – obserwacja/aktywność (przygotowanie do zajęć, ocena ćwiczeń wykonywanych podczas zajęć), F5 - ćwiczenia praktyczne (ćwiczenia z wykorzystaniem sprzętu i oprogramowania fachowego) | P2 – kolokwium praktyczne  |

**8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x”)**

|  |  |  |
| --- | --- | --- |
| **Symbol efektu** | Wykład | Laboratoria |
| F1 | F2 | F5 |
| W\_01 | x |  |  |
| W\_02 | x |  |  |
| U\_01 |  | x | x |
| U\_02 |  | x | x |
| K\_01 | x | x | x |

# 9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Z każdej formy prowadzonych zajęć uzyskaną ilość punktów przelicza się na wartość procentową. Ocena końcowa jest zgoda w progami oceniania zamieszczonymi w tabeli 1.
2. *Tab. 1. Progi ocenia procentowego*

|  |  |
| --- | --- |
| **Wynik procentowy** | **Ocena** |
| 0-50 % | niedostateczny (2.0) |
| 51-60 %. | dostateczny (3.0) |
| 61-70 % | dostateczny plus (3.5) |
| 71-80 % | dobry (4.0) |
| 81-90 % | dobry plus (4.5) |
| 91-100 % | bardzo dobry (5.0) |

 |

10. Forma zaliczenia zajęć

|  |
| --- |
| egzamin z oceną |

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

|  |  |
| --- | --- |
| **Forma aktywności studenta** | **Liczba godzin** |
| **na studiach stacjonarnych** | **na studiach niestacjonarnych** |
| **Godziny kontaktowe studenta (w ramach zajęć):** |
| liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia | **45** | **28** |
| **Praca własna studenta (indywidualna praca studenta związana z zajęciami):** |
| Konsultacje | 5 | 5 |
| Zapoznanie z literaturą | 5 | 10 |
| Przygotowanie sprawozdań | 10 | 17 |
| Przygotowanie do egzaminu | 10 | 15 |
| **suma godzin:** | **75** | **75** |
| **liczba pkt ECTS przypisana do zajęć:** (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta) | **3** | **3** |

12. Literatura zajęć

|  |
| --- |
| **Literatura obowiązkowa:**1. Materiały kursu CISCO pt. **CyberOps**, dostępny po zalogowaniu na platformie netacad.com, 2020.
2. Stallings W., Brown L., **Bezpieczeństwo systemów informatycznych**. Zasady i praktyka, Tom I i II, Helion, Gliwice 2019.
3. Adam Józefiok, **CCNA 200-301 : zostań administratorem sieci komputerowych Cisco**, Gliwice, Helion 2020
 |
| **Literatura zalecana / fakultatywna:**1. O. Santos, Cisco **Cyberops Associate Cbrops 200-201 Official Cert Guide**, CISCO, 20202. G. D. Singh, Cisco **Certified CyberOps Associate 200-201 Certification Guide**, Packt Publishing Limited, 20213. Vickie Li ; przekład: Lech Lachowski, **Bug bounty bootcamp : przewodnik po tropieniu i zgłaszaniu luk w zabezpieczeniach** , Gliwice, Helion, 2023 |

13. Informacje dodatkowe

|  |  |
| --- | --- |
| imię i nazwisko sporządzającego | dr inż. Łukasz Lemieszewski |
| data sporządzenia / aktualizacji | 10.06.2024 r.  |
| dane kontaktowe (e-mail) | llemieszewski@ajp.edu.pl |
| podpis |  |

|  |  |  |
| --- | --- | --- |
| Akademia_logo (4) | **Wydział** | Techniczny |
| **Kierunek** | Informatyka |
| **Poziom studiów** | drugiego stopnia |
| **Forma studiów** | stacjonarna/niestacjonarna |
| **Profil studiów** | praktyczny |
| **Pozycja w planie studiów (lub kod przedmiotu)** | C.4.4 |

**KARTA ZAJĘĆ**

**1. Informacje ogólne**

|  |  |
| --- | --- |
| Nazwa zajęć | Bezpieczeństwo nowoczesnych systemów operacyjnych |
| Punkty ECTS | 8 |
| Rodzaj zajęć | ~~obowiązkowe~~/obieralne |
| Moduł/specjalizacja | Cyberbezpieczeństwo |
| Język, w którym prowadzone są zajęcia | Polski |
| Rok studiów | 1 |
| Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia | mgr inż. Piotr Winiarski, mgr inż. Grzegorz Remiszewski |

**2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze**

|  |  |  |  |
| --- | --- | --- | --- |
| **Forma zajęć** | **Liczba godzin****Stacjonarne/niestacjonarne** | **Rok studiów/semestr** | **Punkty ECTS** (zgodnie z programem studiów) |
| **wykład** | **30/20** | **1,2/2,3;** | **8** |
| **laboratoria** | **60/36** | **1,2/2,3;** |
| **projekt** | **30/20** | **1,2/2,3;** |

**3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć**

|  |
| --- |
| Student przedmiotu Bezpieczeństwo nowoczesnych systemów operacyjnych posiada wiedzę, umiejętności i kompetencje społeczne, które nabył podczas realizacji studiów informatycznych I stopnia w szczególnosci przedmiotów: wprowadzenie do sieci komputerowych, routing i przełączanie w sieciach LAN i WAN, systemy operacyjne.  |

**4. Cele kształcenia**

|  |
| --- |
| C1 – Zapoznanie z definicjami i standardami oraz unormowanymi dotyczącymi zagadnień odnoszących się do bezpieczeństwa systemów i sieci komputerowych.C2 - Stosowanie poznanych narzędzi i metod oraz technik projektowania, konfigurowania, testowania w eliminowaniu podatności oraz przeciwdziałaniu skutkom incydentów bezpieczeństwa systemów i sieci komputerowychC3 - Diagnozowanie, eliminowanie i przewidywanie zagrożenia bezpieczeństwa systemów i sieci komputerowych.C4 - Zarządzanie ryzykiem na podstawie oceny bezpieczeństwa systemów operacyjnych i wdrażanie odpowiednich środków zaradczych w celu jego zminimalizowania. |

**5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych**

|  |  |  |
| --- | --- | --- |
| **Symbol efektu uczenia się** | **Opis efektu uczenia się** | **Odniesienie do efektu kierunkowego** |
| **WIEDZA** |
| W\_01 | Student ma elementarną wiedzę z zakresu bezpieczeństwa nowoczesnych systemów operacyjnych | K\_W03 |
| W\_02 | Student orientuje się w obecnym stanie oraz trendach rozwojowych zapewnienia bezpieczeństwa systemów operacyjnych | K\_W06 |
| **UMIEJĘTNOŚCI** |
| U\_01 | Student potrafi ocenić ryzyko i bezpieczeństwo baz danych, aplikacji internetowych, systemów i sieci komputerowych, stosując techniki oraz narzędzia sprzętowe i programowe. | K\_U04 |
| U\_02 | Student potrafi zaplanować i przeprowadzić symulację oraz przeprowadzić eksperyment pomiarowy z zakresu bezpieczeństwa systemów; potrafi przedstawić otrzymane wyniki w formie liczbowej oraz dokonać ich interpretacji i wyciągnąć właściwe wnioski | K\_U11K\_U14 |
| **KOMPETENCJE SPOŁECZNE** |
| K\_01 | Student rozumie ważność mechanizmów zapewnienia bezpieczeństwa nowoczesnych systemów operacyjnych | K\_K02K\_K04 |

**6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć** (zgodnie z programem studiów):

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści wykładów**  | **Liczba godzin na studiach** |
| **stacjonarnych** | **stacjonarnych** |
| W1 | Nowoczesne systemy operacyjne. Przegląd koncepcji. | 2 | 2 |
| W2 | Wielowarstwowa budowa systemów operacyjnych. | 2 | 1 |
| W3 | Wirtualizacja zasobów. | 2 | 2 |
| W4 | Konteneryzacja zasobów. | 2 | 1 |
| W5 | Orchestracja zasobów. | 2 | 1 |
| W6 | Zarządzanie zasobami dyskowymi. | 2 | 1 |
| W7 | Wdrażanie IRM.  | 2 | 1 |
| W8 | Przegląd rozwiązań w zakresie wirtualizacji i konteneryzacji.  | 1 | 1 |
| W9 | Środowisko wysokiej dostępności. | 2 | 2 |
| W10 | Monitorowanie systemu operacyjnego. | 2 | 1 |
| W11 | Środowiska przetwarzania danych.  | 2 | 2 |
| W12 | Wybrane aspekty bezpieczeństwa systemów operacyjnych. | 2 | 1 |
| W13 | Zapory programowe i systemowe. | 2 | 1 |
| W14 | Zarządzanie polityka bezpieczeństwa. | 2 | 1 |
| W15 | Wdrażanie planu DLP. | 2 | 1 |
| W16 | Backup zasobów.  | 1 | 1 |
|  | **Razem liczba godzin wykładów**  | **30** | **20** |

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści laboratoriów** | **Liczba godzin na studiach** |
| **stacjonarnych** | **stacjonarnych** |
| L1 | Serwer proxy z wykorzystaniem Nginx. | 2 | 1 |
| L2 | Udostępnianie infrastruktury hiperkonwergentnej z wykorzystaniem Proxmox VE. | 4 | 2 |
| L3 | Wirtualizacja z wykorzystaniem Vagrant. | 4 | 2 |
| L4 | Konteneryzacja środowiska pracy z wykorzystaniem Docera. | 4 | 4 |
| L5 | Orchestracja zasobów z wykorzystaniem Terraform. | 4 | 2 |
| L6 | Orchestracja zasobów z wykorzystaniem SaltStack. | 4 | 2 |
| L7 | Konfiguracja playbook’ów - automatyzacja wdrażania, konfiguracji i zarządzania na przykładzie Ansible. | 4 | 2 |
| L8 | Zarządzanie zasobami dyskowymi z wykorzystaniem FREENAS. | 2 | 2 |
| L9 | Kolokwium podsumowujące po I semestrze. | 2 | 1 |
| L10 | Monitorowanie sieci z wykorzystaniem PfSense. | 2 | 2 |
| L11 | Monitorowanie sieci z wykorzystaniem Zabbix. | 4 | 2 |
| L12 | Utwardzone dystrybucje Linux na przykładzie VyOS ora IPFire. | 4 | 2 |
| L13 | Środowisko Pi-Hole. | 4 | 2 |
| L14 | Środowisko wielo-serwerowe Linux z wykorzystaniem OpenLDAP. | 4 | 2 |
| L15 | Środowisko Parrot. | 4 | 2 |
| L16 | Kubernetes – konteneryzacja aplikacji skalowanej. | 2 | 2 |
| L17 | Konfiguracja aspektów bezpieczeństwa np. FAIL2BAN, GPO. | 4 | 2 |
| L18 | Kolokwium podsumowujące po II semestrze. | 2 | 2 |
|  | **Razem liczba godzin laboratoriów** | **60** | **36** |

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści projektów** | **Liczba godzin na studiach** |
| **stacjonarnych** | **stacjonarnych** |
| P1 | Określenie celów i wymagań klienta. | 2 | 2 |
| P2 | Analiza wymagań i celów. Studium przypadku. | 2 | 1 |
| P3 | Harmonogram prac. | 2 | 2 |
| P4 | Implementacja rozwiązania w środowisku wirtualnym. | 2 | 1 |
| P5 | Implementacja rozwiązania w środowisku onpromice. | 2 | 1 |
| P6 | Budżetowanie zaproponowanego rozwiązania. Określenie TCO. | 2 | 1 |
| P7 | Dokumentacja zaproponowanego rozwiązania. | 2 | 1 |
| P8 | Obrona projektu po I semestrze. | 1 | 1 |
| P9 | Określenie celów i wymagań klienta. | 2 | 2 |
| P10 | Analiza wymagań i celów. Studium przypadku. | 2 | 1 |
| P11 | Harmonogram prac. | 2 | 2 |
| P12 | Implementacja rozwiązania w środowisku wirtualnym. | 2 | 1 |
| P13 | Implementacja rozwiązania w środowisku onpromice. | 2 | 1 |
| P14 | Budżetowanie zaproponowanego rozwiązania. Określenie TCO. | 2 | 1 |
| P15 | Dokumentacja zaproponowanego rozwiązania. | 2 | 1 |
| P16 | Obrona projektu po II semestrze. | 1 | 1 |
|  |  | **30** | **20** |

**7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć**

|  |  |  |
| --- | --- | --- |
| **Forma zajęć** | **Metody dydaktyczne (wybór z listy)** | **Środki dydaktyczne** |
| Wykład | M1, M2 - wykład informacyjny jako prelekcja z objaśnieniami połączone z dyskusją oraz możliwością prezentacji prac własnych zrealizowanych jako prezentacje z przeglądu literatury | projektor, dostęp do Internetu,prezentacja multimedialna |
| Laboratoria | M5 - ćwiczenia doskonalące umiejętność pozyskiwania informacji ze źródeł internetowych i doskonalących obsługę narzędzi informatycznych  | Komputer z środowiskiem GNS3 oraz dostępem do Internetu, Urządzenia sieciowe zgodnie ze specyfikacją CCNA Security |
| Projekt | M5 - ćwiczenia doskonalące umiejętność pozyskiwania informacji ze źródeł internetowych i doskonalących obsługę narzędzi informatycznych oraz obrona projektu końcowego. | Komputer z środowiskiem GNS3 oraz dostępem do Internetu, Urządzenia sieciowe zgodnie ze specyfikacją CCNA Security |

**8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta**

**8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć**

|  |  |  |
| --- | --- | --- |
| **Forma zajęć** | **Ocena formująca (F)** **–** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)** | **Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)** |
| Wykład | F1 - sprawdzian pisemny (kolokwium cząstkowe testy z pytaniami wielokrotnego wyboru i pytaniami otwartymi)  | P1 – zaliczenie pisemne |
| Laboratoria | F2 – obserwacja/aktywność (przygotowanie do zajęć, ocena ćwiczeń wykonywanych podczas zajęć), F5 - ćwiczenia praktyczne (ćwiczenia z wykorzystaniem sprzętu i oprogramowania fachowego) | P2 – kolokwium praktyczne  |
| Projekt | F3 – dokumentacja projektu F4 – wystąpienie – analiza projektu | P4 – praca pisemna - projekt |

**8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x”)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Symbol efektu** | Wykład | Laboratoria | Projekt |
| F1 | F2 | F5 | F3 | F4 | P4 |
| W\_01 | x |  |  | x | x | x |
| W\_02 | x |  |  | x | x | x |
| U\_01 |  | x | x | x | x | x |
| U\_02 |  | x | x | x | x | x |
| K\_01 | x | x | x | x | x | x |

# 9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Z każdej formy prowadzonych zajęć uzyskaną ilość punktów przelicza się na wartość procentową. Ocena końcowa jest zgoda w progami oceniania zamieszczonymi w tabeli 1.
2. *Tab. 1. Progi ocenia procentowego*

|  |  |
| --- | --- |
| **Wynik procentowy** | **Ocena** |
| 0-50 % | niedostateczny (2.0) |
| 51-60 %. | dostateczny (3.0) |
| 61-70 % | dostateczny plus (3.5) |
| 71-80 % | dobry (4.0) |
| 81-90 % | dobry plus (4.5) |
| 91-100 % | bardzo dobry (5.0) |

 |

10. Forma zaliczenia zajęć

|  |
| --- |
| Zaliczenie z oceną |

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

|  |  |
| --- | --- |
| **Forma aktywności studenta** | **Liczba godzin** |
| **na studiach stacjonarnych** | **na studiach niestacjonarnych** |
| **Godziny kontaktowe studenta (w ramach zajęć):** |
| liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia | **120** | **76** |
| **Praca własna studenta (indywidualna praca studenta związana z zajęciami):** |
| Zapoznanie z literaturą rok 1 semestrze 2 | 5 | 15 |
| Zapoznanie z literaturą rok 2 semestrze 3 | 5 | 15 |
| Przygotowanie sprawozdań rok 1 semestrze 2 | 20 | 27 |
| Przygotowanie sprawozdań rok 2 semestrze 3 | 20 | 27 |
| Przygotowanie do zaliczenia rok 1 semestrze 2 | 15 | 20 |
| Przygotowanie do egzaminu rok 2 semestrze 3 | 15 | 20 |
| **suma godzin:** | **200** | **200** |
| **liczba pkt ECTS przypisana do zajęć:** (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta) | **8** | **8** |

12. Literatura zajęć

|  |
| --- |
| **Literatura obowiązkowa:**1.Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley, Dan Mackin, James Garnett, Fabrizio Branca, Adrian Mouat, **Unix i Linux : przewodnik administratora systemów,** Helion 2023.2. VandenBrink, Rob, **Linux i obsługa sieci dla profesjonalistów : konfiguracja i stosowanie bezpiecznych usług sieciowych,** Helion 20233. Stallings W., Brown L., **Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Tom I i II**, Helion, Gliwice 2019. |
| **Literatura zalecana / fakultatywna:**1. O. Santos, **Cisco Cyberops Associate Cbrops 200-201 Official Cert Guide**, CISCO, 20202. Velu, Vijay Kumar, **Kali Linux i zaawansowane testy penetracyjne : zostań ekspertem cyberbezpieczeństwa za pomocą Metasploit, Nmap, Wireshark i Burp Suite**, Helion 2023.3. Krzysztof Wosiński, **Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu : OSINT**, Wydawnictwo Naukowe PWN SA, 20244. Filip Radoniewicz, **Cyberprzestępstwa przeciwko danym komputerowym i systemom informatycznym w kodeksie karnym - propozycje zmian**, Wydawnictwo C. H. Beck, 2024 |

13. Informacje dodatkowe

|  |  |
| --- | --- |
| imię i nazwisko sporządzającego | mgr inż. Grzegorz Remieszewski |
| data sporządzenia / aktualizacji | 10.06.2024 r.  |
| dane kontaktowe (e-mail) | gremiszewski@ajp.edu.pl |
| podpis |  |

|  |  |  |
| --- | --- | --- |
| Akademia_logo (4) | **Wydział** | Techniczny |
| **Kierunek** | Informatyka |
| **Poziom studiów** | drugiego stopnia |
| **Forma studiów** | stacjonarna/niestacjonarna |
| **Profil studiów** | praktyczny |
| **Pozycja w planie studiów (lub kod przedmiotu)** | D.4.6 |

**KARTA ZAJĘĆ**

**1. Informacje ogólne**

|  |  |
| --- | --- |
| Nazwa zajęć | Zaawansowane zagrożenia inżynierii społecznej w cyberprzestrzeni |
| Punkty ECTS | 3 |
| Rodzaj zajęć | ~~obowiązkowe~~/obieralne |
| Moduł/specjalizacja | Cyberbezpieczeństwo |
| Język, w którym prowadzone są zajęcia | Polski/Angielski |
| Rok studiów | 2 |
| Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia | Dr. inż., Łukasz Lemieszewskimgr inż. Szymon Prochacki |

**2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze**

|  |  |  |  |
| --- | --- | --- | --- |
| **Forma zajęć** | **Liczba godzin****Stacjonarne/niestacjonarne** | **Rok studiów/semestr** | **Punkty ECTS** (zgodnie z programem studiów) |
| **wykład** | **15/10** | **2/3;** | **3** |
| **laboratoria** | **30/18** | **2/3;** |

**3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć**

|  |
| --- |
| Student przedmiotu Zarządzanie bezpieczeństwem w systemach sieciowych posiada wiedzę, umiejętności i kompetencje społeczne, które nabył podczas realizacji przedmiotu operacje cyberbezpieczeństwa, etyczny haker i bezpieczeństwo aplikacji webowych. |

**4. Cele kształcenia**

|  |
| --- |
| C1 - Zna definicje i standardy oraz unormowania dotycząc zagadnień odnoszących się do bezpieczeństwa i ataków społecznychC2 - korzysta z poznanych narzędzi i metod oraz technik zapobiegania i, testowania w eliminowaniu podatności oraz przeciwdziałaniu skutkom incydentów bezpieczeństwa oraz dezinformacjiC3 - Diagnozowanie, eliminowanie i przewidziałanie zagrożeniom bezpieczeństwa inżynierii społecznej.C4 - Analiza psychologicznych aspektów inżynierii społecznejC5 - Ocena podatności na ataki inżynierii społeczne oraz opracowywanie zaawansowanych strategii obrony przed inżynierią społeczną |

**5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych**

|  |  |  |
| --- | --- | --- |
| **Symbol efektu uczenia się** | **Opis efektu uczenia się** | **Odniesienie do efektu kierunkowego** |
| **WIEDZA** |
| W\_01 | Student ma elementarną wiedzę z zakresu podstaw informatyki obejmującą bezpieczeństwo danych i inżynierii społecznej. | K\_W02 |
| W\_02 | Student orientuje się w obecnym stanie oraz trendach rozwojowych zapobieganiu ataków, wycieków danych i manipulacji socjotechnicznych.  | K\_W09 |
| **UMIEJĘTNOŚCI** |
| U\_01 | Student potrafi ocenić ryzyko i bezpieczeństwo baz danych, aplikacji internetowych oraz socialmediów stosując techniki oraz narzędzia sprzętowe i programowe. | K\_U04 |
| U\_02 | Student potrafi zaplanować i przeprowadzić symulację oraz przeprowadzić eksperyment pomiarowy z zakresu zagrożeń inżynierii społecznej w cyberprzestrzeni; potrafi przedstawić otrzymane wyniki w formie liczbowej oraz dokonać ich interpretacji i wyciągnąć właściwe wnioski. Wie jak przeciwdziałać niepożądanym skutkom zagrożeń inżynierii społecznej w cyberprzestrzeni i ich przyczynom. | K\_U11 |
| **KOMPETENCJE SPOŁECZNE** |
| K\_01 | Student prawidłowo identyfikuje i rozstrzyga dylematy zagrożeń inżynierii społecznej w cyberprzestrzeni. | K\_K02K\_K04 |

**6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć** (zgodnie z programem studiów):

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści wykładów**  | **Liczba godzin na studiach** |
| **stacjonarnych** | **niestacjonarnych** |
| W1 | Omówienie karty przedmiotu (cele i Efekty uczenia się, treści programowe, formy i warunki zaliczenia). Wprowadzenie do zagrożeń inżynierii społecznej w cyberprzestrzeni. | 1 | 1 |
| W2 | Podstawy inżynierii społecznej, rodzaje aktorów w atakach | 2 | 1 |
| W3 | Wybrane aspekty i zasady wykrywania podatności (OSINT) | 2 | 2 |
| W4 | Socjotechnika i psychologia manipulacji | 2 | 1 |
| W5 | Deepfake i ich wykorzystanie w inżynierii społecznej | 2 | 1 |
| W6 | Socjotechnika w mediach społecznościowych | 2 | 1 |
| W7 | Inżynieria społeczna w kontekście bezpieczeństwa korporacyjnego | 2 | 1 |
| W8 | Socjotechnika w atakach na infrastrukturę krytyczną | 2 | 2 |
|  | **Razem liczba godzin wykładów**  | **15** | **10** |

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści laboratoriów** | **Liczba godzin na studiach** |
| **stacjonarnych** | **niestacjonarnych** |
| L1 | Omówienie zakresu zajęć laboratoryjnych.  | 1 | 1 |
| L2 | Metody ochrony infrastruktury krytycznej przed socjotechniką | 2 | 1 |
| L3 | Studium przypadków: wybrane incydenty i ich analiza | 2 | 1 |
| L4 | Wykorzystywanie danych z mediów społecznościowych do ataków | 2 | 1 |
| L5 | Kampanie dezinformacyjne i metody prewencji | 2 | 1 |
| L6 | Zastosowania deepfake w atakach socjotechnicznych | 2 | 1 |
| L7 | Narzędzia ataku społecznego: Social Engineer Toolkit | 2 | 1 |
| L8 | Spersonalizowane ataki społeczne, manipulacji i wykorzystanie danych. | 2 | 1 |
|  | **Razem liczba godzin laboratoriów** | **15** | **8** |

**7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć**

|  |  |  |
| --- | --- | --- |
| **Forma zajęć** | **Metody dydaktyczne (wybór z listy)** | **Środki dydaktyczne** |
| Wykład | M1, M2 - wykład informacyjny jako prelekcja z objaśnieniami połączone z dyskusją oraz możliwością prezentacji prac własnych zrealizowanych jako prezentacje z przeglądu literatury | projektor, dostęp do Internetu,prezentacja multimedialna |
| Laboratoria | M5 - ćwiczenia doskonalące umiejętność pozyskiwania informacji ze źródeł internetowych i doskonalących obsługę narzędzi informatycznych oraz analiza sprawozdań przedstawionych przez studentów | Komputer z oprogramowaniem IDE dla aplikacji WEB oraz dostępem do Internetu. |

**8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta**

**8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć**

|  |  |  |
| --- | --- | --- |
| **Forma zajęć** | **Ocena formująca (F)** **–** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)** | **Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)** |
| Wykład | F1 - sprawdzian pisemny (kolokwium cząstkowe testy z pytaniami wielokrotnego wyboru i pytaniami otwartymi)  | P1 – zaliczenie pisemne |
| Laboratoria | F2 – obserwacja/aktywność (przygotowanie do zajęć, ocena ćwiczeń wykonywanych podczas zajęć), F5 - ćwiczenia praktyczne (ćwiczenia z wykorzystaniem sprzętu i oprogramowania fachowego) | P2 – kolokwium praktyczne  |

**8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x”)**

|  |  |  |
| --- | --- | --- |
| **Symbol efektu** | Wykład | Laboratoria |
| F1 | F2 | F5 |
| W\_01 | x |  |  |
| W\_02 | x |  |  |
| U\_01 |  | x | x |
| U\_02 |  | x | x |
| K\_01 | x | x | x |

# 9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Z każdej formy prowadzonych zajęć uzyskaną ilość punktów przelicza się na wartość procentową. Ocena końcowa jest zgoda w progami oceniania zamieszczonymi w tabeli 1.
2. *Tab. 1. Progi ocenia procentowego*

|  |  |
| --- | --- |
| **Wynik procentowy** | **Ocena** |
| 0-50 % | niedostateczny (2.0) |
| 51-60 %. | dostateczny (3.0) |
| 61-70 % | dostateczny plus (3.5) |
| 71-80 % | dobry (4.0) |
| 81-90 % | dobry plus (4.5) |
| 91-100 % | bardzo dobry (5.0) |

 |

10. Forma zaliczenia zajęć

|  |
| --- |
| zaliczenie z oceną |

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

|  |  |
| --- | --- |
| **Forma aktywności studenta** | **Liczba godzin** |
| **na studiach stacjonarnych** | **na studiach niestacjonarnych** |
| **Godziny kontaktowe studenta (w ramach zajęć):** |
| liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia | **45** | **28** |
| **Praca własna studenta (indywidualna praca studenta związana z zajęciami):** |
| Zapoznanie z literaturą | 10 | 15 |
| Przygotowanie sprawozdań | 15 | 22 |
| Przygotowanie do zaliczenia wykładu | 15 | 20 |
| **suma godzin:** | **85** | **85** |
| **liczba pkt ECTS przypisana do zajęć:** (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta) | **3** | **3** |

12. Literatura zajęć

|  |
| --- |
| **Literatura obowiązkowa:**1. Joe Gray, **Socjotechniki w praktyce. Podręcznik etycznego hakera**, Helion 2023
2. Christopher Hadnagy **,Socjotechnika. Sztuka zdobywania władzy nad umysłami. Wydanie II**, Helion 2020
 |
| **Literatura zalecana / fakultatywna:**1. Christopher Hadnagy, Michele Fincher, Robin Dreeke (Foreword), **Mroczne odmęty phishingu. Nie daj się złowić**, Helion 2023
2. Megan Roddie, Jason Deyalsingh, Gary J. Katz, **Inżynieria detekcji cyberzagrożeń w praktyce. Planowanie, tworzenie i walidacja mechanizmów wykrywania zagrożeń**, Helion 2022
3. Kunal Sehgal, Nikolaos Thymianis, **Cyberbezpieczeństwo i strategie blue teamów. Walka z cyberzagrożeniami w Twojej organizacji**, Helion 2024.
 |

13. Informacje dodatkowe

|  |  |
| --- | --- |
| imię i nazwisko sporządzającego | dr inż. Łukasz Lemieszewski, mgr inż. Szymon Prochacki |
| data sporządzenia / aktualizacji | 10.06.2024 r.  |
| dane kontaktowe (e-mail) | llemieszewski@ajp.edu.pl |
| podpis |  |

|  |  |  |
| --- | --- | --- |
| Akademia_logo (4) | **Wydział** | Techniczny |
| **Kierunek** | Informatyka |
| **Poziom studiów** | drugiego stopnia |
| **Forma studiów** | stacjonarna/niestacjonarna |
| **Profil studiów** | praktyczny |
| **Pozycja w planie studiów (lub kod przedmiotu)** | D.4.6 |

**KARTA ZAJĘĆ**

**1. Informacje ogólne**

|  |  |
| --- | --- |
| Nazwa zajęć | Algorytmy szyfrujące i deszyfrujące w systemach przetwarzania danych |
| Punkty ECTS | 3 |
| Rodzaj zajęć | ~~obowiązkowe~~/obieralne |
| Moduł/specjalizacja | Cyberbezpieczeństwo |
| Język, w którym prowadzone są zajęcia | Polski/Angielski |
| Rok studiów | 1 |
| Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia | dr inż. Łukasz Lemieszewskimgr inż. Szymon Prochacki |

**2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze**

|  |  |  |  |
| --- | --- | --- | --- |
| **Forma zajęć** | **Liczba godzin****Stacjonarne/niestacjonarne** | **Rok studiów/semestr** | **Punkty ECTS** (zgodnie z programem studiów) |
| **wykład** | **15/10** | **2/1;** | **3** |
| **laboratoria** | **30/18** | **2/1;** |

**3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć**

|  |
| --- |
| Student przedmiotu Zarządzanie bezpieczeństwem w systemach sieciowych posiada wiedzę, umiejętności i kompetencje społeczne, które nabył podczas realizacji przedmiotu operacje cyberbezpieczeństwa. |

**4. Cele kształcenia**

|  |
| --- |
| C1 – Zapoznanie z definicjami i standardami oraz unormowaniami dotyczącymi zagadnień odnoszących się do podstaw kryptografii i bezpieczeństwa systemów kryptograficznych.C2 – Analiza algorytmów szyfrujących.C3 - Stosowanie poznanych narzędzi i metod oraz technik projektowania, konfigurowania, testowania w eliminowaniu podatności oraz przeciwdziałaniu skutkom incydentów bezpieczeństwa kryptograficznych.C4 – Diagnozowanie, eliminowanie oraz przewidywanie zagrożenia bezpieczeństwa systemów kryptograficznych. |

**5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych**

|  |  |  |
| --- | --- | --- |
| **Symbol efektu uczenia się** | **Opis efektu uczenia się** | **Odniesienie do efektu kierunkowego** |
| **WIEDZA** |
| W\_01 | Student ma elementarną wiedzę z zakresu podstaw informatyki obejmującą algorytmy szyfrujące i deszyfrujące w systemach przetwarzania danych. | K\_W03 |
| W\_02 | Student orientuje się w obecnym stanie oraz trendach rozwojowych bezpieczeństwa systemów kryptograficznych. | K\_W08 |
| **UMIEJĘTNOŚCI** |
| U\_01 | Student potrafi ocenić ryzyko i bezpieczeństwo baz danych, aplikacji internetowych, systemów i sieci komputerowych, stosując techniki oraz narzędzia sprzętowe i programowe. | K\_U05 |
| U\_02 | Student potrafi zaplanować i przeprowadzić symulację oraz przeprowadzić eksperyment pomiarowy z zakresu bezpieczeństwa systemów kryptograficznych; potrafi przedstawić otrzymane wyniki w formie liczbowej oraz dokonać ich interpretacji i wyciągnąć właściwe wnioski | K\_U16 |
| **KOMPETENCJE SPOŁECZNE** |
| K\_01 | Student prawidłowo identyfikuje i rozstrzyga dylematy bezpieczeństwa systemów kryptograficznych | K\_K02 |

**6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć** (zgodnie z programem studiów):

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści wykładów**  | **Liczba godzin na studiach** |
| **stacjonarnych** | **niestacjonarnych** |
| W1 | Omówienie karty przedmiotu (cele i Efekty uczenia się, treści programowe, formy i warunki zaliczenia). Szyfry i ataki na nie. | 1 | 1 |
| W2 | Szyfry P&P i szyfry przedkomputerowe. Kryptologia historyczna | 2 | 1 |
| W3 | Liczby pierwsze. Wprowadzenie do elementarnej teorii liczb z przykładami. | 2 | 2 |
| W4 | Idee matematyczne stojące za nowoczesną (asymetryczną) kryptografią. Funkcje skrótu, podpisy cyfrowe i PKI | 2 | 1 |
| W5 | Krzywa eliptyczna Kryptografia (ECC). Podstawy współczesnego szyfrowania symetrycznego. | 2 | 1 |
| W6 | Szyfry homomorficzne. Lekkie wprowadzenie do krat | 2 | 1 |
| W7 | Rozwiązywanie logarytmów dyskretnych i rozkład na czynniki | 2 | 1 |
| W8 | Przyszłe wykorzystanie kryptografii. Zaliczenie wykładu. | 2 | 2 |
|  | **Razem liczba godzin wykładów**  | **15** | **10** |

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści laboratoriów** | **Liczba godzin na studiach** |
| **stacjonarnych** | **niestacjonarnych** |
| L1 | Omówienie zakresu zajęć laboratoryjnych. Wprowadzenie do szyfrów i ataków na nie. | 2 | 1 |
| L2 | Liczby pierwsze, pseudopierwsze i testowanie pierwszości. | 2 | 1 |
| L3 | Podstawowe pojęcia kryptograficzne i szyfry klasyczne. | 2 | 1 |
| L4 | Podzielność i kongruencje. | 2 | 1 |
| L5 | Grupy skończone. | 2 | 1 |
| L6 | Ciała skończone. | 2 | 1 |
| L7 | Wielomiany o współczynnikach w ciele skończonym. | 2 | 1 |
| L8 | Pierścienie przemienne z jedynką. | 2 | 1 |
| L9 | Szyfry z kluczem publicznym. | 2 | 1 |
| L10 | Szyfry z kluczem prywatnym. | 2 | 1 |
| L11 | Efektywna implementacja algorytmów kryptograficznych. | 2 | 1 |
| L12 | Uwierzytelnianie. | 2 | 1 |
| L13 | Dzielenie tajemnic. | 2 | 1 |
| L14 | Funkcje skrótu. | 2 | 1 |
| L15 | Zagadnienia probabilistyczne w kryptografii. Wystawienie ocen. | 2 | 1 |
|  | **Razem liczba godzin laboratoriów** | **30** | **18** |

**7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć**

|  |  |  |
| --- | --- | --- |
| **Forma zajęć** | **Metody dydaktyczne (wybór z listy)** | **Środki dydaktyczne** |
| Wykład | M1, M2 - wykład informacyjny jako prelekcja z objaśnieniami połączone z dyskusją oraz możliwością prezentacji prac własnych zrealizowanych jako prezentacje z przeglądu literatury | projektor, dostęp do Internetu,prezentacja multimedialna |
| Laboratoria | M5 - ćwiczenia doskonalące umiejętność pozyskiwania informacji ze źródeł internetowych i doskonalących obsługę narzędzi informatycznych oraz analiza sprawozdań przedstawionych przez studentów | Komputer z oprogramowaniem IDE dla aplikacji WEB oraz dostępem do Internetu. |

**8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta**

**8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć**

|  |  |  |
| --- | --- | --- |
| **Forma zajęć** | **Ocena formująca (F)** **–** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)** | **Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)** |
| Wykład | F1 - sprawdzian pisemny (kolokwium cząstkowe testy z pytaniami wielokrotnego wyboru i pytaniami otwartymi)  | P1 – zaliczenie pisemne |
| Laboratoria | F2 – obserwacja/aktywność (przygotowanie do zajęć, ocena ćwiczeń wykonywanych podczas zajęć), F5 - ćwiczenia praktyczne (ćwiczenia z wykorzystaniem sprzętu i oprogramowania fachowego) | P2 – kolokwium praktyczne  |

**8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x”)**

|  |  |  |
| --- | --- | --- |
| **Symbol efektu** | Wykład | Laboratoria |
| F1 | F2 | F5 |
| W\_01 | x |  |  |
| W\_02 | x |  |  |
| U\_01 |  | x | x |
| U\_02 |  | x | x |
| K\_01 | x | x | x |

# 9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Z każdej formy prowadzonych zajęć uzyskaną ilość punktów przelicza się na wartość procentową. Ocena końcowa jest zgoda w progami oceniania zamieszczonymi w tabeli 1.
2. *Tab. 1. Progi ocenia procentowego*

|  |  |
| --- | --- |
| **Wynik procentowy** | **Ocena** |
| 0-50 % | niedostateczny (2.0) |
| 51-60 %. | dostateczny (3.0) |
| 61-70 % | dostateczny plus (3.5) |
| 71-80 % | dobry (4.0) |
| 81-90 % | dobry plus (4.5) |
| 91-100 % | bardzo dobry (5.0) |

 |

10. Forma zaliczenia zajęć

|  |
| --- |
| Zaliczenie z oceną |

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

|  |  |
| --- | --- |
| **Forma aktywności studenta** | **Liczba godzin** |
| **na studiach stacjonarnych** | **na studiach niestacjonarnych** |
| **Godziny kontaktowe studenta (w ramach zajęć):** |
| liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia | **45** | **28** |
| **Praca własna studenta (indywidualna praca studenta związana z zajęciami):** |
| Zapoznanie z literaturą | 5 | 10 |
| Przygotowanie sprawozdań | 10 | 17 |
| Przygotowanie do zaliczenia | 15 | 20 |
| **suma godzin:** | **75** | **75** |
| **liczba pkt ECTS przypisana do zajęć:** (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta) | **3** | **3** |

12. Literatura zajęć

|  |
| --- |
| **Literatura obowiązkowa:**1. Bernhard Esslinger, **Learning and Experiencing Cryptography with CrypTool and SageMath**, ARTECH HOUSE, 20242. Materiały kursu CISCO pt. **Ethical hacker** , dostępny po zalogowaniu na platformie skillsforall.com, 2023.3. Stallings W., Brown L., **Bezpieczeństwo systemów informatycznych.** **Zasady i praktyka, Tom I i II,** Helion, Gliwice 2019. |
| **Literatura zalecana / fakultatywna:**1. Dominic Chell, Shaun Colley, Tyrone Erasmus, Ollie Whitehouse, **Bezpieczeństwo aplikacji mobilnych. Podręcznik hakera**, Helion 2023.2. O. Santos, Cisco **Cyberops Associate Cbrops 200-201 Official Cert Guide**, CISCO, 2020.3. Vickie Li ; przekład: Lech Lachowski, **Bug bounty bootcamp : przewodnik po tropieniu i zgłaszaniu luk w zabezpieczeniach** , Gliwice, Helion, 2023.3. Sedgewick, Robert, **Algorytmy**, Helion 2012.4. Wirth, Niklaus, **Algorytmy + struktury danych,** Wydawnictwa Naukowo-Techniczne, 2004. |

13. Informacje dodatkowe

|  |  |
| --- | --- |
| imię i nazwisko sporządzającego | dr inż. Łukasz Lemieszewski,  |
| data sporządzenia / aktualizacji | 10.06.2024 r.  |
| dane kontaktowe (e-mail) | llemieszewski@ajp.edu.pl |
| podpis |  |

|  |  |  |
| --- | --- | --- |
| Akademia_logo (4) | **Wydział** | Techniczny |
| **Kierunek** | Informatyka |
| **Poziom studiów** | drugiego stopnia |
| **Forma studiów** | stacjonarna/niestacjonarna |
| **Profil studiów** | praktyczny |
| **Pozycja w planie studiów (lub kod przedmiotu)** | D.4.7. |

**KARTA ZAJĘĆ**

**1. Informacje ogólne**

|  |  |
| --- | --- |
| Nazwa zajęć | Zaawansowane bezpieczeństwo sieci i VPN |
| Punkty ECTS | 4 |
| Rodzaj zajęć | ~~obowiązkowe~~/obieralne |
| Moduł/specjalizacja | Sieci komputerowe i systemy teleinformatyczne |
| Język, w którym prowadzone są zajęcia | Polski/Angielski |
| Rok studiów | 2 |
| Imię i nazwisko koordynatora zajęć oraz osób prowadzących zajęcia | mgr inż. Robert Suchocki, mgr inż. Grzegorz Remiszewski |

**2. Formy dydaktyczne prowadzenia zajęć i liczba godzin w semestrze**

|  |  |  |  |
| --- | --- | --- | --- |
| **Forma zajęć** | **Liczba godzin****Stacjonarne/niestacjonarne** | **Rok studiów/semestr** | **Punkty ECTS** (zgodnie z programem studiów) |
| **wykład** | **15/10** | **2/3;** | **4** |
| **laboratoria** | **30/18** | **2/3;** |
| **projekt** | **15/10** | **2/3;** |

**3. Wymagania wstępne, z uwzględnieniem sekwencyjności zajęć**

|  |
| --- |
| Student przedmiotu Zarządzanie bezpieczeństwem w systemach sieciowych posiada wiedzę, umiejętności i kompetencje społeczne, które nabył podczas realizacji przedmiotu wprowadzenie do sieci komputerowych, routing i przełączanie w sieciach LAN i WAN, cyberbezpieczeństwo. |

**4. Cele kształcenia**

|  |
| --- |
| C1 - Poznanie zaawansowanych zagrożeń sieciowych, ich identyfikacja i analiza w celu skutecznemu im przeciwdziałaniuC2 - Analiza i konfiguracja zaawansowanych zabezpieczeń sieciowych w celu zapewnienia optymalnej ochrony sieci.C3 – Projektowanie transmisji szyfrowanej oraz wdrażanie i zarządzanie VPN typu site-to-site, VPN typu remote-access i VPN typu SSL. |

**5. Efekty uczenia się dla zajęć wraz z odniesieniem do efektów kierunkowych**

|  |  |  |
| --- | --- | --- |
| **Symbol efektu uczenia się** | **Opis efektu uczenia się** | **Odniesienie do efektu kierunkowego** |
| **WIEDZA** |
| W\_01 | Student ma elementarną wiedzę z zakresu podstaw informatyki obejmującą bezpieczeństwo sieci i VPN | K\_W04 |
| W\_02 | Student orientuje się w obecnym stanie oraz trendach rozwojowych systemów i sieci teleinformatycznych z naciskiem na VPN | K\_W09 |
| **UMIEJĘTNOŚCI** |
| U\_01 | Student potrafi ocenić ryzyko i bezpieczeństwo baz danych, aplikacji internetowych, systemów i sieci komputerowych, stosując techniki oraz narzędzia sprzętowe i programowe. | K\_U03 |
| U\_02 | Student potrafi zaplanować i przeprowadzić symulację oraz przeprowadzić eksperyment pomiarowy z zakresu bezpieczeństwa systemów; potrafi przedstawić otrzymane wyniki w formie liczbowej oraz dokonać ich interpretacji i wyciągnąć właściwe wnioski | K\_U16 |
| **KOMPETENCJE SPOŁECZNE** |
| K\_01 | Student prawidłowo identyfikuje i rozstrzyga dylematy bezpieczeństwa transmisji danych w sieci i za pomocą wirtualnych sieci prywatnych. | K\_K04 |

**6. Treści programowe oraz liczba godzin na poszczególnych formach zajęć** (zgodnie z programem studiów):

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści wykładów**  | **Liczba godzin na studiach** |
| **stacjonarnych** | **stacjonarnych** |
| W1 | Wybrane zagadnienia kryptologii i kryptografii. | 1 | 1 |
| W2 | Bezpieczeństwo protokołu BGP i OSPF. | 2 | 1 |
| W3 | Koncepcje współczesnego bezpieczeństwa systemy SIEM, IPS, IDS. | 2 | 1 |
| W3 | Koncepcja Virtual Routing and Forwarding. | 1 | 1 |
| W4 | Tunele VPN GRE. | 2 | 1 |
| W5 | IPsec VPN. | 2 | 1 |
| W6 | Dynamic Multipoint VPN. | 2 | 1 |
| W7 | Sieci MPLS. | 2 | 2 |
| W8 | Sieci MPLS. | 2 | 1 |
|  | **Razem liczba godzin wykładów**  | **15** | **10** |

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści laboratoriów** | **Liczba godzin na studiach** |
| **stacjonarnych** | **stacjonarnych** |
| L1 | Bezpieczeństwo protokołu BGP i OSPF. | 4 | 2 |
| L2 | Koncepcja Virtual Routing and Forwarding. | 2 | 2 |
| L3 | Tunele VPN GRE. | 4 | 2 |
| L4 | IPsec VPN. | 4 | 2 |
| L5 | Dynamic Multipoint VPN. | 4 | 2 |
| L6 | Sieci MPLS.  | 4 | 4 |
| L7 | Konteneryzacja i wirtualizacja aplikacji. | 4 | 2 |
| L8 | Kolokwium zaliczające. | 4 | 2 |
|  | **Razem liczba godzin laboratoriów** | **30** | **18** |

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Treści projektów** | **Liczba godzin na studiach** |
| **stacjonarnych** | **stacjonarnych** |
| P1 | Określenie celów i wymagań klienta. | 2 | 2 |
| P2 | Analiza wymagań i celów. Studium przypadku. | 2 | 1 |
| P3 | Harmonogram prac. Wykresy Ganta. | 2 | 2 |
| P4 | Implementacja rozwiązania w środowisku wirtualnym. | 2 | 1 |
| P5 | Implementacja rozwiązaniaw środowisku onpromice | 2 | 1 |
| P6 | Budżetowanie zaproponowanego rozwiązania. Określenie TCO. | 2 | 1 |
| P7 | Dokumentacja zaproponowanego rozwiązania. | 2 | 1 |
| P8 | Obrona projektów. Wystawienie ocen. | 1 | 1 |
|  | **Razem liczba godzin wykładów**  | **15** | **10** |

**7. Metody oraz środki dydaktyczne wykorzystywane w ramach poszczególnych form zajęć**

|  |  |  |
| --- | --- | --- |
| **Forma zajęć** | **Metody dydaktyczne (wybór z listy)** | **Środki dydaktyczne** |
| Wykład | M1, M2 - wykład informacyjny jako prelekcja z objaśnieniami połączone z dyskusją oraz możliwością prezentacji prac własnych zrealizowanych jako prezentacje z przeglądu literatury | projektor, dostęp do Internetu,prezentacja multimedialna |
| Laboratoria | M5 - ćwiczenia doskonalące umiejętność pozyskiwania informacji ze źródeł internetowych i doskonalących obsługę narzędzi informatycznych  | Komputer z środowiskiem GNS3 oraz dostępem do Internetu, Urządzenia sieciowe zgodnie ze specyfikacją CCNA Security |
| Projekt | M5 - ćwiczenia doskonalące umiejętność pozyskiwania informacji ze źródeł internetowych i doskonalących obsługę narzędzi informatycznych oraz obrona projektu końcowego. | Jednostka komputerowa wyposażona w oprogramowanie oraz z dostępem do sieci Internetu |

**8. Sposoby (metody) weryfikacji i oceny efektów uczenia się osiągniętych przez studenta**

**8.1. Sposoby (metody) oceniania osiągnięcia efektów uczenia się na poszczególnych formach zajęć**

|  |  |  |
| --- | --- | --- |
| **Forma zajęć** | **Ocena formująca (F)** **–** wskazuje studentowi na potrzebę uzupełniania wiedzy lub stosowania określonych metod i narzędzi, stymulujące do doskonalenia efektów pracy **(wybór z listy)** | **Ocena podsumowująca (P) –** podsumowuje osiągnięte efekty uczenia się **(wybór z listy)** |
| Wykład | F1 - sprawdzian pisemny (kolokwium cząstkowe testy z pytaniami wielokrotnego wyboru i pytaniami otwartymi)  | P1 – egzamin pisemny w formie pytań testowych |
| Laboratoria | F2 – obserwacja/aktywność (przygotowanie do zajęć, ocena ćwiczeń wykonywanych podczas zajęć), F5 - ćwiczenia praktyczne (ćwiczenia z wykorzystaniem sprzętu i oprogramowania fachowego) | P2 – kolokwium praktyczne  |
| Projekt | F3 – dokumentacja projektu F4 – wystąpienie – analiza projektu | P4 – praca pisemna - projekt |

**8.2. Sposoby (metody) weryfikacji osiągnięcia przedmiotowych efektów uczenia się (wstawić „x”)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Symbol efektu** | Wykład | Laboratoria | Projekt |
| F1 | F2 | F5 | F3 | F4 | P4 |
| W\_01 | x |  |  | x | x | x |
| W\_02 | x |  |  | x | x | x |
| U\_01 |  | x | x | x | x | x |
| U\_02 |  | x | x | x | x | x |
| K\_01 | x | x | x | x | x | x |

# 9. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Z każdej formy prowadzonych zajęć uzyskaną ilość punktów przelicza się na wartość procentową. Ocena końcowa jest zgoda w progami oceniania zamieszczonymi w tabeli 1.
2. *Tab. 1. Progi ocenia procentowego*

|  |  |
| --- | --- |
| **Wynik procentowy** | **Ocena** |
| 0-50 % | niedostateczny (2.0) |
| 51-60 %. | dostateczny (3.0) |
| 61-70 % | dostateczny plus (3.5) |
| 71-80 % | dobry (4.0) |
| 81-90 % | dobry plus (4.5) |
| 91-100 % | bardzo dobry (5.0) |

 |

10. Forma zaliczenia zajęć

|  |
| --- |
| egzamin z oceną |

11. Obciążenie pracą studenta (sposób wyznaczenia punktów ECTS):

|  |  |
| --- | --- |
| **Forma aktywności studenta** | **Liczba godzin** |
| **na studiach stacjonarnych** | **na studiach niestacjonarnych** |
| **Godziny kontaktowe studenta (w ramach zajęć):** |
| liczba godzin pracy studenta z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia | **45** | **28** |
| **Praca własna studenta (indywidualna praca studenta związana z zajęciami):** |
| Zapoznanie z literaturą | 10 | 12 |
| Przygotowanie sprawozdań | 15 | 20 |
| Przygotowanie projektu | 15 | 20 |
| Przygotowanie do egzaminu | 15 | 20 |
| **suma godzin:** | **100** | **100** |
| **liczba pkt ECTS przypisana do zajęć:** (1 pkt ECTS odpowiada od 25 do 30 godzin aktywności studenta) | **4** | **4** |

12. Literatura zajęć

|  |
| --- |
| **Literatura obowiązkowa:**1. Raymond Lacoste, Brad Edgeworth, **CCNP Enterprise Advenced Routing : Enarsi 300-410:Official Cert Guide**, Hoboken : Cisco Press, 2020.2. Brad Edgeworth, Ramiro Garza Rios, Jason Gooley, David Hucaby, **CCNP and CCIE Enterprise Core:ENCOR 350-401 : Official Cert Guide,** Indianapolis : Cisco Press, 2020.3. Adam Józefiok **CCNA 200-301 : zostań administratorem sieci komputerowych Cisco**, Gliwice, Helion 20204. Omar Santos, **CCNP and CCIE Security Core : SCOR 350-701:Official Cert Guide,** Hoboken : Cisco Press, 2020 |
| **Literatura zalecana / fakultatywna:**1. Jan Just Keijser, **OpenVPN Cookbook. Get the most out of OpenVPN by exploring it's advanced features**. 2017. 2. Lin Song, **Build Your Own VPN Server: A Step by Step Guide**, 2023  |

13. Informacje dodatkowe

|  |  |
| --- | --- |
| imię i nazwisko sporządzającego | mgr inż. Robert Suchocki, mgr inż. Grzegorz Remiszewski |
| data sporządzenia / aktualizacji | 10.06.2024 r.  |
| dane kontaktowe (e-mail) | gremiszewski@ajp.edu.pl |
| podpis |  |