# **KARTA KURSU**

|  |  |  |
| --- | --- | --- |
| Nazwa | Bezpieczeństwo systemów informatycznych |  |
| Nazwa w j. ang. | Security of IT systems |  |

|  |  |  |
| --- | --- | --- |
| Koordynator | Dr hab. Andrzej Kruk | Zespół dydaktyczny |
| Dr hab. Andrzej Kruk |
|  |  |
| Punktacja ECTS\* | 1 |

Opis kursu (cele kształcenia)

|  |
| --- |
| Zapoznanie studentów z podstawowymi problemami bezpieczeństwa systemów informatycznych, w tym wykorzystywania, konfigurowania i administrowania mechanizmami bezpieczeństwa na poziomie systemowym i aplikacyjnym, ze szczególnym uwzględnieniem mechanizmów i protokołów sieciowych. Uzyskanie przez studentów umiejętności efektywnego posługiwania się mechanizmami kryptograficznymi, kontroli dostępu, filtracji ruchu sieciowego, tuneli wirtualnych oraz narzędziami zabezpieczeń warstwy aplikacyjnej. |

Warunki wstępne

|  |  |  |
| --- | --- | --- |
| Wiedza | Znajomość obsługi usług sieciowych, zasada działania systemów operacyjnych, zasada działania sieci lokalnych i Internet. Znajomość zagrożeń sieciowych. |  |
| Umiejętności | Obsługa systemów operacyjnych, konfiguracja sieci lokalnych, tworzenie algorytmów, umiejętności programistyczne. |  |
| Kursy | Podstawy informatyki i systemów informatycznych, Matematyka – kurs podstawowy, Algorytmy i struktury danych, Cyberbezpieczeństwo |  |

Efekty uczenia się

|  |  |  |
| --- | --- | --- |
| Wiedza | Efekt uczenia się dla kursu | Odniesienie do efektów kierunkowych |
| W01, Wykazuje wiedzę dotyczącą rozpoznania zagrożeń podczas użytkowania systemów operacyjnych, sieci komputerowych.  W02. Posiada wiedzę na temat o najnowszych rozwiązaniach programistycznych oraz o osiągnięciach w informatyce, w aspekcie monitorowania bezpieczeństwa i metod ochrony –  W03.Zna protokoły i standardy dotyczące bezpieczeństwa systemów informatycznych, w tym wiedzę dotyczącą usług sieciowych i aplikacji użytkowych, takich jak: tunele VPN, zapory sieciowe, inne narzędzia kryptograficzne oraz IDS  W05. Ma wiedzę pozwalającą na właściwy dobór i implementacje w praktyce narzędzi informatycznych do zapewnienia uwierzytelniania, ochrony poufności i integralności danych i komunikacji –  W06. Zna podstawowe metody, techniki i narzędzia stosowane przy rozwiązywaniu prostych zadań  informatycznych z zakresu zabezpieczeń systemów operacyjnych, sieci lokalnych, Internet,  W07. Rozumie znaczenie kodeksu etycznego w pracy informatyka, potrafi oszacować niebezpieczeństwo i wskazać wrażliwe/krytyczne punkty oprogramowania i sieci. | K\_W06, K\_W07  K\_W06, K\_W07  K\_W06, K\_W07  K\_W06, K\_W07  K\_W06, K\_W07  K\_W06, K\_W07 |

|  |  |  |
| --- | --- | --- |
| Umiejętności | Efekt uczenia się dla kursu | Odniesienie do efektów kierunkowych |
| U01. Potrafi korzystać z literatury popularnonaukowej i fachowej, ogólnodostępnych baz danych z analizą krytyczną.  U02. Umie implementować w praktyce narzędzia informatyczne, integrować je z istniejącym systemami, oraz analizować i wyciągać wnioski ich działania  U03. Umie wskazać na istniejące i potencjalne zagrożenia w systemach komputerowych i im skutecznie zapobiegać  U04. Skutecznie analizuje zalety i wady systemów informatycznego,  U05. Umie zaprojektować sieć komputerową oraz  zaimplementować w niej standardowe mechanizmy  bezpieczeństwa. | K\_U12, K\_U23  K\_U12  K\_U12  K\_U12  K\_U13 |

|  |  |  |
| --- | --- | --- |
| Kompetencje społeczne | Efekt uczenia się dla kursu | Odniesienie do efektów kierunkowych |
| K01, Na poziomie profesjonalnym nawiązuje współpracę z otoczeniem dotyczącą projektowania bezpieczeństwa i monitorowania systemów teleinformatycznych  K02, Rozumie konieczność ustawicznego monitorowania stanu wiedzy i pogłębiania swoich umiejętności wraz z rozwojem budowy i zarządzania systemami teleinformatycznych w aspekcie bezpieczeństwa | K\_K02  K\_K01 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Organizacja | | | | | | | | | | | | | |
| Forma zajęć | Wykład  (W) | Ćwiczenia w grupach | | | | | | | | | | | |
| A |  | K |  | L |  | S |  | P |  | E |  |
| Liczba godzin | 15 |  | |  | | 15 | |  | |  | |  | |

Opis metod prowadzenia zajęć

|  |
| --- |
| Wykład klasyczny wsparty prezentacjami multimedialnymi oraz dyskusją  Praca laboratoryjna z komputerami, rozwiazywanie zadań, analiza tekstu źródłowego. |

Formy sprawdzania efektów uczenia się

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | E – learning | Gry dydaktyczne | Ćwiczenia w szkole | Zajęcia terenowe | Praca laboratoryjna | Projekt indywidualny | Projekt grupowy | Udział w dyskusji | Referat | Praca pisemna (esej) | Egzamin ustny | Egzamin pisemny | Inne |
| W01 |  |  |  |  |  |  |  | X |  |  |  |  |  |
| W02 |  |  |  |  |  |  |  | X |  |  |  |  |  |
| W03 |  |  |  |  |  |  |  | X |  |  |  |  |  |
| W04 |  |  |  |  |  |  |  | X |  |  |  |  |  |
| W05 |  |  |  |  |  |  |  | X |  |  |  |  |  |
| W06 |  |  |  |  |  |  |  | X |  |  |  |  |  |
| W07 |  |  |  |  |  |  |  | X |  |  |  |  |  |
| U01 |  |  |  |  | X |  |  | X |  |  |  |  |  |
| U02 |  |  |  |  | X |  |  | X |  |  |  |  |  |
| U03 |  |  |  |  | X |  |  |  |  |  |  |  |  |
| U04 |  |  |  |  | X |  |  |  |  |  |  |  |  |
| U05 |  |  |  |  | X |  |  |  |  |  |  |  |  |
| K01 |  |  |  |  |  |  |  | X |  |  |  |  |  |
| K02 |  |  |  |  |  |  |  | X |  |  |  |  |  |

|  |  |
| --- | --- |
| Kryteria oceny | Aktywność na zajęciach, udział w dyskusji, ocena z zadań. |

|  |  |
| --- | --- |
| Uwagi |  |

Treści merytoryczne (wykaz tematów)

|  |
| --- |
| 1. Wprowadzenie do współczesnych problemów bezpieczeństwa IT. Polityka bezpieczeństwa, Podstawy prawa polskiego i UE.  2. Klasyfikacja i podział zagrożeń, źródła ataków i aktualnych informacji.  3. Podstawy bezpieczeństwa: poufność, dostępność i integralność; Testy penetracyjne - techniki skanowania  4. Bezpieczeństwo baz danych  5. Klasy bezpieczeństwa w systemach Windows oraz Linux, BSD. Zdalne rozpoznawanie systemów operacyjnych i sniffing. Mechanizmy kontroli dostepu  6. Bezpieczeństwo podczas transmisji i podczas przetwarzania danych ; mechanizmy bezpieczeństwa: technologie, polityki i procedury, czynnik ludzki. Techniki enumeracji  7. Monitorowanie systemów IT pod kątem zagrożeń (skanery portów, skanery podatności, oprogramowanie antywirusowe, systemy IPS/IDS).  8. Konfiguracja zapór sieciowych, Kerberos, BASH  9. Kontrola dostępu, IPtables  10. Zapewnienie bezpieczeństwa w infrastrukturze IT, Metody uwierzytelniania  11. Kryptograficzne mechanizmy bezpieczeństwa (metody szyfrowania, klucze, funkcje skrótu, certyfikaty i podpisy cyfrowe). Ochrona poczty elektronicznej  12. Bezpieczne połączenia SSH, VPN, tokeny,  13. Problemy bezpieczeństwa specyficzne dla technologii bezprzewodowych.  14. Metody ataków na systemy informatyczne ich narzędzia  15. Wprowadzenie do algorytmów kwantowych , qubit, splątanie, teleportacja, przyszłość informatyki |

Wykaz literatury podstawowej

|  |
| --- |
| * D. R. Ahmad, Hack Proofing Your Network, Syngress Publ. 2001. * C. P. Pfleeger. Security in Computing. Prentice Hall International, 1997. * Patrick Engebretson, Hacking i testy penetracyjne. Podstawy, Helion * Mark Stamp, "Information Security: Principles and Practice", Wiley, 2011 * William Stallings, "Cryptography and Network Security: Principles and Practice", Pearson Education, * William Stallings, Lawrie Brown, "Computer Security: Principles and Practice", Pearson Education, * Materiały szkoleniowe CISCO * Doktryna Cyberbezpieczeństwa RP. * Ustawa o krajowym systemie cyberbezpieczeństwa. * Polityka Ochrony Cyberprzestrzeni RP. |

Wykaz literatury uzupełniającej

|  |
| --- |
| M. Schiffman, Hacker's Challenge, Osborne/McGraw-Hill 2001.  W. Stallings. Network and Internetwork Security, Principles and Practice. Prentice Hall International, 1994.  D. Atkins. Internet Security. Professional Reference. New Riders Publishing, 1997.  Rozporządzenie prezesa Rady Ministrów ws. podstawowych wymagań bezpieczeństwa teleinformatycznego.  Krajowy Plan Zarządzania Kryzysowego. RCB. 2020.  Michał Szychowiak, "Bezpieczeństwo systemów informatycznych. Zaawansowane ćwiczenia w systemach Windows i Linux", WPP, 2017  John Savard, "A Cryptographic Compendium" |

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta)

|  |  |  |
| --- | --- | --- |
| liczba godzin w kontakcie z prowadzącymi | Wykład | 15 |
| Konwersatorium (ćwiczenia, laboratorium itd.) | 15 |
| Pozostałe godziny kontaktu studenta z prowadzącym |  |
| liczba godzin pracy studenta bez kontaktu z prowadzącymi | Lektura w ramach przygotowania do zajęć |  |
| Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu |  |
| Przygotowanie projektu lub prezentacji na podany temat (praca w grupie) |  |
| Przygotowanie do egzaminu/zaliczenia |  |
| Ogółem bilans czasu pracy | | 30 |
| Liczba punktów ECTS w zależności od przyjętego przelicznika | | 1 |