**KARTA KURSU**

|  |  |
| --- | --- |
| Nazwa | Administracja i bezpieczeństwo systemów sieciowych |
| Nazwa w j. ang. | Administration and security of network systems |

|  |  |  |
| --- | --- | --- |
| Koordynator |  | Zespół dydaktyczny |
| dr hab. Olesia Afanasieva, prof. UP |
|  |  |
| Punktacja ECTS\* | 3 |

Opis kursu (cele kształcenia)

|  |
| --- |
| Celem kursu jest zapoznanie studenta z podstawowymi pojęciami i współczesnymi problemami związanymi z bezpieczeństwem sieci komputerowych:  - administracja nad siecią komputerową;  - network administrator – obowiązki zadania;  - podstawy monitorowania sieci;  - system zautomatyzowanego wspomagania;  - ochroną informacji w sieciach, podstawowe pojęcia o wirusach, wykorzystanie „firewall”;  - podstawowymi technikami i protokołami identyfikacyjnymi;  - podstawami zabezpieczenia bezpiecznych połączeń;  - ochroną informacji w sieci World Wide Web;  - algorytmami i protokołami, które zapewniają bezpieczeństwo sieci;  - sieciowymi systemami wykrywania intruzów;  - modelami kontroli dostępu.  Kurs prowadzony jest w języku polskim. |

Warunki wstępne

|  |  |
| --- | --- |
| Wiedza | Posiada wiedzę z zakresu teorii matematycznej: elementy teorii liczb, struktury algebraiczne, złożoność obliczeniowa, elementy teorii informacji.  Posiada wiedzę z zakresu kryptografii i szyfrowania danych, kryptoanalizy. |
| Umiejętności | Umiejętność zapisu podstawowych algorytmów i tworzenia prostych programów komputerowych przy użyciu języka programowania C/C++.  Potrafi przeprowadzić standardowe algorytmy szyfrowania danych i opracować podstawowe programy szyfrujące. |
| Kursy | --- |

Efekty uczenia się

|  |  |  |
| --- | --- | --- |
| Wiedza | Efekt uczenia się dla kursu | Odniesienie do efektów kierunkowych |
| W01 Ma pogłębioną i uporządkowaną wiedzę z zakresu informatyki technicznej i telekomunikacji;    W02 Ma pogłębioną i uporządkowaną wiedzę z zakresu bezpieczeństwa informacyjnego  W03 Zna strukturę zagrożeń, metody pomiaru oraz prognozowania zagrożeń;  W04 Zna zasady modelowania procesów deterministycznych i stochastycznych oraz możliwości ich zastosowania w obszarze bezpieczeństwa;  W05 Ma poszerzoną i ugruntowaną wiedzę z zakresu wybranych języków programowania, w tym języków wizualnych, skryptowych i języków opisu sprzętu oraz ich zastosowań przemysłowych;  W06 Zna zaawansowane metody modelowania i symulacji systemów technicznych z użyciem odpowiednich narzędzi informatycznych. | K\_W01  K\_W05  K\_W07  K\_W08  K\_W01  K\_W01 |

|  |  |  |
| --- | --- | --- |
| Umiejętności | Efekt uczenia się dla kursu | Odniesienie do efektów kierunkowych |
| U01 Rozpoznaje problemy inżynierii bezpieczeństwa, do rozwiązania, których powinien zastosować modelowanie matematyczne, metody statystyczne oraz informatyczne; potrafi wykorzystać dostępne algorytmy i programy komputerowe;  U02 Potrafi pozyskać informacje z literatury, baz danych oraz innych źródeł, dokonać ich krytycznej weryfikacji, analizy i interpretacji,  a także formułować i uzasadnić wnioski i opinie;  U03 Potrafi zaprojektować potencjał obronny (plan ochrony) podmiotu adekwatny do zagrożeń bezpieczeństwa;  U04 Potrafi porozumiewać się w języku obcym na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego łącznie ze znajomością elementów języka z zakresu inżynierii bezpieczeństwa;  U05 Potrafi korzystać z systemów wersjonowania oprogramowania oraz technik testowania aplikacji;  U06 Potrafi zamodelować złożony system techniczny i dokonać symulacji jego działania, wykorzystując odpowiednie narzędzia sprzętowo-programowe;  U07 Umie dokonać analizy i syntezy złożonych systemów teleinformatycznych, potrafi ocenić przydatność nowych rozwiązań w tych systemach. | K\_U01  K\_U03  K\_U05  K\_U06  K\_U01  K\_U01  K\_U02 |

|  |  |  |
| --- | --- | --- |
| Kompetencje społeczne | Efekt uczenia się dla kursu | Odniesienie do efektów kierunkowych |
| K01 Jest gotów do formułowania i komunikowania opinii dotyczących zagadnień bezpieczeństwa oraz do ich krytycznej oceny;  K02 Jest gotów do działania w sposób przedsiębiorczy, znajdując, społeczne i komercyjne zastosowania tworzonych rozwiązań;  K03 Potrafi myśleć i działać w sposób kreatywny prawidłowo identyfikując i rozstrzygając problemy inżynierii bezpieczeństwa. | K\_K01  K\_K03  K\_K05 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Organizacja | | | | | | | | | | | | | |
| Forma zajęć | Wykład  (W) | Ćwiczenia w grupach | | | | | | | | | | | |
| A |  | K |  | L |  | S |  | P |  | E |  |
| Liczba godzin | 15 |  | |  | | 30 | |  | |  | |  | |
|  |  |  | |  | |  | |  | |  | |  | |

##### Opis metod prowadzenia zajęć

|  |
| --- |
| Kurs składa się z wykładów i zajęć prowadzonych w formie laboratoriów.  Wykład obejmuje zagadnienia merytoryczne prezentowane w formie prezentacji i omówienia podstaw przez wykładowcę.  W ramach ćwiczeń laboratoryjnych na bieżąco będzie weryfikowana wiedza przekazywana podczas wykładów. Studenci w ramach pracy indywidualnej realizują zadane projekty, dotyczące administracji nad siecią komputerową, analizy sieci w celu oceny systemy bezpieczeństwa, używając odpowiednie narzędzia. |

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 | x |  | x |  | x |  |  |  |
| W02 |  |  |  |  | x |  | x | x |  |  |  |  |  |
| W03 |  |  |  |  | x |  |  | x |  |  |  |  |  |
| W04 |  |  |  |  | x |  |  |  |  |  |  |  |  |
| W05 |  |  |  |  | x | x |  | x |  |  |  |  | x |
| W06 |  |  |  |  | x |  |  | x |  |  |  |  |  |
| U01 |  |  |  |  | x | x |  | x |  |  |  |  |  |
| U02 |  |  |  |  |  | x | x |  |  |  |  |  |  |
| U03 |  |  |  |  | x | x |  | x |  |  |  |  |  |
| U04 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| U05 |  |  |  |  | x | x |  | x |  |  |  |  |  |
| U06 |  |  |  |  |  | x |  |  |  |  |  |  |  |
| U07 |  |  |  |  |  | x |  | x |  |  |  |  |  |
| K01 |  |  |  |  |  |  |  | x |  |  |  |  |  |
| K02 |  |  |  |  |  | x | x |  |  |  |  |  |  |
| K03 |  |  |  |  |  | x |  |  |  |  |  |  |  |

|  |  |
| --- | --- |
| Kryteria oceny | Ocenę dobrą i bardzo dobrą uzyska student, który:  - posiada wiedzę z zakresu network administrator;  - posiada wiedzę z zakresu ochrony informacji w sieciach komputerowych;  - potrafi przeprowadzić monitorowanie sieci;  - potrafi stworzyć system kontroli dostępu;  - orientuje się w podstawowych problemach i wyzwaniach w zakresie ochrony informacji w sieci WWW;  - wykorzystuje podstawowe narzędzia do analizy poziomu bezpieczeństwa sieci;  - potrafi tworzyć dodatki dla programów znanych, jako narzędzia do analizy bezpieczeństwa sieci, które rozszerzają możliwości odpowiednich narzędzi i dostosować ich do wymogów określonego środowiska sieciowego. |

|  |  |
| --- | --- |
| Uwagi | Brak |

Treści merytoryczne (wykaz tematów)

|  |
| --- |
| 1. Kontrolowanie poprawności działania sieci poprzez reagowanie na wszelkie zakłócenia i nieprawidłowości.  2. Konfigurowanie interfejsów sieciowych komputerów.  3. Nadzór nad pracą urządzeń wspomagających.  4. Przestrzeganie zasad ochrony haseł. Tworzenie systemu haseł dostępu do urządzeń.  5. Zarządzanie adresacją sieci.  6. Wprowadzenie do problemów współczesnej ochrony informacji w sieciach komputerowych.  7. Podstawowe techniki identyfikacyjne. Identyfikacja użytkowników, protokoły i schematy identyfikacji.  8. Internet Protocol Security (IPsec). Bezpieczeństwo połączeń.  9. Bezpieczeństwo w sieciach bezprzewodowych.  10. Modele detekcji intruzów. Wprowadzenie do sieciowych systemów wykrywania intruzów.  11. Wprowadzenie do podstaw kontroli dostępu, modeli i implementacja. |

Wykaz literatury podstawowej

|  |
| --- |
| 1. James F. Kurose, Keith W. Ross. Computer Networking: A Top-Down Approach, published by Pearson Education, Inc, publishing as Addison-Wesley, 2013  2. J.Pieprzyk, T.Hardjono, J.Seberry. Teoria bezpieczeństwa systemów komputerowych. Helion, Springer.  3. N.Dhanjani, J.Clarke. Bezpieczeństwo sieci. Narzędzia. Helion, O’REILLY.  4. W.Stallings. Ochrona danych w sieci i intersieci. W teorii i w praktyce. WNT, 1997.  5. C.Kaufman, R.Perlman, M.Speciner. Network Security. Private Communication in a Public World. Prentice Hall.  6. R.Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. New York: John Wiley & Sons. 2008.  6. C.Kaufman, R.Perlman, M. Speciner. Network Security. Engle-wood Cliffs, NJ: Prentice Hall, 2002.  7. B. Schneier. Secrets and Lies. New York: John Wiley & Sons. 2004.  8. Chris McNab. Ocena bezpieczeństwa sieci. O’Reilly 2017  9. Nitesh Dhanjani, Justin Clarke. Bezpieczeństwo sieci. Narzędzia. O’Reilly 2006 |

Wykaz literatury uzupełniającej

|  |
| --- |
| 1. G. Brassard, P. Bratley. Algorithms, Theory and Practice. Prentice Hall, 1988.  2. J. Seberry, J. Pieprzyk. Cryptography: An Introduction to Computer Security. Prentice-Hall, 1989.  3. H. Anton. Elementary Linear Algebra (Sixth Edition). John Wiley and Sons, 1991.  4. K. H. Rosen. Elementary Number Theory and its Application (Third Edition). Addison Wesley, 1993.  5. E.Skoudis, T.Liston. Counter Hack Reloaded. Upper Saddle River. NJ: Prentice Hall, 2006. |

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta)

|  |  |  |
| --- | --- | --- |
| liczba godzin w kontakcie z prowadzącymi | Wykład | 15 |
| Konwersatorium (ćwiczenia, laboratorium itd.) | 30 |
| Pozostałe godziny kontaktu studenta z prowadzącym | 5 |
| liczba godzin pracy studenta bez kontaktu z prowadzącymi | Lektura w ramach przygotowania do zajęć | 5 |
| Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu | 10 |
| Przygotowanie projektu lub prezentacji na podany temat (praca w grupie) | 5 |
| Przygotowanie do egzaminu/zaliczenia | 5 |
| Ogółem bilans czasu pracy | | 75 |
| Liczba punktów ECTS w zależności od przyjętego przelicznika | | 3 |