|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **KARTA PRZEDMIOTU** | | | | |
| **Kod przedmiotu** | 717603 | | | |
| **Nazwa przedmiotu w języku** | | **polskim** | | Kryptografia |
| **angielskim** | | Cryptography |
|  | | | | |
| **1. USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW** | | | | |
| **1.1. Kierunek studiów** | | Bezpieczeństwo narodowe | | |
| **1.2. Forma studiów** | | studia stacjonarne | | |
| **1.3. Profil studiów** | | ogólnoakademicki | | |
| **1.4. Jednostka prowadząca przedmiot** | | | Katedra Stosunków Międzynarodowych  i Bezpieczeństwa | |
| **1.5. Osoba odpowiedzialna za przedmiot** | | | dr Grzegorza Tutak | |

|  |  |
| --- | --- |
| **2. OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU** | |
| **2.1. Przynależność do modułu** | Cyberbezpieczeństwo |
| **2.2. Status przedmiotu** | fakultatywny |
| **2.3. Język wykładowy** | polski |
| **2.4. Semestry, na których**  **realizowany jest przedmiot** | Semestr III |
| **2.5. Wymagania wstępne** | 1. Algorytmy i struktury danych 2. Podstawy programowania (zalecany język C++) 3. Znajomość podstaw matematyki oraz programowania. |

|  |  |  |
| --- | --- | --- |
| **3. FORMY, TREŚĆ I METODY PROWADZENIA ZAJĘĆ** | | |
| **3.1. Forma zajęć** | konwersatorium | |
| **3.2. Treści kształcenia** | 1. Problem bezpieczeństwa SI 2. Klasyfikacja i podstawowe parametry SI 3. Wpływ długości hasła i stosowanego alfabetu na bezpieczeństwo w sieciach komputerowych 4. Problematyka strat informacji w kanałach transmisyjnych, ich wykrywalność i możliwości korekcyjne 5. Kryptografia symetryczna i asymetryczna. 6. Stosowanie metod kodowania, szyfrowania i funkcji skrótu. 7. Realizacja podpisu cyfrowego na podstawie algorytmu RSA 8. Projektowanie bezpieczeństwa SI i badanie bezpieczeństwa systemów operacyjnych i sieci 9. Zapoznanie studentów z mechanizmami zabezpieczeń w systemach operacyjnych. | |
| **3.3. Metody dydaktyczne** | **Słowne**: wykład konwersatoryjny, dyskusja, opis, referat.  **Oglądowe**: prezentacje multimedialne, matematyczne formy algorytmów kryptograficznych.  **Praktyczne:** kazusy do rozwiązania, praca w grupach, studium przypadku, dyskurs; samodzielne przygotowywanie zagadnienia kryptograficznego, rozwiązywanie przykładowych algorytmów kryptograficznych. | |
| **3.4. Wykaz literatury** | **podstawowa** | 1. William Stallings, Lawrie Brown, Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Tom I, wyd. IV, Wydawnictwo: Helion, 2019 2. William Stallings, Lawrie Brown, Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Tom II, wyd. IV, Wydawnictwo: Helion, 2019. 3. Jean-Philippe Aumasson, Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania, Wydawnictwo PWN, 2018. |
| **uzupełniająca** | 1. Douglas R. Stinson, Kryptografia, Wydawnictwo: WNT, 2005. 2. Mirosław Kutyłowski, Willy-B. Strothman, Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych, RM 1999 |

|  |  |
| --- | --- |
| **4. CELE I EFEKTY KSZTAŁCENIA** | |
| **4.1. CELE PRZEDMIOTU** | **Wiedza:**   * poznanie rangi kryptografii w ochronie informacji i bezpieczeństwa w SI * poznanie różnych metod kryptograficznych * poznanie przeznaczenia stosowania poszczególnych metod kryptograficznych   **Umiejętności:**   * świadomość konieczności poznawania nowych zagrożeń i metod obrony przed nimi * świadomość, że do różnych obszarów SI stosuje się różne metody kryptograficzne i różne poziomy ich bezpieczeństwa * umiejętność oszacowania ryzyka i adekwatnych metod obrony   Kompetencje społeczne:   * potrzeba uświadamiana i pomagania innym zrozumieć ważność zachowywania ostrożności i metod obrony czy ochrony * wskazanie metod obrony i ochrony |
| **4.2. EFEKTY KSZTAŁCENIA** | |
| **KOD DLA KIERUNKU** | **w zakresie WIEDZY** |
| K\_W01 | Student potrafi wymienić i wyjaśnić:   * podstawowe pojęcia teorii informacji, zasady ochrony informacji w sieciach komputerowych * zasady bezpieczeństwa systemów informatycznych * współcześnie stosowane metody kryptograficzne. |
| K\_W05 | Student zna:   * współczesne globalne zagrożenia w cyberprzestrzeni * uwarunkowania bezpieczeństwa globalnego, międzynarodowego, lokalnego oraz instytucjonalnego * współczesne technologie i sprzęt stosujące metody kryptograficzne. |
|  | **W zakresie UMIEJĘTNOŚCI** |
| K\_U01 | Student potrafi:   * analizować potrzebę i poziom bezpieczeństwa w cyberprzestrzeni na poziomie państwa oraz w wymiarze międzynarodowym * prognozować zagrożenia na podstawie rozwoju technologicznego i kulturowego. |
| K\_U03 | Student potrafi:   * dostosować metody kryptograficzne adekwatne do zagrożeń * oszacować ryzyka kryptograficzne. |
|  | **W zakresie KOMPETENCJI SPOŁECZNYCH** |
| K\_K02 | Student jest gotów do:   * myślenia holistycznego w zakresie konieczności stosowania metod kryptograficznych * ciągłej analizy ryzyka z korzystania z cyberprzestrzeni i dynamicznego dostosowywania metod ochrony * uświadamiana osób o zagrożeniach i metodach obrony |

|  |  |  |
| --- | --- | --- |
| **4. METODY I SPOSOBY WERYFIKACJI EFEKTÓW KSZTAŁCENIA** | | |
| **4.1. Sposób realizacji** | Zajęcia odbywają się stacjonarnie (pomieszczenie oznaczone CN-P10) | |
| **4.2. Warunki zaliczenia przedmiotu** | * aktywność na zajęciach – 30% * frekwencja 100% – 10 % * zaliczenie – 60% | |
| **4.3. Metody i sposoby weryfikacji efektów kształcenia** | **Metody weryfikacji efektów kształcenia**   * dialog odnoszący się do wcześniej omawianych zagadnień (każda aktywność związana z poruszanym zagadnieniem oznaczana plusem) * ustna weryfikacja pisemnego opracowania | **Kryteria oceny osiągniętych efektów kształcenia**   * pisemne opracowanie wskazanego zagadnienia kryptograficznego * wymagana prawem frekwencja na zajęciach * ilość zdobytych na zajęciach „plusów” |
| **Zaliczenie ćwiczeń** | Jedna praca pisemna |
|  | **Egzamin ustny** |  |
|  | **Egzamin pisemny** |  |

|  |  |  |
| --- | --- | --- |
| **5. PUNKTY ECTS I ICH ROZKŁAD Z UWZGLĘDNIENIEM PRACY STUDENTA** | | |
| **Kategoria** | **Obciążenia studenta** | |
| **Studia stacjonarne** | **Studia niestacjonarne** |
| Udział w zajęciach dydaktycznych określonych w planie studiów | 1 |  |
| Praca pisemna na temat wskazanego zagadnienia kryptograficznego | 2 |  |
| **PUNKTY ECTS za przedmiot** | 3 |  |

|  |  |
| --- | --- |
| **Nazwisko osoby prowadzącej zajęcia** | Jakub Lasyk |

*Podpis Kierownika Katedry*