Zał. nr 5 do ZW 8/2020

Załącznik nr … do programu studiów

|  |
| --- |
| WYDZIAŁ Elektroniki / STUDIUM……………… KARTA PRZEDMIOTUNazwa przedmiotu w języku polskim: Etyczne, prawne i socjalne aspekty w AI i CyberbezpieczeństwieNazwa przedmiotu w języku angielskim: Ethical, legal and social aspects in AI and CybersecurityKierunek studiów (jeśli dotyczy): Zaufane systemy sztucznej inteligencjiSpecjalność (jeśli dotyczy): ……………………..Poziom i forma studiów: ~~I~~ / II stopień / ~~jednolite studia magisterskie~~\*, stacjonarna / ~~niestacjonarna~~\* **Rodzaj przedmiotu: ~~obowiązkowy /~~ wybieralny / ~~ogólnouczelniany~~ \***  **Kod przedmiotu …………….**  **Grupa kursów TAK / ~~NIE~~\*** |
|  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Wykład | Ćwiczenia | Laboratorium | Projekt | Seminarium |
| Liczba godzin zajęć zorganizowanych w Uczelni (ZZU) | 30 | --- | --- | --- | --- |
| Liczba godzin całkowitego nakładu pracy studenta (CNPS) | 60 | --- | --- | --- | --- |
| Forma zaliczenia | ~~Egzamin /~~ zaliczenie na ocenę\* | ~~Egzamin / zaliczenie na ocenę\*~~ | ~~Egzamin / zaliczenie na ocenę\*~~ | ~~Egzamin /~~ zaliczenie na ocenę\* | ~~Egzamin /~~ zaliczenie na ocenę\* |
| Dla grupy kursów zaznaczyć kurs końcowy (X) | X |  |  |  |  |
| Liczba punktów ECTS | **3** |  |  |  |  |
| w tym liczba punktów odpowiadająca zajęciom  o charakterze praktycznym (P) |  |  |  |  |  |
| w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU) | 2 |  |  |  |  |

\*niepotrzebne skreślić

|  |
| --- |
| **WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH**   1. Student ma podstawową wiedzę na temat sieci teleinformatycznych. 2. Student ma wiedzę z zakresu zagadnień sieci komputerowych |

|  |
| --- |
| **CELE PRZEDMIOTU**  C1 Zdobycie podstawowej wiedzy związanej z aspektami prawnymi i etycznymi w obszarze bezpieczeństwa zasobów sieci teleinformatycznych.  C2 Zdobycie ogólnej wiedzy o etycznych i psychologicznych aspektach zapewniania bezpieczeństwa informacji |

|  |
| --- |
| PRZEDMIOTOWE EFEKTY UCZENIA SIĘ **Z zakresu wiedzy:**  PEU\_W01 Student ma wiedzę o zakresie regulacji prawnych w obszarze bezpieczeństwa zasobów sieci teleinformatycznych  PEU\_W02 Student ma spójną wiedzę związaną z aspektami prawnymi, etycznymi i psychologicznymi w obszarze bezpieczeństwa zasobów sieci teleinformatycznych.  **Z zakresu umiejętności:**  PEU\_U01 Student potrafi odnaleźć i przeanalizować regulacje prawne w obszarze bezpieczeństwa zasobów sieci teleinformatycznych  PEU\_U01 Student potrafi określić konsekwencje etyczne związane z działaniami w obszarze bezpieczeństwa zasobów sieci teleinformatycznych.  **Z zakresu kompetencji społecznych:**  PEU\_K01 Rozumie konieczność samokształcenia oraz rozwijania zdolności do samodzielnego stosowania posiadanej wiedzy i umiejętności.  PEU\_K02 Potrafi przedstawić efekty swojej pracy w zrozumiałej formie. |

|  |  |  |
| --- | --- | --- |
| **TREŚCI PROGRAMOWE** | | |
| Forma zajęć - wykład | |  |
| Wy1-Wy2 | Źródła praw dotyczące ochrony informacji | 4 |
| Wy3 | Podstawowe pojęcia systemu bezpieczeństwa informacji oraz podstawowe podmioty odpowiedzialne za bezpieczeństwo informacji | 2 |
| Wy4 | Modele ochrony danych | 4 |
| Wy5 | Odpowiedzialność za naruszenie przepisów o ochronie informacji w zakresie karnym, cywilnym, pracowniczym, administracyjnym | 2 |
| Wy6-Wy8 | Dokumenty normatywne w obszarze bezpieczeństwa informacji | 4 |
| Wy9 | Anonimowość w Internecie. Zastosowanie i konsekwencje. Sieć Darknet. | 2 |
| Wy10 | Etyczne aspekty analizy bezpieczeństwa systemów IT, wyszukiwania, raportowania i ujawniania podatności. | 2 |
| Wy11-Wy12 | Zagrożenia i wyzwania związane ze sztuczną inteligencją. Etyczne aspekty zastosowania algorytmów SI do podejmowania i wspomagania krytycznych decyzji. | 4 |
| Wy13 | Psychologiczne aspekty funkcjonowania specjalisty / administratora bezpieczeństwa informacji | 2 |
| Wy14 | Socjologiczne aspekty bezpieczeństwa informacji | 2 |
| Wy15 | Kolokwium | 2 |
|  | Suma godzin | 30 |

|  |  |  |
| --- | --- | --- |
| **Forma zajęć - ćwiczenia** | | **Liczba godzin** |
| Ćw1 | --- | --- |
| Ćw2 | --- | --- |
| Ćw3 | --- | --- |
| Ćw4 | --- | --- |
| .. |  |  |
|  | Suma godzin | --- |

|  |  |  |
| --- | --- | --- |
| **Forma zajęć - laboratorium** | | **Liczba godzin** |
| La1 | --- | --- |
| La2 | --- | --- |
| La3 | --- | --- |
| La4 | --- | --- |
| La5 | --- | --- |
| … |  |  |
|  | Suma godzin | --- |

|  |  |  |
| --- | --- | --- |
| **Forma zajęć - projekt** | | **Liczba godzin** |
| Pr1 | --- | --- |
| Pr 2 | --- | --- |
| Pr 3 | --- | --- |
| Pr 4 | --- | --- |
| Pr 5 | --- | --- |
| … |  |  |
|  | Suma godzin | --- |

|  |  |  |
| --- | --- | --- |
| **Forma zajęć - seminarium** | | **Liczba godzin** |
| Se1 |  | --- |
| Se2 |  | --- |
| Se3 |  | --- |
| … |  |  |
|  | Suma godzin | --- |

|  |
| --- |
| STOSOWANE NARZĘDZIA DYDAKTYCZNE |
| 1. Wykład problemowy 2. Studia literaturowe 3. Opracowanie pisemne 4. Praca własna |

**OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ**

|  |  |  |
| --- | --- | --- |
| **Oceny** (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru) | Numer efektu uczenia się | Sposób oceny osiągnięcia efektu uczenia się |
| **F1** | PEU\_W01  PEU\_W02 | 1. Pisemne zaliczenie. |
| P=1\*F1  Warunkiem uzyskania pozytywnej oceny podsumowującej jest uzyskanie pozytywnej oceny z formy: wykład. | | |

|  |
| --- |
| **LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA** |
| **literatura PODSTAWOWA:**   1. Bezpieczeństwo informacyjne : nowe wyzwania. Krzysztof Liderman. – Państwowe Wydawnictwo Naukowe, Wyd. 2. – Warszawa, 2017 2. Mikołaj Karpiński oraz zespół, „Bezpieczeństwo Informacji”, PAK 2012 3. Podręcznik Administratora Bezpieczeństwa Informacji, Presscom 2016   **literatura UZUPEŁNIAJĄCA:**   1. KODEKS ETYKI ZAWODOWEJ ADMINISTRATORÓW BEZPIECZEŃSTWA INFORMACJI z dnia 19 czerwca 2008 r 2. Normy ISO rodziny 27000, PKN 2014 lub późniejsze 3. Zarządzanie bezpieczeństwem informacji - standard BS 7799 i normy serii ISOAEC 2700x 4. Common Criteria i norma ISO/IEC 15408 320 5. Publikacje specjalne NIST serii 800 331 6.1.3. 6. CIS Critical Security Controls 7. Standardy i normy wspierające zarządzanie bezpieczeństwem informacji 8. COBIT™ - dobre praktyki w zakresie ładu informatycznego |
| **OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)** |
|  |