**KARTA PRZEDMIOTU (SYLABUS)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Kod przedmiotu | | Nazwa przedmiotu | Cyberbezpieczeństwo i zarządzanie informacją | | | |
| UTH/F/DZ/2/P/ST/A/7 | | Cybersecurity and information management | | | |
| Język wykładowy | | Polski | | | | |
| Rok akademicki | | 2021/2022 | | | | |
|  | | | | | | |
| Kierunek | | Dziennikarstwo i nowe media | | | | |
| w zakresie | | - | | | | |
| Poziom studiów | | Studia drugiego stopnia | | | | |
| Profil studiów | | Profil praktyczny | | | | |
| Forma studiów | | Studia stacjonarne | | | | |
| Semestr / semestry | | II | | | | |
|  | | | | | | |
| Przynależność do grupy zajęć | | A. Grupa zajęć podstawowych | | | | |
| Status przedmiotu | | Obowiązkowy | | | | |
| Formy realizacji zajęć dydaktycznych,  wymiar, punkty ECTS | | Forma zajęć | | Liczba godzin zajęć dydaktycznych | Liczba punktów ECTS | |
| Wykład | | 15 | 2 ECTS | |
| Ćwiczenia | | 15 |
| - | | - |
| Powiązanie przedmiotu | z profilem studiów | Kształtuje umiejętności praktyczne (profil praktyczny) | | | | 1 ECTS |
| z uprawnieniami | - | | | | 0 ECTS |
| z dyscypliną | Nauki o komunikacji społecznej i mediach | | | | 2 ECTS |
| Forma nauczania | | Tradycyjna – zajęcia zorganizowane na Uczelni | | | | |
| Wymagania wstępne | | Znajomość zagadnień z zakresu technologii informacyjnych. | | | | |
|  | | | | | | |
| Jednostka prowadząca | | Wydział Prawa i Administracji /  Katedra Prawa Administracyjnego i Nauki o Administracji | | | | |
| Koordynator | | Dr Paweł Śwital | | | | |
| Adres strony internetowej pjo | | www.wpia.uniwersytetradom.pl | | | | |
| Adres e-mail, telefon koordynatora | | p.swital@uthrad.pl 483617433 | | | | |

**EFEKTY UCZENIA SIĘ, TREŚCI PROGRAMOWE, REALIZACJA ZAJĘĆ DYDAKTYCZNYCH, WERYFIKACJA EFEKTÓW UCZENIA SIĘ**

|  |  |
| --- | --- |
| Cel kształcenia: | 1. Celem kształcenia Studentów jest zapoznanie ich z podstawowymi zasadami zarządzania informacją w XXI wieku oraz wskazanie kluczowych zagrożeń bezpieczeństwa w cyberprzestrzeni. Przedstawienie zastosowania nowoczesnych rozwiązań teleinformatycznych w wspieraniu zadań bezpieczeństwa. Umiejętność rozpoznawania zagrożeń płynących z użytkowania sieci lokalnej oraz Internetu, a także aplikacji i systemów operacyjnych, w tym usług bankowych, opanowanie umiejętności wprowadzenia w temat bezpieczeństwa infrastruktury krytycznej. |
| Treści programowe: | **Wykład**   1. Wprowadzenie do przedmiotu, pojęcie informacji na gruncie prawa. 2. Wprowadzenie do tematyki zarządzania informacją – metody, formy, techniki. 3. Formy dostępu do informacji w polskim systemie prawnym. 4. Ochrona informacji i informacji niejawnych w systemie prawnym. 5. Podstawowe pojęcia z zakresu cyberbezpieczeństwa. 6. Wybrane zagrożenia sieciowe. 7. Krajowy i europejski system cyberbezpieczeństwa.   **Ćwiczenia**   1. Ochrona danych osobowych w świetle regulacji krajowych i RODO. 2. Współpraca międzynarodowa w zakresie zwalczania przestępczości  w cyberprzestrzeni. 3. Bezpieczeństwo przechowywania i przetwarzania danych. 4. Bezpieczeństwo usług bankowych. 5. Bezpieczeństwo infrastruktury krytycznej. 6. Podstawy kryptografii i podpisów cyfrowych. 7. Bezpieczeństwo aplikacji i systemów operacyjnych. |
| Metody dydaktyczne (kształcenia): | Słowne: wykład, dyskusja Praktyczne: wykorzystanie komputera, studia przypadków Oglądowe: prezentacje multimedialne, instrukcje, analiza kodeksów, analiza baz danych |
| Rygor zaliczenia, kryteria oceny osiągniętych efektów uczenia się, sposób obliczania oceny końcowej: | Warunkiem zaliczenia przedmiotu jest osiągnięcie przez studenta wymaganych efektów uczenia się. Uzyskanie pozytywnych ocen ze wszystkich form zajęć wchodzących w skład przedmiotu jest równoznaczne ze zdobyciem przez studenta liczby punktów ECTS przyporządkowanej temu przedmiotowi. Sposób obliczania oceny z poszczególnych form zajęć przedstawia się następująco:  **Wykład**  Zaliczenie pisemne test + pytania opisowe. Zaliczenie na ocenę pozytywną od 51 % prawidłowych odpowiedzi.  **Ćwiczenia**  Projekt z zakresu omawianych zagadnień (90 %), aktywność (10%). |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Efekty uczenia się dla przedmiotu w odniesieniu do efektów kierunkowych i formy zajęć | | | | Metody weryfikacji efektów uczenia się | |
| Numer efektu uczenia się | Opis efektów uczenia się dla przedmiotu (PEU)  Student, który zaliczył przedmiot  (W) zna i rozumie/ (U) potrafi /(K) jest gotów do: | Kierunkowy efekt uczenia się  (KEU) | Forma zajęć | Forma weryfikacji  (zaliczeń) | Metody sprawdzania  i oceny |
| W1 | Zna i rozumie podstawowe pojęcia, metody, formy i techniki zarządzania informacją oraz miejsce informacji we współczesnym świecie. | K\_WG01  K\_WG02 | Wykład/Ćwiczenia | Egzamin/  Zaliczenie na ocenę | Zaliczenie pisemne |
| W2 | Zna i rozumie współczesne problemy cyberbezpieczeństwa w zakresie ochrony systemów informatycznych | K\_WG02  K\_WK09 | Wykład/Ćwiczenia | Egzamin/ Zaliczenie na ocenę | Zaliczenie pisemne |
| W3 | Student zrozumie jakie możliwości dla podmiotów państwowych i prywatnych wynikają z wykorzystywania nowych technologii. | K\_WG07  K\_WK09 | Wykład/Ćwiczenia | Egzamin/ Zaliczenie na ocenę | Zaliczenie pisemne |
| U1 | Potrafi rozpoznawać i identyfikować zagrożenia w cyberprzestrzeni. | K\_UW02  K\_UW05 | Ćwiczenia | Zaliczenie na ocenę | Projekt |
| U2 | Potrafi poszukiwać, analizować i rozumieć informacje związane z obowiązkami nałożonymi na najważniejszych aktorów funkcjonujących w obszarze cyberbezpieczeństwa. | K\_UW02  K\_UW03 | Wykład/Ćwiczenia | Egzamin/  Zaliczenie na ocenę | Zaliczenie pisemne  Projekt |
| U3 | Potrafi sporządzić dokumenty z zakresu ochrony informacji i danych osobowych. | K\_UW02  K\_UK07 | Ćwiczenia | Zaliczenie na ocenę | Projekt |
| K1 | Jest przygotowany do wykorzystania swoich umiejętności komunikacyjno-medialnych w inspirowaniu i organizowaniu działań mających na celu rozwój środowiska społeczno-gospodarczego, w tym lokalnego. | K\_KO03 | Wykład/Ćwiczenia | Zaliczenie na ocenę | Projekt |

|  |
| --- |
| Literatura i pomoce naukowe |
| **Literatura podstawowa**  D. L. Pipkin, Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa, Warszawa 2006.  T. Hoffmann, Wybrane aspekty cyberbezpieczeństwa w Polsce, Poznań 2018.  **Literatura uzupełniająca**  W. Kitler (red.), K. Chałubińska-Jentkiewicz, K. Badźmirowska-Masłowska, System bezpieczeństwa w cyberprzestrzeni RP, Warszawa 2018.  D. Lisiak-Felicka, M.Szmit, Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia, Kraków 2016.  **Pomoce naukowe**  Prezentacje multimedialne. |

|  |  |  |  |
| --- | --- | --- | --- |
| Nakład pracy studenta potrzebny do osiągnięcia zakładanych efektów uczenia się – bilans punktów ECTS | | | |
| Udział w zajęciach, aktywność | Obciążenie studenta [h] | | |
| Inne godz. kontaktowe  (IGK) | Zajęcia bez nauczyciela-praca własna studenta  (ZBN) | Zajęcia dydaktyczne |
| Udział w wykładach | - | - | 15 |
| Udział w ćwiczeniach | - | - | 15 |
| Udział w konsultacjach | 5 | - | - |
| Przygotowanie do zajęć i zaliczenia,  w tym wykonanie prac zaliczeniowych | - | 15 | - |
| Sumaryczne obciążenie pracą studenta | 5[h] / 0,2 ECTS | 15[h] / 0,6 ECTS | 30[h] / 1,2 ECTS |
| Punkty ECTS za przedmiot | 2 ECTS | | |

|  |
| --- |
| Informacje dodatkowe, uwagi |
|  |