|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Wypełnia Zespół Kierunku | Nazwa modułu (bloku przedmiotów): **PRZEDMIOTY DO WYBORU** | | | | | | Kod modułu: **E** | |
| Nazwa przedmiotu: **Cyberprzestępczość** | | | | | | Kod przedmiotu: **46.2** | |
| Nazwa jednostki organizacyjnej prowadzącej przedmiot / moduł: **INSTYTUT EKONOMICZNY** | | | | | | | |
| Nazwa kierunku: **Administracja** | | | | | | | |
| Forma studiów: **SS** | | | Profil kształcenia: **praktyczny** | | | **Specjalność: APiZPS** | |
| Rok / semestr: **II/IV** | | | Status przedmiotu /modułu: **obowiązkowy** | | | Język przedmiotu / modułu: **polski** | |
| Forma zajęć | wykład | ćwiczenia | | laboratorium | projekt | seminarium | inne  (wpisać jakie) |
| Wymiar zajęć (godz.) | 15 |  | | 15 |  |  |  |

|  |  |
| --- | --- |
| Koordynator przedmiotu / modułu | dr Mariusz Darabasz |
| Prowadzący zajęcia | dr Mariusz Darabasz |
| Cel kształcenia przedmiotu / modułu | Celem kształcenia jest nabycie przez studentów wiedzy, umiejętności praktycznych i kompetencji społecznych na temat zagrożeń występujących w cyberprzestrzeni, która jest jednym z obszarów działania przestępców, zorganizowanych grup przestępczych oraz środowisk eksternistycznych i organizacji terrorystycznych. W trakcie kształcenia ukształtowane zostaną wśród studentów postawy i umiejętności pozwalające identyfikować zagrożenia w cyberprzestrzeni, przewidywać ich skutki i w przyszłości wiedzieć jak unikać tych zagrożeń. |
| Wymagania wstępne | Umiejętność korzystania z zasobów sieci Internet oraz znajomość prawa karnego materialnego i prawa karnego procesowego. |

|  |  |  |
| --- | --- | --- |
| **EFEKTY UCZENIA SIĘ** | | |
| Nr efektu uczenia się/ grupy efektów | Opis efektu uczenia się | Kod kierunkowego efektu  uczenia się |
| 01 | Ma wiedzę w zakresie kwalifikacji prawnej poszczególnych rodzajów zagrożeń związanych z cyberprzestępczością. | K1P\_W02  K1P\_W14 |
| 02 | Ma wiedzę w zakresie zadań, organizacji i zasad funkcjonowania organów państwa i innych instytucji  odpowiedzialnych za zapobieganie i zwalczanie cyberprzestępczości. | K1P\_W04 |
| 03 | Ma wiedzę w zakresie pojęć i zasad z zakresu ochrony własności intelektualnej i prawa autorskiego. | K1P\_W09 |
| 04 | Ma wiedzę w zakresie mechanizmów kontroli cyberprzestępczości | K1P\_W10 |
| 05 | Potrafi identyfikować oraz analizować  przyczyny i konsekwencje zagrożeń związanych z cyberprzestępczością | K1P\_U01  K1P\_U02 |
| 06 | Potrafi zastosować technologie informacyjne w realizacji zadań związanych z zapobieganiem i zwalczaniem przestępczości. | K1P\_U05 |
| 07 | W oparciu o przeprowadzoną analizę przypadków cyberprzestępstw potrafi opracować strategię zapobiegania tym zagrożeniom. | K1P\_U09 |
| 08 | Potrafi współdziałać w grupie, przyjmując w niej różne role oraz brać odpowiedzialność za powierzone mu zadania. | K1P\_K03 |
| 09 | Jest gotów do uczestniczenia w projektach społecznych i innych przedsięwzięciach mających na celu zapobieganie zagrożeniom związanym z cyberprzestępczością. | K1P\_K09 |

|  |  |  |
| --- | --- | --- |
| **TREŚCI PROGRAMOWE** | | |
| Wykład: | | |
| Cyberprzestrzeń oraz przestępczość w cyberprzestrzeni; Cechy cyberprzestepczości; Systematyka oraz kwalifikacja prawna wybranych cyberprzestępstw; Komputer jako narzędzie cyberprzestępstwa; Rodzaje cyberprzestępczości (cyberprzestępstwa przeciw poufności, integralności i dostępności danych, cyberprzestępstwa związane z treścią, naruszenie prawa autorskiego i praw pokrewnych, inne cyberprzestępstwa); Cyberprzestępstwa związane z uzyskaniem nieuprawnionego dostępu do systemów komputerowych oraz związane z dokonywaniem nieuprawnionych czynności wewnątrz systemu; Zagrożenia związane z cyberprzestępczością (malware, spam, spam nigeryjski, fałszywa reklama, pay per click, spam w mediach społecznościowych, kradzież tożsamości, phishing, botnet, płatności anonomowe,pranie pieniędzy, pornografia dziecięca i pedofilia, hazard internetowy, oszustwa na aukcjach internetowych); Charakterystyka oraz klasyfikacja śladów cyberprzestępstw; Dowodowe czynności procesowe w cyberprzestrzeni; Model systemu zwalczania cyberprzestępczości; Wymiar międzynarodowy zwalczania cyberprzestępczości; Wymiar krajowy zwalczania cyberprzestępczości; Cyberprzestępczość a przestępczość zorganizowana, terroryzm i szpiegostwo, Media społecznościowe a cyberprzestępczość. | | |
| Laboratorium | | |
| Ochrona danych osobowych w sieci Internet; Oszustwa na Facebooku – studium przypadków; Prawno-karne aspekty cyberstalkingu; Oszustwa w sieci Internet; Internet a terroryzm – studium przypadków, Identyfikacja na podstawie analizy sieci Internet obszarów szczególnie zagrożonych cyberprzestępczością oraz  sporządzenie projektu działań mających na celu zapobieganie tym zagrożeniom. | | |
| W tym treści powiązane z praktycznym przygotowaniem zawodowym: **100[%]** | | |
| Literatura podstawowa | 1. J. Kosiński, Paradygmaty cyberprzestępczości, Warszawa 2015. 2. A. Lach, Dowody elektroniczne w procesie karnym, Toruń 2004. 3. W. Dubis, T. Szarek, A. Skrobich, B. Wójcik, Prawo elektroniczne z praktycznym komentarzem, Infor 2007. 4. D. L. Shinder, Cyberprzestępczość, Helion, Gliwice 2004. | |
| Literatura uzupełniająca | 1. J. Kosiński red., Przestępczość teleinformatyczna, Szczytno 2000-2017. 2. Konwencja Rady Europy o cyberprzestępczości – ETS - 185. 3. Protokół dodatkowy do Konwencji rady Europy o cyberprzestępczości, dotyczący kryminalizacji aktów natury rasistowskiej i ksenofobicznej popełnianych przy pomocy systemów komputerowych – ETS – 189. 4. Ustawa z dnia 6 czerwca 1997, kodeks karny (Dz. U. z 1997, nr 88, poz. 553 z późn. zm.). 5. Ustawa z dnia 6 czerwca 1997 r., kodeks postępowania karnego (Dz. U. z 1997, nr 89, poz. 555 z późn. zm.). 6. Ustawa z dnia 4 lutego 1994 r., o prawie autorskim i pokrewnych (tekst jednolity Dz. U. 2000 r. nr 80, poz.904 z późn. zm.). | |
| Metody kształcenia stacjonarnego | Wykład, metody praktyczne - studium przypadku, zajęcia laboratoryjne | |
| Metody kształcenia z wykorzystaniem metod i technik kształcenia na odległość | Nie dotyczy | |
| Metody weryfikacji efektów uczenia się | | Nr efektu uczenia się/grupy efektów |
| Test wiedzy | | 01 - 07 |
| Aktywny udział w zajęciach laboratoryjnych + esej. | | 05 - 09 |
| Formy i warunki zaliczenia | Test wiedzy - 50 % oceny końcowej.  Ćwiczenia laboratoryjne - 50 % oceny końcowej. | |

|  |  |  |  |
| --- | --- | --- | --- |
| NAKŁAD PRACY STUDENTA | | | |
| Rodzaj działań/zajęć | Liczba godzin | | |
| Ogółem | W tym zajęcia powiązane  z praktycznym przygotowaniem zawodowym | W tym udział w zajęciach przeprowadzanych z wykorzystaniem metod i technik kształcenia na odległość |
| Udział w wykładach | 15 |  |  |
| Samodzielne studiowanie | 5 |  |  |
| Udział w ćwiczeniach audytoryjnych i laboratoryjnych, warsztatach, seminariach | 15 | 15 |  |
| Samodzielne przygotowywanie się do ćwiczeń |  |  |  |
| Przygotowanie projektu / eseju / itp. | 15 | 15 |  |
| Przygotowanie się do egzaminu / zaliczenia | 10 | 5 |  |
| Udział w konsultacjach | 0,1 |  |  |
| Inne | - | - |  |
| ŁĄCZNY nakład pracy studenta w godz. | **60,1** | **35** |  |
| **Liczba punktów ECTS za przedmiot** | **2** | | |
| **Liczba punktów ECTS przypisana do dyscypliny naukowej** | **2 (nauki o bezpieczeństwie)** | | |
| Liczba punktów ECTS związana z zajęciami praktycznymi | **1,2** | | |
| Liczba punktów ECTS związana z kształceniem na odległość (kształcenie z wykorzystaniem metod i technik kształcenia na odległość) | **0,0** | | |
| Liczba punktów ECTS za zajęciach wymagające bezpośredniego udziału nauczycieli akademickich | **1,0** | | |