*Załącznik nr 1.5 do Zarządzenia Rektora UR nr 12/2019*

**SYLABUS**

**dotyczy cyklu kształcenia** *.2019-2022*

*(skrajne daty*)

Rok akademicki 2020/2021

1. Podstawowe informacje o przedmiocie

|  |  |
| --- | --- |
| Nazwa przedmiotu | Zwalczanie przestępczości w cyberprzestrzeni |
| Kod przedmiotu\* | BW45 |
| nazwa jednostki prowadzącej kierunek | Kolegium Nauk Społecznych |
| Nazwa jednostki realizującej przedmiot | Kolegium Nauk Społecznych |
| Kierunek studiów | Bezpieczeństwo wewnętrzne |
| Poziom studiów | studia I stopnia |
| Profil | praktyczny |
| Forma studiów | stacjonarne |
| Rok i semestr/y studiów | rok II, semestr IV |
| Rodzaj przedmiotu | do wyboru |
| Język wykładowy | polski |
| Koordynator | dr inż. Zbigniew Małodobry |
| Imię i nazwisko osoby prowadzącej / osób prowadzących | dr inż. Zbigniew Małodobry |

\* *-opcjonalni*e, *zgodnie z ustaleniami w Jednostce*

1.1.Formy zajęć dydaktycznych, wymiar godzin i punktów ECTS

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Semestr  (nr) | Wykł. | Ćw. | Konw. | Lab. | Sem. | ZP | Prakt. | Inne (jakie?) | **Liczba pkt. ECTS** |
| IV | - | - | 15 | - | - | - | - | - | 2 |

1.2. Sposób realizacji zajęć

⊠ zajęcia w formie tradycyjnej

☐ zajęcia realizowane z wykorzystaniem metod i technik kształcenia na odległość

1.3 Forma zaliczenia przedmiotu (z toku) (egzamin, zaliczenie z oceną, zaliczenie bez oceny)

zaliczenie z oceną

2.Wymagania wstępne

|  |
| --- |
| brak |

3. cele, efekty uczenia się , treści Programowe i stosowane metody Dydaktyczne

3.1 Cele przedmiotu

|  |  |
| --- | --- |
| C1 | Omówienie aktów prawa krajowego, unijnego i międzynarodowego dotyczącego przestępstw w cyberprzestrzeni |
| C2 | Analiza poszczególnych typów przestępstw w cyberprzestrzeni. Charakterystyka strategii przeciwdziałania przestępstwom w cyberprzestrzeni |
| C3 | Zapoznanie studentów z polityką kryminalną wobec przestępstw w cyberprzestrzeni |

**3.2 Efekty uczenia się dla przedmiotu**

|  |  |  |
| --- | --- | --- |
| EK (efekt uczenia się) | Treść efektu uczenia się zdefiniowanego dla przedmiotu | Odniesienie do efektów kierunkowych [[1]](#footnote-1) |
| EK­\_01 | posiada wiedzę na temat instytucji przeciwdziałających zagrożeniom w cyberprzestrzeni | K\_W14 |
| EK\_02 | rozróżnia rodzaje zagrożeń dla bezpieczeństwa związanych z cyberprzestrzenią | K\_U07 |
| EK\_03 | prawidłowo rozstrzyga dylematy etyczne związane ze skutkami działań w cyberprzestrzeni | K\_U14 |
| EK\_04 | posiada kompetencje do pracy w zespołach zajmujących się bezpieczeństwem sieciowym | K\_K01 |
| EK\_05 | jest przystosowany do pracy zespołowej w identyfikowaniu zagrożeń i tworzeniu scenariuszy przeciwdziałania zagrożeniom komputerowym | K\_K08 |

**3.3 Treści programowe**

1. Problematyka wykładu

|  |
| --- |
| Treści merytoryczne |
|  |
|  |
|  |

1. Problematyka ćwiczeń audytoryjnych, konwersatoryjnych, laboratoryjnych, zajęć praktycznych

|  |
| --- |
| Treści merytoryczne |
| zakłócanie pracy systemu komputerowego |
| bezprawne wykorzystanie programów i danych |
| sabotaż komputerowy |
| naruszenie integralności danych |
| niszczenie informacji |
| oszustwo komputerowe |
| nielegalne uzyskanie programu komputerowego |
| hacking |
| przestępstwo nielegalnego pozyskania informacji |
| publiczne nawoływanie do popełnienia czynu zabronionego |
| przestępstwo zniesławienia |

3.4 Metody dydaktyczne

Np.:

*Wykład: wykład problemowy, wykład z prezentacją multimedialną, metody kształcenia na odległość*

*Ćwiczenia: analiza tekstów z dyskusją, metoda projektów (projekt badawczy, wdrożeniowy, praktyczny), praca w grupach (rozwiązywanie zadań, dyskusja),gry dydaktyczne, metody kształcenia na odległość*

*Laboratorium: wykonywanie doświadczeń, projektowanie doświadczeń*

praca w grupach, analiza przypadków, dyskusja

4. METODY I KRYTERIA OCENY

4.1 Sposoby weryfikacji efektów uczenia się

|  |  |  |
| --- | --- | --- |
| Symbol efektu | Metody oceny efektów uczenia się  (np.: kolokwium, egzamin ustny, egzamin pisemny, projekt, sprawozdanie, obserwacja w trakcie zajęć) | Forma zajęć dydaktycznych  (w, ćw, …) |
| ek\_ 01 | Kolokwium ustne, obecność | konwersatorium |
| Ek\_ 02 | Kolokwium ustne, obecność | konwersatorium |
| EK\_03 | Kolokwium ustne, obecność | konwersatorium |
| EK\_04 | obserwacja w trakcie zajęć, obecność | konwersatorium |
| EK\_05 | obserwacja w trakcie zajęć, obecność | konwersatorium |

4.2 Warunki zaliczenia przedmiotu (kryteria oceniania)

|  |
| --- |
| Warunkiem zaliczenia jest 70 % poprawnych odpowiedzi (kolokwium ustne)  Ocena bardzo dobra – aktywność na zajęciach, uzyskanie od 95% do 100% punktów z kolokwium  Ocena +dobra – aktywność na zajęciach, uzyskanie od 90% do 94% punktów z kolokwium  Ocena dobra – aktywność na zajęciach, uzyskanie od 85% do 89% punktów z kolokwium  Ocena +dostateczna – aktywność na zajęciach, uzyskanie od 80 do 84% punktów z kolokwium  Ocena dostateczna – brak aktywności na zajęciach, uzyskanie od 70% do 79% punktów z kolokwium  Ocena niedostateczna – brak aktywności na zajęciach, uzyskanie mniej niż 70 % punktów z kolokwium |

**5. CAŁKOWITY NAKŁAD PRACY STUDENTA POTRZEBNY DO OSIĄGNIĘCIA ZAŁOŻONYCH EFEKTÓW W GODZINACH ORAZ PUNKTACH ECTS**

|  |  |
| --- | --- |
| **Forma aktywności** | **Średnia liczba godzin na zrealizowanie aktywności** |
| Godziny kontaktowe wynikające z harmonogramu studiów | 15 |
| Inne z udziałem nauczyciela akademickiego  (udział w konsultacjach, egzaminie) | 10 |
| Godziny niekontaktowe – praca własna studenta  (przygotowanie do zajęć, egzaminu, napisanie referatu itp.) | 25 |
| SUMA GODZIN | 50 |
| **SUMARYCZNA LICZBA PUNKTÓW ECTS** | 2 |

*\* Należy uwzględnić, że 1 pkt ECTS odpowiada 25-30 godzin całkowitego nakładu pracy studenta.*

6. PRAKTYKI ZAWODOWE W RAMACH PRZEDMIOTU

|  |  |
| --- | --- |
| wymiar godzinowy | - |
| zasady i formy odbywania praktyk | - |

7. LITERATURA

|  |
| --- |
| Literatura podstawowa:  Adamski A., *Przestępczość w cyberprzestrzeni : prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, Toruń : TNOiK Dom Organizatora, 2001  Grabowski *R.* (red.), *Wpływ Internetu na ewolucję państwa i prawa*, Rzeszów 2008.  Kardas P., *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, „Czasopismo Prawa Karnego i Nauk Penalnych” 2000, nr 1.  Siwicki M., *Nielegalna i szkodliwa treść w Internecie: aspekty prawnokarne*, wyd. Wolters Kluwer. 2011.  Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, Warszawa 2010. |
| Literatura uzupełniająca:  *Adamski A., Cyberprzestępczość – aspekty prawne i kryminologiczne, „Studia Prawnicze” 2005, nr 4.*  *Jakubski K.J., Przestępczość komputerowa – zarys problematyki, „Prokuratura i Prawo” 1996, nr 12.*  Jerzy Kosiński(red.); *Przestępczość teleinformatyczna : VIII seminarium naukowe: materiały seminaryjne,* Wyższa Szkoła Policji Szczytno : Wydawnictwo Wyższej Szkoły Policji, 2005. |

Akceptacja Kierownika Jednostki lub osoby upoważnionej

1. W przypadku ścieżki kształcenia prowadzącej do uzyskania kwalifikacji nauczycielskich uwzględnić również efekty uczenia się ze standardów kształcenia przygotowującego do wykonywania zawodu nauczyciela. [↑](#footnote-ref-1)