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

**SYLABUS**

**dotyczy cyklu kształcenia** *2021-2024*

*(skrajne daty*)

Rok akademicki 2022/2023

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 | niestacjonarne |
| Rok i semestr/y studiów | rok II, IV |
| Rodzaj przedmiotu | do wyboru |
| Język wykładowy | polski |
| Koordynator | dr Krystian Dzimira |
| Imię i nazwisko osoby prowadzącej / osób prowadzących | dr Krystian Dzimira |

\* *-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 |  |  | 10 |  |  |  |  |  | 2 |
|  |  |  |  |  |  |  |  |  |  |

1.2. Sposób realizacji zajęć

x 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 treści Programowe i stosowane metody Dydaktyczne

3.1. Cele przedmiotu

|  |  |
| --- | --- |
| C1 | Wprowadzenie podstawowych pojęć związanych z cyberbezpieczeństwem. Zapoznanie z zagrożeniami płynącymi z użytkowania sieci Internet, systemów informacyjnych oraz aplikacji. Przyswojenie wiedzy na temat polskich i europejskich regulacji prawnych w zakresie ochrony cyberprzestrzeni, a także poznanie podstawowych metod rozpoznania i analizy zagrożeń oraz zwalczania przestępczości cybernetycznej. |
| C2 | Wykorzystanie wspomnianej wiedzy jako narzędzia pozwalającego na dokonanie samodzielnej analizy zagrożeń w cyberprzestrzeni oraz formułowania wniosków w odniesieniu do różnorodnych aspektów bezpieczeństwa w sieci Internet, w tym w zakresie usług publicznych. |

**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 systemu cyberbezpieczeństwa w Polsce, ze szczególnym uwzględnieniem najważniejszych aktów prawnych oraz strategii państwa; potrafi określić elementy świadczące o mocnych i słabych stronach tego systemu; | W09, W10, U10 |
| EK\_02 | - posiada wiedzę i potrafi posługiwać się podstawowymi pojęciami oraz terminologią odnoszącą się do cyberbezpieczeństwa oraz przeanalizować i zinterpretować kluczowe zagrożenia; | W09, W10, U12 |
| EK\_03 | - potrafi opisać wpływ zagrożeń w cyberprzestrzeni na życie społeczne oraz instytucje i usługi kluczowe państwa; | W09, W10, U10 |
| EK\_04 | - potrafi samodzielnie lub we współdziałaniu z grupą poszerzać posiadany zakres wiedzy z dodatkowych źródeł; systematycznie aktualizuje oraz potrafi dokonać analizy bieżących informacji odnoszących się do współcześnie występujących zagrożeń w cyberprzestrzeni; | W09, W10, U10, U12, K08 |
| EK\_05 | - potrafi samodzielnie lub we współdziałaniu z grupą - przy wykorzystaniu dotychczas nabytej wiedzy - analizować i wykorzystywać uzyskaną wiedzę do identyfikacji i klasyfikacji zagrożeń w cyberprzestrzeni, a także potrafi aktywnie uczestniczyć w dyskusji dotyczącej cyberbezpieczeństwa. | W09, W10, U10, U12, K08 |

**3.3. Treści programowe**

1. Problematyka wykładu

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

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

|  |
| --- |
| Treści merytoryczne |
| Wprowadzenia w problematykę konserwatorium, podstawowe pojęcia i narzędzia. |
| Wybrane zagrożenia oraz przestępczość w cyberprzestrzeni. |
| Krajowy i europejski system cyberbezpieczeństwa. |
| Przepisy prawa polskiego, europejskiego i międzynarodowego w dziedzinie ochrony cyberprzestrzeni. |
| Systemy i mechanizmy bezpieczeństwa informacji, charakterystyki i metodyki stosowania. |
| Standardy bezpieczeństwa dotyczące przechowywania i przetwarzania danych. |
| Bezpieczeństwo usług publicznych dostarczanych w sieci Internet. |
| Bezpieczeństwo cybernetyczne infrastruktury krytycznej państwa. |
| Podstawy kryptografii. |
| Omówienie Deep web i Dark web. |

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*

- wykład konwersatoryjny z elementami wykładu problemowego;

- dyskusja dydaktyczna w formie okrągłego stołu;

- prelekcja;

- ekspozycja;

- samokształcenie;

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 | - dyskusja dydaktyczna, obserwacja w trakcie zajęć, zaliczenie w formie referatu lub prezentacji multimedialnej, a także zaliczenie na ocenę; | konwersatorium; |
| Ek\_ 02 | - dyskusja dydaktyczna, obserwacja w trakcie zajęć, zaliczenie w formie referatu lub prezentacji multimedialnej, a także zaliczenie na ocenę; | konwersatorium; |
| EK\_03 | - dyskusja dydaktyczna, obserwacja w trakcie zajęć, zaliczenie w formie referatu lub prezentacji multimedialnej, a także zaliczenie na ocenę;  - obserwacja; | konwersatorium; |
| EK\_04 | - dyskusja dydaktyczna, obserwacja w trakcie zajęć, zaliczenie w formie referatu lub prezentacji multimedialnej, a także zaliczenie na ocenę;  - obserwacja; | konwersatorium; |
| EK\_05 | - dyskusja dydaktyczna, obserwacja w trakcie zajęć, zaliczenie w formie referatu lub prezentacji multimedialnej, a także zaliczenie na ocenę;  - obserwacja; | konwersatorium; |

4.2. Warunki zaliczenia przedmiotu (kryteria oceniania)

|  |
| --- |
| Zaliczenie z oceną w formie przygotowanego referatu lub prezentacji multimedialnej oraz kolokwium w formie testu z odpowiedziami wielokrotnego wyboru – uzyskanie od 20% punktów przy wysokim stopniu szczegółowości testu, od 35% punktów przy średnim stopniu szczegółowości oraz 55% przy niskim stopniu szczegółowości;  kryteria oceny: zakres kompletności wiedzy, wysoka umiejętność kojarzenia faktów, zdolność uzupełniania i aktualizowania posiadanych informacji;  (uwaga: w przypadku zarządzenia właściwych organów trybu zajęć w formie online zaliczenie będzie miało formę ustną w tym trybie). |

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

|  |  |
| --- | --- |
| **Forma aktywności** | **Średnia liczba godzinna zrealizowanie aktywności** |
| Godziny kontaktowe wynikające z harmonogramu studiów | 10 |
| Inne z udziałem nauczyciela akademickiego  (udział w konsultacjach, egzaminie) | 10 |
| Godziny niekontaktowe – praca własna studenta  (przygotowanie do zajęć, egzaminu, napisanie referatu itp.) | 30 |
| SUMA GODZIN | 50 |
| **SUMARYCZNA LICZBA PUNKTÓW ECTS** | 2 |

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

6. PRAKTYKI ZAWODOWE W RAMACH PRZEDMIOTU

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

7. LITERATURA

|  |
| --- |
| Literatura podstawowa:  Hoffmann T., *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Poznań 2018.  *System bezpieczeństwa w cyberprzestrzeni RP*, red. W. Kitler, K. Chałubińska-Jentkiewicz, K. Badźmirowska-Masłowska, Warszawa 2018.  Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369). |
| Literatura uzupełniająca:  Aumasson J., *Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania*, Warszawa 2018.  International Organization for Standardization (https://www.iso.org/home.html).  National Institute of Standard and Technology (<https://www.nist.gov/>)  Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (M.P. z 30.10.2019 r. poz. 1037).  *Sztuczna inteligencja, block-chain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, red. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Warszawa 2019.  Zetter K., *Odliczając do dnia zero. Stuxnet, czyli prawdziwa historia cyfrowej broni,* Gliwice 2017. |

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)