*Załącznik nr 1.5 do Zarządzenia Rektora UR nr 61/2025*

**SYLABUS**

**dotyczy cyklu kształcenia**  *2025/2026 - 2027/2028*

*(skrajne daty*)

Rok akademicki 2027/28

1. Podstawowe informacje o przedmiocie

|  |  |
| --- | --- |
| Nazwa przedmiotu | Cyberprzestępczość |
| Kod przedmiotu\* | ASO 50 |
| nazwa jednostki prowadzącej kierunek | Wydział Prawa i Administracji Uniwersytet Rzeszowski |
| Nazwa jednostki realizującej przedmiot | Zakład Prawa Karnego |
| Kierunek studiów | Administracja |
| Poziom studiów | Studnia I stopnia |
| Profil | Ogólnoakademicki |
| Forma studiów | Stacjonarne |
| Rok i semestr/y studiów | Rok III, semestr VI |
| Rodzaj przedmiotu | Fakultatywny |
| Język wykładowy | Polski |
| Koordynator | dr hab. Anna Golonka, prof. UR |
| Imię i nazwisko osoby prowadzącej / osób prowadzących | dr Katarzyna Czeszejko-Sochacka |

\* *-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** |
| VI |  |  | 20 |  |  |  |  |  | 3 |

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

|  |
| --- |
| Podstawowe wiadomości z zakresu logiki, organów ochrony prawnej, znajomość metod wykładni. |

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

3.1. Cele przedmiotu

|  |  |
| --- | --- |
| C1 | Celem przedmiotu jest przekazanie wiedzy z zakresu problematyki cyberprzestępczości. |

**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 | definiuje podstawowe pojęcia z zakresu cyberprzestępczości. | K\_WO1 |
| EK\_02 | opisuje istotę podstawowych instytucji związanych z zagadnieniami cyberprzestępczości | K\_WO3 |
| EK\_03 | zna i rozumie podstawowe pojęcia i zasady z zakresu cyberprzestępczości | K\_WO7 |
| EK\_04 | dyskutuje na tematy poruszone na zajęciach | K\_W10 |
| EK\_05 | posiada umiejętność zdobywania wiedzy z zakresu omawianej tematyki. | K\_UO3 |
| EK\_06 | potrafi prawidłowo interpretować i wskazywać instytucje służące walce z cyberprzestępczością | K\_UO1 |
| EK\_07 | posiada umiejętność prowadzenia dyskusji na tematy związane z zagrożeniem cyberprzestępczością | K\_UO7 |
| EK\_08 | dyskutuje pojawiający się problem | K\_KO1 |
| EK\_09 | uzasadnia zajmowane przez siebie stanowisko | K\_KO4 |

**3.3. Treści programowe**

1. Problematyka wykładu – nie dotyczy
2. Problematyka ćwiczeń audytoryjnych, konwersatoryjnych, laboratoryjnych, zajęć praktycznych

|  |
| --- |
| **Treści merytoryczne** |
| Wprowadzenie do podstaw prawa karnego materialnego – 3 h |
| Charakterystyka zjawiska cyberprzestępczości– 3 h |
| Międzynarodowe i krajowe aspekty walki z cyberprzestępczości – 4h |
| Problematyka walki z cyberprzestępczością – 2 h |
| Przestępstwa popełnione z wykorzystaniem komputera -3 h |
| Przestępstwa związane z naruszeniem praw autorskich i pokrewnych – 5h |

3.4. Metody dydaktyczne

Konwersatorium - wykład problemowy, wykład z prezentacją multimedialną

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 | Zaliczenie pisemne w formie testu jednokrotnego wyboru | Konwers. |
| EK\_02 | Zaliczenie pisemne w formie testu jednokrotnego wyboru | Konwers. |
| EK\_03 | Zaliczenie pisemne w formie testu jednokrotnego wyboru | Konwers. |
| EK\_04 | Zaliczenie pisemne w formie testu jednokrotnego wyboru | Konwers. |
| EK\_05 | Zaliczenie pisemne w formie testu jednokrotnego wyboru | Konwers. |
| EK\_06 | Zaliczenie pisemne w formie testu jednokrotnego wyboru | Konwers. |
| EK\_07 | Zaliczenie pisemne w formie testu jednokrotnego wyboru | Konwers. |
| EK\_08 | Zaliczenie pisemne w formie testu jednokrotnego wyboru | Konwers. |
| EK\_09 | Zaliczenie pisemne w formie testu jednokrotnego wyboru | Konwers. |

4.2. Warunki zaliczenia przedmiotu (kryteria oceniania)

|  |
| --- |
| **Zaliczenie pisemne w formie testu jednokrotnego wyboru, jako końcowa forma zaliczenia przedmiotu lub zaliczenie w formie ustnej (w zależności od wyboru osoby prowadzącej przedmiot).** Metodą weryfikacji wiedzy, umiejętności i efektów kształcenia będzie zaliczenie złożone z pytań testowych bazujących na tematyce objętej ko9nwersatorium z przedmiotu cyberprzestępczość. Kryteria oceny zostaną w pełni zobiektywizowane, co umożliwi forma zaliczenia.  **Ocena formułująca i podsumowująca** zostaną wystawione w oparciu o wynik zaliczenia.  Test zaliczeniowy jest testem jednokrotnego wyboru, składającym się z 25 pytań. Punktowanych po 1 pkt.- za odpowiedź poprawną.  Warunkiem zaliczenia przedmiotu jest uzyskanie 13 pkt.  Skala ocen:  25-24 5.0  23-22 4.5  21-18 4.0  17-15 3.5  14-13 3.0  Istnieje możliwość podniesienia oceny końcowej w przypadku wyjątkowej aktywności studenta w trakcie prowadzonych zajęć. |

**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 planu z studiów | 20 |
| Inne z udziałem nauczyciela  (udział w konsultacjach, egzaminie) | 5 |
| Godziny niekontaktowe – praca własna studenta  (przygotowanie do zajęć, egzaminu, napisanie referatu itp.) | 50 |
| SUMA GODZIN | 75 |
| **SUMARYCZNA LICZBA PUNKTÓW ECTS** | 3 |

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

6. PRAKTYKI ZAWODOWE W RAMACH PRZEDMIOTU/ MODUŁU

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

7. LITERATURA

|  |
| --- |
| **Literatura podstawowa:**   1. P. Opitek, D. Robert jaworski, Cyberprzestępczość w prawie karnym i kryminalistyce, Warszawa 2025 2. I. A. Jaroszewska, Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne, Olsztyn 2017. 3. M. Siwicki, Cyberprzestępczość, Warszawa 2013. 4. J. Kosiński, Paradygmaty cyberprzestępczości, Warszawa 2015. 5. A. Adamski, Prawo karne komputerowe, Warszawa 2000. |
| **Literatura uzupełniająca:**   1. A. Suchorzewska, Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem, Warszawa 2010 2. A. Golonka, Terroryzm i jego finansowanie w kontekście nowelizacji art. 165a k.k., „Zeszyty Prawnicze UR. Seria Prawo” 2019, z. 25 (nr 106), 3. A. Golonka, Występek finansowania terroryzmu (art. 165a k.k.) w kontekście problemów związanych ze stroną podmiotową tego przestępstwa, „Zeszyty Prawnicze” 2019, 4. A. Golonka, Penalizacja finansowania terroryzmu- uwagi na tle zmian do art. 165a k.k**.,**„Państwo i Prawo” 2019, nr 8, 5. D. Habrat, Legal Challenges of Digitalization and Automation in the Context of Industry 4.0, [Procedia Manufacturing](http://bibliografia.ur.edu.pl/cgi-bin/expertus3.cgi), 2020 r.,Vol. 51. 6. M. Trybus, D. Kamuda, Ochrona informacji niejawnych w aspekcie bezpieczeństwa teleinformatycznego, Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie, 2016 r., t.14, z. 1(34). 7. M. Trybus, Hacking komputerowy z art. 267 k.k. zagrożeniem bezpieczeństwa cyberprzestrzeni RP”, s. 295-304 (w:) red. nauk. P. Bogdalski, Z. Nowakowski, T. Płusa, J. Rajchel, K. Rajchel “Współczesne zagrożenia cyberterrorystyczne i bioterrorystyczne a bezpieczeństwo narodowe Polski”, Warszawa-Dęblin 2015. 8. M. Trybus, D. Kamuda, Przestępstwo wyrządzenia szkody w danych informatycznych z art. 268a k.k. zagrożeniem bezpieczeństwa informatycznego RP (w:), Współczesne zagrożenia bioterrorystyczne  i cyberterrorystyczne a bezpieczeństwo narodowe Polski, red. P. Bogdalski,  Z. Nowakowski, T. Płusa, J. Rajchel, K. Rajchel, Wyższa Szkoła Policji  w Szczytnie 2013. 9. K. Czeszejko-Sochacka, Konstytucyjne i karne aspekty demoralizacji młodzieży na przykładzie zjawiska happy slapping, Przegląd Prawa Konstytucyjnego 2021 , nr 1 (59). |

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)