| AKADEMIA WSB | | | | | | |
|---|---|---|---|---|---|---|
| **Kierunek studiów: Bezpieczeństwo Narodowe** | | | | | | |
| **Przedmiot: Bezpieczeństwo w cyberprzestrzeni** | | | | | | |
| **Profil kształcenia: praktyczny** | | | | | | |
| **Poziom kształcenia: studia I stopnia** | | | | | | |
| **Liczba godzin w semestrze** | 1 | | 2 | | 3 | |
| | I | II | III | IV | V | **VI** |
| **Studia stacjonarne** (w/ćw/lab/pr/e)* | | | | | 16ćw | |
| **Studia niestacjonarne** (w/ćw/lab/pr/e) | | | | | 16ćw | |
| **JĘZYK PROWADZENIA ZAJĘĆ** | Polski | | | | | |
| **WYKŁADOWCA** | Mgr Patryk Błasik | | | | | |
| **FORMA ZAJĘĆ** | Ćwiczenia | | | | | |
| **CELE PRZEDMIOTU** | Zapoznanie studenta z obowiązującymi przepisami prawa w zakresie ochrony danych w sieci Internet oraz w zakresie ochrony cyberprzestrzeni RP jak również zdobycie umiejętności w zakresie umiejętności pracy z tekstami przepisów prawa. Dostarczenie studentom umiejętności rozumienia podstawowych kategorii pojęciowych opisujących problem bezpieczeństwa w cyberprzestrzeni. Wskazanie i charakterystyka rodzajów przestępczości w cyberprzestrzeni. Przekazanie umiejętności interpretacji przepisów prawnych, szczególnie w obszarze cyberbezpieczeństwa. Wskazanie i wypracowanie czynników wpływających na zapobieganie i zwalczanie przestępczości w cyberprzestrzeni. | | | | | |

| **Odniesienie do efektów uczenia się** | | **Opis efektów uczenia się** | **Sposób weryfikacji efektu uczenia się** |
|---|---|---|---|
| **Efekt kierunkowy** | **PRK** | | |
| **WIEDZA** | | | |
| BN_W0 4 | P6U_WK | Zna przepisy prawa w zakresie ochrony danych osobowych oraz gromadzenia i przesyłania danych cyfrowych oraz ich bezpieczeństwa; | egzamin zaliczeniowy pisemny (test wiedzy)<br>• dyskusja w trakcie zajęć ,<br>Realizacja prac etapowych - kazusy na kursie moodle. |
| **UMIEJĘTNOŚCI** | | | |
| BN_U01 | P6U_U | Potrafi pracować z tekstami ustaw, rozporządzeń, norm dotyczących cyberbezpieczeństwa; | • obserwacja wykonania zleconego zadania<br>• obserwacja zachowań i umiejętności podczas działań praktycznych |
| BN_U03 | P6U_U | Potrafi opracować regulamin, politykę, wytyczne dotyczące bezpieczeństwa danych cyfrowych; | • obserwacja wykonania zleconego zadania<br>• obserwacja zachowań i umiejętności podczas działań praktycznych |
| **KOMPETENCJE SPOŁECZNE** | | | |
| BN_K06 | P6U_K | Jest gotów do profesjonalnych działań w zakresie opracowywania regulaminów i polityk bezpieczeństwa danych cyfrowych; | obserwacja zachowań i umiejętności podczas zajęć i działań praktycznych |

**Nakład pracy studenta (w godzinach dydaktycznych 1h dyd.=45 minut)****

| **Stacjonarne** | **Niestacjonarne** |
|---|---|
| udział w wykładach = | udział w wykładach = |
| udział w ćwiczeniach = 16 | udział w ćwiczeniach = 16 |
| przygotowanie do ćwiczeń = 5 | przygotowanie do ćwiczeń = 5 |

| | |
|---|---|
| przygotowanie do wykładu =<br>przygotowanie do zaliczenia/egzaminu = 20<br>realizacja zadań projektowych = 20<br>e-learning =<br>zaliczenie/egzamin =<br>inne (konsultacje) = 2<br>**RAZEM:63**<br>**Liczba punktów ECTS:2,5**<br>**w tym w ramach zajęć praktycznych: 2,5** | przygotowanie do wykładu =<br>przygotowanie do zaliczenia/egzaminu = 20<br>realizacja zadań projektowych = 20<br>e-learning =<br>zaliczenie/egzamin =<br>inne (konsultacje) = 2<br>**RAZEM:63**<br>**Liczba punktów ECTS:2,5**<br>**w tym w ramach zajęć praktycznych: 2,5** |
| **WARUNKI WSTĘPNE** | Student posiada podstawową wiedzę z zakresu działania sieci Internet i obsługi komputera. |
| **TREŚCI PRZEDMIOTU** | Treści realizowane w formie bezpośredniej:<br>• Pojęcie Internetu, cyberprzestrzeni oraz cyberprzestępstwa w kontekście normatywnym i naukowym<br>• Omówienie założeń Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych RODO)<br>• Omówienie założeń Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa<br>• Rodzaje cyberprzestępstw<br>- przestępstwa stricte komputerowe<br>- przestępstwa związane z treścią informacji<br>- przestępstwa przeciwko czci<br>• Rozmiary i tendencje cyberprzestępczości<br>• Czynniki utrudniające ściganie cyberprzestępstw<br>• Zapobieganie i zwalczanie cyberprzestępczości<br>• Treści realizowane w formie e-learning: |
| **LITERATURA OBOWIĄZKOWA** | • Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych<br>• Tanner Nadean H." Blue team i cyberbezpieczeństwo. Zestaw narzędzi dla specjalistów od zabezpieczeń w sieci" Wydawnictwo Helion, 2021 |
| **LITERATURA UZUPEŁNIAJĄCA** | • Wasilewski, Janusz. "Zarys definicyjny cyberprzestrzeni." Przegląd Bezpieczeństwa Wewnętrznego 5.9 (2013): 225-234.<br>• Pala, Mariusz. "Wybrane aspekty bezpieczeństwa w cyberprzestrzeni." De Securitate et Defensione. O Bezpieczeństwie i Obronności 1.1 (2015): 113-130<br>• Stevens, Tim. Cyber security and the politics of time. Cambridge University Press, 2016. |
| **METODY NAUCZANIA** | W formie bezpośredniej:<br>- mini wykład<br>- case study<br>- praca w grupach i indywidualna<br>- prezentacja multimedialna |
| **POMOCE NAUKOWE** | Rzutnik multimedialny, tablica |
| **PROJEKT** | Cel projektu:<br>Temat projektu:<br>Forma projektu: |
| **FORMA I WARUNKI ZALICZENIA** | Prace etapowe : 3 kazusy.<br><br>Test wiedzy składa się z 12 pytań zamkniętych jednokrotnego wyboru. |

** W-wykład, ćw- ćwiczenia, lab- laboratorium, pro- projekt, e- e-learning*