**Załącznik do**
**Uchwały nr 17/15/07/2026**
**Senatu Uniwersytetu VIZJA**
**z dnia 15 lipca 2026 r.**

UNIWERSYTET VIZJA

# PROGRAM STUDIÓW

## CYBERBEZPIECZEŃSTWO

## STUDIA I STOPNIA

## PROFIL PRAKTYCZNY

Rok akademicki rozpoczęcia cyklu kształcenia: 2026/2027

## Ogólne informacje i wskaźniki dotyczące programu studiów

| | |
|---|---|
| Tytuł zawodowy nadawany absolwentom | **Licencjat** |
| Forma/formy studiów | **Studia stacjonarne i niestacjonarne** |
| Liczba semestrów konieczna do ukończenia studiów na danym poziomie | **6** |
| Liczba punktów ECTS konieczna do ukończenia studiów na danym poziomie | **180** |
| Łączna liczba godzin zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia | **Studia stacjonarne: 2338 godz.**<br>**Studia niestacjonarne 1620 godz.** |
| Procentowy udział liczby punktów ECTS dla każdej z dyscyplin, do których przyporządkowany jest kierunek w liczbie punktów ECTS koniecznej do ukończenia studiów na danym poziomie – w przypadku kierunku przyporządkowanego do więcej niż jednej dyscypliny | **Nauki o polityce i administracji 50,6%**<br>**Nauki o bezpieczeństwie 28,9%**<br>**Informatyka techniczna i telekomunikacja 20,6%** |
| Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia | **Studia stacjonarne: 90 (50 %)**<br>**Studia niestacjonarne: 63 (35 %)** |
| Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć kształtujących umiejętności praktyczne | **101 pkt. ECTS (56 %)** |
| Liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć z dziedziny nauk humanistycznych lub nauk społecznych – w przypadku kierunków studiów przyporządkowanych do dyscyplin w ramach dziedzin innych niż odpowiednio nauki humanistyczne lub nauki społeczne | **5 pkt. ECTS***<br>*W tym za zajęcia/grupy zajęć:<br>Wprowadzenie do filozofii |
| Liczba punktów ECTS przyporządkowana zajęciom lub grupom zajęć do wyboru | **58 pkt. ECTS (32 %)** |
| Wymiar praktyk zawodowych oraz liczba punktów ECTS, jaką student musi uzyskać w ramach tych praktyk | **6 miesięcy**<br>**720 godz.**<br>**28 pkt. ECTS** |
| Liczba godzin zajęć z wychowania fizycznego – w przypadku stacjonarnych studiów pierwszego stopnia i jednolitych studiów magisterskich | **60 godz.** |

## Zajęcia przewidziane programem studiów w podziale na moduły kształcenia wraz z liczbą godzin i punktów ECTS

| | Nazwa zajęć | ECTS | Liczba godzin zajęć dydaktycznych ogółem | |
|---|---|---|---|---|
| | | | Studia stacjonarne | Studia niestacjonarne |
| **1. Kształcenie ogólne** | | | | |

| | | | | |
|---|---|---|---|---|
| 1. | BHP | **0** | 8 | 8 |
| 2. | Zajęcia sportowo-rekreacyjne | **0** | 60 | 0 |
| 3. | Język obcy **(DW)** | **9** | 120 | 64 |
| 4. | Umiejętności akademickie | **1** | 15 | 8 |
| 5. | Wprowadzenie do filozofii | **5** | 35 | 20 |
| 6. | Podstawy komunikacji społecznej | **4** | 30 | 16 |
| 7. | Wstęp do nauk o państwie i prawie | **5** | 30 | 24 |
| 8. | Własność intelektualna | **5** | 30 | 24 |
| 9. | Metodologia badań naukowych | **4** | 30 | 16 |
| 10. | Prawoznawstwo | **5** | 60 | 40 |
| 11. | Podstawy ekonomii | **5** | 30 | 24 |
| 12. | Administracja publiczna | **4** | 30 | 24 |
| 13. | Podstawy socjologii | **3** | 30 | 16 |
| 14. | Zarządzanie projektami | **3** | 30 | 16 |
| | **Razem** | **48** | **508** | **276** |
| | **2. Kształcenie kierunkowe** | | | |
| 15. | Problemy bezpieczeństwa społeczeństwa informacyjnego | **3** | 30 | 16 |
| 16. | Wstęp do cyberbezpieczeństwa | **5** | 30 | 16 |
| 17. | Polityka cyberbezpieczeństwa państwa | **3** | 30 | 16 |
| 18. | Międzynarodowe stosunki polityczne | **4** | 30 | 24 |
| 19. | Wprowadzenie do nauk o bezpieczeństwie | **3** | 30 | 16 |
| 20. | Zarządzanie w sytuacjach kryzysowych | **4** | 45 | 32 |
| 21. | Bezpieczeństwo metropolii i społeczności lokalnych | **3** | 30 | 16 |
| 22. | Zarządzanie bezpieczeństwem informacji | **3** | 30 | 16 |
| 23. | Struktury bezpieczeństwa państwa | **3** | 30 | 16 |
| 24. | Współczesny terroryzm polityczny | **3** | 30 | 16 |
| 25. | Inżynieria informacji w przestrzeni publicznej | **3** | 30 | 16 |
| 26. | Wojna informacyjna i hybrydowa / Geoinformacja i geolokalizacja **(DW)** | **3** | 30 | 16 |
| 27. | Ochrona danych osobowych: ujęcie krajowe i międzynarodowe | **3** | 30 | 16 |
| 28. | Zarządzanie ryzykiem w polityce / Zarządzanie ryzykiem IT **(DW)** | **3** | 30 | 16 |
| 29. | Systemy i technologie w cyberbezpieczeństwie | **4** | 45 | 24 |
| 30. | Elementy kryptografii | **3** | 45 | 24 |
| 31. | Zachowania przestępcze w cyberprzestrzeni | **2** | 30 | 16 |
| 32. | Audyt bezpieczeństwa sieci teleinformatycznych | **4** | 60 | 32 |
| 33. | Metodyka przygotowania projektu | **3** | 30 | 16 |
| 34. | Cyberbezpieczeństwo w sektorze publicznym / Cyberbezpieczeństwo w organizacjach międzynarodowych **(DW)** | **3** | 30 | 16 |
| 35. | Przestępczość w sieci / Bezpieczeństwo dzieci i młodzieży online **(DW)** | **3** | 30 | 16 |
| 36. | Cyberkultura w XXI w. / Ramy prawne białego i czarnego wywiadu **(DW)** | **3** | 30 | 16 |
| 37. | Zwalczanie dezinformacji w Internecie | **3** | 30 | 16 |
| 38. | Techniki eksploracji Internetu | **3** | 30 | 16 |
| 39. | Bezpieczeństwo informacji w obrocie gospodarczym / Bezpieczeństwo informacji w administracji rządowej **(DW)** | **3** | 30 | 16 |
| 40. | Projekt społeczny | **5** | 30 | 16 |

| | | | | |
|---|---|---|---|---|
| 41. | Praktyka zawodowa | **28** | 720 | 720 |
| | **Razem** | **114** | **1599** | **1200** |
| | **3. Kształcenie informatyczne** | | | |
| 42. | Wstęp do programowania | **5** | 75 | 40 |
| 43. | Architektura systemów komputerowych | **5** | 60 | 32 |
| 44. | Technologie sieciowe | **4** | 60 | 32 |
| 45. | Systemy operacyjne | **4** | 60 | 32 |
| | **Razem** | **18** | **255** | **136** |
| | | | | |
| | **Ogółem w całym toku studiów** | **180** | **2362** | **1612** |

DW – zajęcia do wyboru

## Zajęcia lub grupy zajęć kształtujących umiejętności praktyczne

| **Nazwa zajęć lub grupy zajęć** | **Forma/formy zajęć** | **Łączna liczba godzin** | | **Liczba punktów ECTS** |
|---|---|---|---|---|
| | | **Studia stacjonarne** | **Studia niestacjonarne** | |
| Język obcy **(DW)** | lektoraty | 120 | 64 | **9** |
| Prawoznawstwo | ćwiczenia | 30 | 16 | **2,5** |
| Polityka cyberbezpieczeństwa państwa | ćwiczenia | 30 | 16 | **3** |
| Zarządzanie w sytuacjach kryzysowych | ćwiczenia | 30 | 24 | **2** |
| Bezpieczeństwo metropolii i społeczności lokalnych | konwersatorium | 30 | 16 | **3** |
| Zarządzanie bezpieczeństwem informacji | konwersatorium | 30 | 16 | **3** |
| Zwalczanie dezinformacji w Internecie | konwersatorium | 30 | 16 | **3** |
| Wstęp do programowania | laboratorium | 45 | 24 | **3** |
| Inżyniera informacji w przestrzeni publicznej | konwersatorium | 30 | 16 | **3** |
| Wojna informacyjna i hybrydowa / Geoinformacja i geolokalizacja **(DW)** | konwersatorium | 30 | 16 | **3** |
| Zarządzanie ryzykiem w polityce / Zarządzanie ryzykiem IT **(DW)** | konwersatorium | 30 | 16 | **3** |
| Systemy i technologie w cyberbezpieczeństwie | laboratorium | 30 | 16 | **2,7** |
| Architektura systemów komputerowych | laboratorium | 30 | 16 | **2,5** |
| Elementy kryptografii | ćwiczenia | 30 | 16 | **2** |
| Zachowania przestępcze w cyberprzestrzeni | konwersatorium | 30 | 16 | **2** |
| Audyt bezpieczeństwa sieci teleinformatycznych | ćwiczenia | 30 | 16 | **2** |
| Technologie sieciowe | laboratorium | 30 | 16 | **2** |
| Systemy operacyjne | laboratorium | 30 | 16 | **2** |
| Metodyka przygotowania projektu | konwersatorium | 30 | 16 | **3** |
| Cyberbezpieczeństwo w sektorze publicznym / Cyberbezpieczeństwo w organizacjach międzynarodowych **(DW)** | konwersatorium | 30 | 16 | **3** |
| Przestępczość w sieci / Bezpieczeństwo dzieci i młodzieży online **(DW)** | konwersatorium | 30 | 16 | **3** |
| Techniki eksploracji Internetu | laboratorium | 30 | 16 | **3** |
| Bezpieczeństwo informacji w obrocie gospodarczym / Bezpieczeństwo informacji w administracji rządowej **(DW)** | konwersatorium | 30 | 16 | **3** |
| Projekt społeczny | konwersatorium | 30 | 16 | **5** |
| Praktyka zawodowa **(DW)** | praktyki | 720 | 720 | **28** |
| | **Razem** | **1545** | **1160** | **101** |

DW – zajęcia do wyboru

## Zajęcia lub grupy zajęć do wyboru

| Nazwa zajęć lub grupy zajęć | Forma/formy zajęć | Łączna liczba godzin | | Liczba punktów ECTS |
|---|---|---|---|---|
| | | Studia stacjonarne | Studia niestacjonarne | |
| Język obcy | lektoraty | 120 | 64 | **9** |
| Polityka cyberbezpieczeństwa państwa/Problemy bezpieczeństwa społeczeństwa informacyjnego | konwersatorium | 30 | 16 | **3** |
| Zarządzanie ryzykiem w polityce / Zarządzanie ryzykiem IT | konwersatorium | 30 | 16 | **3** |
| Przestępczość w sieci / Bezpieczeństwo dzieci i młodzieży online | konwersatorium | 30 | 16 | **3** |
| Cyberbezpieczeństwo w sektorze publicznym / Cyberbezpieczeństwo w organizacjach międzynarodowych | konwersatorium | 30 | 16 | **3** |
| Wojna informacyjna i hybrydowa / Geoinformacja i geolokalizacja | konwersatorium | 30 | 16 | **3** |
| Cyberkultura w XXI w. / Ramy prawne białego i czarnego wywiadu | wykłady | 30 | 16 | **3** |
| Bezpieczeństwo informacji w obrocie gospodarczym / Bezpieczeństwo informacji w administracji rządowej | konwersatorium | 30 | 16 | **3** |
| Praktyka zawodowa | praktyki | 720 | 720 | **28** |
| | **Razem** | **1050** | **896** | **58** |

## *Efekty uczenia się*

Efekty uczenia się uwzględniają uniwersalne charakterystyki drugiego stopnia dla poziomów 6-7 określone w ustawie z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji *(Dz. U. z 2016 r., poz. 64 i 1010)* oraz charakterystyki drugiego stopnia określone w rozporządzeniu Ministra Nauki i Szkolnictwa Wyższego z dnia 14 listopada 2018 r. w sprawie charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 Polskiej Ramy Kwalifikacji oraz charakterystyki dotyczące kompetencji inżynierskich.

Absolwent **studiów pierwszego stopnia** na kierunku **cyberbezpieczeństwo** uzyskuje kwalifikację pełną na poziomie 6 Polskiej Ramy Kwalifikacji.

| Kategoria charakterystyki efektów uczenia się | Symbol kierunkowych efektów uczenia się | Po ukończeniu studiów pierwszego stopnia na kierunku **CYBERBEZPIECZEŃSTWO** absolwent: | Odniesienie do | |
|---|---|---|---|---|
| | | | uniwersalnych charakterystyk pierwszego stopnia PRK | charakterystyki drugiego stopnia PRK |
| **W ZAKRESIE WIEDZY** | | | | |
| WIEDZA - zakres i głębia | CYB_WG01 | zna i rozumie w zaawansowanym stopniu miejsce nauk o bezpieczeństwie, nauk o polityce i administracji oraz wybranych nauk technicznych i informatycznych w systemie nauk, ich wzajemne zależności oraz zastosowania praktyczne w obszarze cyberbezpieczeństwa | P6U_W | P6S_WG |
| | CYB_WG02 | zna i rozumie w zaawansowanym stopniu struktury, instytucje i procesy społeczne, polityczne, prawne, ekonomiczne i kulturowe istotne dla funkcjonowania państwa, administracji, organizacji oraz systemu bezpieczeństwa cyfrowego oraz praktyczne zastosowanie tej wiedzy w obszarze cyberbezpieczeństwa | P6U_W | P6S_WG |
| | CYB_WG03 | zna i rozumie w zaawansowanym stopniu relacje między strukturami i instytucjami społecznymi, politycznymi i gospodarczymi w wymiarze krajowym, europejskim, międzynarodowym i międzykulturowym, ze szczególnym uwzględnieniem ich znaczenia dla cyberbezpieczeństwa oraz praktyczne zastosowanie tej wiedzy w obszarze cyberbezpieczeństwa | P6U_W | P6S_WG |
| | CYB_WG04 | zna i rozumie w zaawansowanym stopniu normy, reguły prawne, organizacyjne, etyczne i społeczne regulujące funkcjonowanie struktur publicznych, gospodarczych i społecznych, w tym instytucji odpowiedzialnych za bezpieczeństwo i cyberbezpieczeństwo oraz praktyczne zastosowanie tej wiedzy w obszarze cyberbezpieczeństwa | P6U_W | P6S_WG |
| | CYB_WG06 | zna i rozumie w zaawansowanym stopniu rolę informacji, technologii cyfrowych, społeczeństwa informacyjnego i komunikacji cyfrowej w procesach społecznych, politycznych, administracyjnych, gospodarczych i bezpieczeństwa oraz praktyczne zastosowanie tej wiedzy w obszarze cyberbezpieczeństwa | P6U_W | P6S_WG |

| | | | | |
|---|---|---|---|---|
| | CYB_WG07 | zna i rozumie w zaawansowanym stopniu metody, narzędzia i techniki pozyskiwania, przetwarzania, analizy i interpretacji danych oraz informacji wykorzystywanych do opisu struktur, instytucji, procesów i zagrożeń w obszarze cyberbezpieczeństwa bezpieczeństwa oraz praktyczne zastosowanie tej wiedzy w obszarze cyberbezpieczeństwa | P6U_W | P6S_WG |
| WIEDZA<br>- kontekst | | | | |
| | CYB_WK01 | .<br>zna i rozumie fundamentalne dylematy współczesnej cywilizacji związane z rozwojem technologii cyfrowych, bezpieczeństwem informacji, ochroną prywatności, funkcjonowaniem państwa, społeczeństwa i gospodarki cyfrowej | P6U_W | P6S_WK |
| | CYB_WK02 | zna i rozumie podstawowe pojęcia i zasady z zakresu ochrony własności przemysłowej i prawa autorskiego oraz podstawowe zasady tworzenia i rozwoju różnych form przedsiębiorczości, w tym inicjatyw związanych z technologiami cyfrowymi i cyberbezpieczeństwem | P6U_W | P6S_WK |
| | CYB_WK03 | .<br>zna i rozumie podstawowe ekonomiczne, prawne, etyczne, społeczne i organizacyjne uwarunkowania działalności zawodowej związanej z cyberbezpieczeństwem, w tym zasady odpowiedzialnego stosowania nowych technologii cyfrowych | P6U_W | P6S_WK |
| **W ZAKRESIE UMIEJĘTNOŚCI** | | | | |
| UMIEJĘTNOŚCI<br>– wykorzystanie wiedzy | CYB_UW01 | .<br>potrafi wykorzystywać posiadaną wiedzę do formułowania i rozwiązywania złożonych oraz nietypowych problemów społecznych, organizacyjnych, prawnych i technologicznych związanych z bezpieczeństwem cyfrowym | P6U_U | P6S_UW |
| | CYB_UW02 | potrafi pozyskiwać, analizować, interpretować i krytycznie oceniać dane oraz informacje dotyczące zjawisk społeczno-politycznych, technologicznych i bezpieczeństwa, w tym zagrożeń cybernetycznych | P6U_U | P6S_UW |
| | CYB_UW03 | .<br>potrafi dobierać i stosować właściwe metody, narzędzia oraz techniki informacyjno-komunikacyjne do analizy problemów, oceny ryzyka i proponowania rozwiązań w obszarze cyberbezpieczeństwa | P6U_U | P6S_UW |
| | CYB_UW04 | potrafi analizować proponowane rozwiązania problemów praktycznych z zakresu cyberbezpieczeństwa, oceniać ich skutki oraz formułować uzasadnione rekomendacje działań | P6U_U | P6S_UW |

| | | | | |
|---|---|---|---|---|
| | | | | |
| UMUMIEJĘTNOŚCI – komunikowanie się | | | | |
| | CYB_UK01 | potrafi komunikować się z otoczeniem z użyciem specjalistycznej terminologii właściwej dla bezpieczeństwa, cyberbezpieczeństwa, technologii cyfrowych i nauk społecznych | P6U_U | P6S_UK |
| | CYB_UK02 | .<br>potrafi przygotowywać wypowiedzi pisemne i ustne, w tym komunikaty, raporty, ekspertyzy i prezentacje, oraz przedstawiać i uzasadniać własne stanowisko na podstawie analizy źródeł i danych | P6U_U | P6S_UK |
| | CYB_UK03 | potrafi posługiwać się językiem obcym na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego, w tym podstawową terminologią specjalistyczną z zakresu bezpieczeństwa i cyberbezpieczeństwa | P6U_U | P6S_UK |
| UMIEJĘTNOŚCI – organizacja pracy | | | | |
| | CYB_UO01 | potrafi planować i organizować pracę indywidualną oraz współdziałać z innymi osobami w zespołach, także interdyscyplinarnych, realizujących zadania analityczne, diagnostyczne, projektowe lub pomocowe w obszarze cyberbezpieczeństwa | P6U_U | P6S_UO |
| UMIEJĘTNOŚCI – uczenie się | | | | |
| | CYB_UU01 | potrafi samodzielnie planować i realizować własne uczenie się przez całe życie, korzystać z różnorodnych źródeł informacji, w tym w języku obcym, oraz aktualizować wiedzę z zakresu cyberbezpieczeństwa i technologii cyfrowych | P6U_U | P6S_UU |
| **W ZAKRESIE KOMPETENCJI SPOŁECZNYCH** | | | | |
| KOMPETENCJE – oceny – krytyczne | CYB_KK01 | .<br>jest gotów do krytycznej oceny posiadanej wiedzy, wiarygodności źródeł i odbieranych treści, uznawania znaczenia wiedzy eksperckiej w rozwiązywaniu problemów praktycznych oraz zasięgania opinii specjalistów w przypadku trudności z samodzielnym rozwiązaniem problemu | P6U_K | P6S_KK |
| KOMPETENCJE - odpowiedzialn | | | | |
| | CYB_KO01 | jest gotów do myślenia i działania w sposób przedsiębiorczy, w tym do inicjowania, wspierania i rozwijania przedsięwzięć związanych z cyfryzacją, bezpieczeństwem informacji i cyberbezpieczeństwem | P6U_K | P6S_KO |
| | CYB_KO02 | jest gotów do wypełniania zobowiązań społecznych oraz współorganizowania działań na rzecz interesu publicznego, w szczególności w zakresie bezpieczeństwa cyfrowego, ochrony informacji i odpowiedzialnego korzystania z technologii | P6U_K | P6S_KO |
| | | | | |

| | | | | |
|---|---|---|---|---|
| | CYB_KR01 | jest gotów do odpowiedzialnego pełnienia ról zawodowych w obszarze cyberbezpieczeństwa, przestrzegania zasad etyki zawodowej, dbałości o dorobek i standardy zawodu oraz odpowiedzialności za skutki własnych działań, opinii i decyzji | P6U_K | P6S_KR |

Objaśnienia oznaczeń:

| | |
|---|---|
| **CYB** | - kierunek studiów: „cyberbezpieczeństwo” |
| **WG** | - kategoria efektów uczenia się: „wiedza” – „zakres i głębia” |
| **WK** | - kategoria efektów uczenia się: „wiedza” – „kontekst” |
| **UK** | - kategoria efektów uczenia się: „umiejętności” – „komunikowanie się” |
| **UO** | - kategoria efektów uczenia się: „umiejętności” – „organizacja pracy” |
| **UU** | - kategoria efektów uczenia się: „umiejętności” – „uczenie się” |
| **UW** | - kategoria efektów uczenia się: „umiejętności” – „wykorzystanie wiedzy” |
| **KK** | - kategoria efektów uczenia się: „kompetencje społeczne” – „krytyczne podejście” |
| **KO** | - kategoria efektów uczenia się: „kompetencje społeczne” – „odpowiedzialność” |
| **KR** | - kategoria efektów uczenia się: „kompetencje społeczne” – „rola zawodowa” |
| **01 i kolejne** | - numery efektów uczenia się |

**Zajęcia lub grupy zajęć, niezależnie od formy ich prowadzenia, wraz z przypisaniem do nich efektów uczenia się i treści programowych zapewniających uzyskanie tych efektów oraz liczby punktów ECTS**

| 1. KSZTAŁCENIE OGÓLNE | | |
|---|---|---|
| | | |
| **Kierunkowe efekty uczenia się** | **BHP** | **ECTS: 0** |
| | Definicja i istota bezpieczeństwa i higieny pracy. Podstawowe akty prawne z zakresu BHP (Kodeks Pracy, Rozporządzenie w sprawie BHP na uczelniach, Ustawa o Ochronie Przeciwpożarowej, Rozporządzenie w sprawie ogólnych przepisów BHP, Rozporządzenie w sprawie szkolenia z zakresu BHP, Rozporządzenie w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie). Instytucje pełniące nadzór nad przestrzeganiem przepisów BHP. Obowiązki i uprawnienia Rektora w zakresie przestrzegania zasad BHP na uczelni. Ogólne zasady BHP obowiązujące na terenie uczelni. Ogólne zasady dotyczące budynków, pomieszczeń, maszyn i urządzeń oraz wymagania, jakie powinny spełniać. Zasady wyposażenia budynków/pomieszczeń w sprzęt gaśniczy, apteczki. Zasady poruszania się w ciągach komunikacyjnych. Definicja czynników szkodliwych oraz działania optymalizujące działania czynników. Zagrożenia wypadkowe, rodzaje wypadków. Przyczyny wypadków. Podstawowe zasady ochrony przeciwpożarowej. Akty prawne w zakresie PPOŻ. Zapobieganie zagrożeniom pożarowym. Zasady postępowania w przypadku wystąpienia zagrożenia pożaru. Zasady posługiwania się sprzętem gaśniczym. Rodzaje gaśnic. Procedury ewakuacyjne. Stosowane znaki ewakuacji. Znaki bezpieczeństwa stosowane w ochronie przeciwpożarowej. Postępowanie w razie wypadku. Przepisy regulujące obowiązek udzielenia pierwszej pomocy poszkodowanemu. Podstawowe zabiegi resuscytacyjne. Pozycja boczna ustalona. Opatrywanie zranień, złamań, zwichnięć, oparzeń. Postępowanie w przypadku porażenia prądem elektrycznym. Postępowanie w przypadku zatruć. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Umiejętności akademickie** | **ECTS: 1** |
| CYB_WG06<br>CYB_WG07<br>CYB_WK01 | Wartości akademickie. Odróżnienie nauki od pseudonauki. Obiektywizm, sceptycyzm, dążenie do prawdy, otwartość na nowe informacje, dążenie do zdobywania kompetencji, sumienność. Ochrona wartości intelektualnej i przemysłowej, bezstronne, niezafałszowane prezentowanie danych. Identyfikowanie problemu. Prezentacja konkretnych przykładów problemów. Poszukiwanie zagadnienia, które dla studenta jest ważne, które wzbudza jego zainteresowanie i potrzebę działania. Przedstawienie opisu problemu. Rozumowanie. Myślenie racjonalne i intuicyjne. Błędy i zniekształcenia myślenia racjonalnego, błędy logiczne. Wnioskowanie. Komunikowanie. Styl pisania tekstów akademickich. Struktura różnych rodzajów tekstów akademickich. Przedstawianie i ocena argumentów obu stron sporu akademickiego. Analiza dyskusji problemu. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Wprowadzenie do filozofii** | **ECTS: 5** |
| CYB_WG02<br>CYB_WG04<br>CYB_WK03 | Filozofia jako refleksja i wiedza o świecie. Struktura filozofii. Metoda filozofii. Cele filozofii. Gatunki wiedzy ludzkiej. Filozofia a nauka. Spory o naturę rzeczywistości (pytanie o arche, spór o substancje: monizm, dualizm, pluralizm, spór o istnienie świata: realizm - idealizm). Wielkie systemy ontologiczno-metafizyczne (Platona, Arystotelesa, św. Augustyna, św. Tomasza, Kartezjusza, Kanta, Hegla). Spór o źródła poznania: racjonalizm genetyczny (natywizm), empiryzm genetyczny, racjonalizm-irracjonalizm. Spór o metodę poznania (aprioryzm, aposterioryzm). Spór o przedmiot (granice) poznania (realizm, sceptycyzm, agnostycyzm). Wybrane koncepcje prawdy: klasyczna (arystotelesowska) koncepcja prawdy, nieklasyczne teorie prawdy. Problem absolutności i względności prawdy. Antropologia filozoficzna: problem psychofizyczny, dualizm antropologiczny (Platon, Kartezjusz), hylemorfizm Arystotelesa, chrześcijańskie koncepcje człowieka, egzystencjalistyczna wizja człowieka). Podstawowe nurty współczesnej filozofii (pozytywizm i neopozytywizm, egzystencjalizm, filozofia dialogu, personalizm, pragmatyzm i postmodernizm). Fundamentalne pytania filozofii wartości (spór o istnienie wartości, ład aksjologiczny, poznanie wartości). Kierunki i szkoły w etyce. Etyka opisowa i etyka normatywna. Zagadnienia sensu i celu życia. Filozofia społeczna. Podstawowe wartości społeczne: sprawiedliwość, równość, wolność. Wizje dobrego państwa. Wybrane zagadnienia estetyki (piękno jako idea, subiektywizacja i indywidualizacja piękna w świetle krytyki smaku, doświadczenie estetyczne, piękno natury). Filozofia języka (język jako medium i jako przedmiot poznania, natura znaczenia, użycie języka, rozumienie języka, relacja między | |

| | | |
|---|---|---|
| | językiem a rzeczywistością). Spór o uniwersalia. Tłumaczenie i interpretacja. Poznanie a rozumienie. Debata oksfordzka nad tezami filozoficznymi. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Podstawy komunikacji społecznej** | **ECTS: 4** |
| CYB_WG02<br>CYB_WG03<br>CYB_WG07<br>CYB_WK03 | Komunikacja społeczna – definicje, modele i tradycje badawcze. Komunikacja interpersonalna – teorie poświęcone przekazom interpersonalnym, budowaniu i podtrzymywaniu relacji oraz wywieraniu wpływu. Komunikacja publiczna i grupowa – teorie poświęcone komunikacji grupowej, publicznej i w organizacjach. Komunikacja masowa – teorie poświęcone kulturze i mediom oraz efektom medialnym. Komunikacja interkulturowa – teorie poświęcone kontaktom interkulturowym i procesom adaptacji. Integracja teorii komunikacji. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Własność intelektualna** | **ECTS: 5** |
| CYB_WG06<br>CYB_WG07<br>CYB_WK02<br>CYB_WK03 | Wprowadzenie do pojęcia własności intelektualnej: zakres, podział, znaczenie społeczne i gospodarcze<br>Prawa autorskie: autorskie prawa osobiste i majątkowe, czas trwania ochrony, pola eksploatacji<br>Dozwolony użytek edukacyjny i prywatny – gdzie leżą granice legalnego korzystania<br>Plagiat, autoplagiat, uczciwość akademicka – standardy etyczne i prawne<br>Własność przemysłowa: wynalazki, znaki towarowe, wzory przemysłowe, know-how<br>Cyfrowe środowisko pracy i twórczości: otwarte zasoby edukacyjne, AI i prawo, ochrona danych | |
| | | |
| **Kierunkowe efekty uczenia się** | **Zajęcia sportowo-rekreacyjne** | **ECTS: 0** |
| | Zasady bezpiecznego uczestnictwa w zajęciach sportowo-rekreacyjnych. Trening zdrowotny. Formy aktywności ruchowej przy muzyce - aerobik, TBC, joga. Ćwiczenia kształtujące sylwetkę z wykorzystaniem sprzętu fitness. Zespołowe gry sportowe - piłka nożna. Zajęcia aerobowe. Rodzaje zajęć aerobowych. Trening aerobowy i jego funkcje. Nauka i demonstracja techniki ćwiczeń. Zespołowe gry sportowe - piłka siatkowa. Tenis stołowy - nauka i doskonalenie wykonania podstawowych elementów technicznych. Elementy tańca towarzyskiego. Samba, cha-cha, rumba, salsa, jive, disco samba, rock'n'roll, walc angielski, tango, walc wiedeński, slow fox i quickstep. Zajęcia korekcyjno- kompensacyjne wsparte ćwiczeniami relaksacyjnymi. Zespołowe gry sportowe – koszykówka. Zespołowe gry sportowe - piłka ręczna. Badminton - nauka i doskonalenie podstawowych elementów technicznych. Futsal - nauka i doskonalenie techniki gry. Kształtowanie sprawności ruchowej oraz umiejętności technicznych przez gry i ćwiczenia ogólnorozwojowe. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Język obcy (angielski)** | **ECTS: 9** |
| CYB_UK01<br>CYB_UK02<br>CYB_UK03 | ***Semestr I***, Przymiotniki opisujące wygląd, osobowość i zachowanie człowieka. Struktura i zastosowanie czasów teraźniejszych: czas teraźniejszy prosty - Present Simple. Środowisko naturalne i ochrona przyrody – leksyka. Struktura i zastosowanie czasów teraźniejszych: czas teraźniejszy ciągły - Present Continuous. Zdrowie i ciało człowieka – leksyka. Kontrastywne zastosowanie czasów teraźniejszych: Present Simple vs Present Continuous. Turystyka, podróże i wakacje – leksyka. Struktura i zastosowanie czasów teraźniejszych: czas Present Perfect Simple and Continuous (skutek vs akcja). Czas wolny człowieka: hobby, sport, rekreacja – leksyka. Kontrastywne, kompleksowe zastosowanie wszystkich czasów teraźniejszych języka angielskiego.<br>***Semestr II.*** Pobyt w hotelu - problemy i ich rozwiązywanie -leksyka. Struktura i zastosowanie czasów przeszłych: czas przeszły prosty - Past Simple - czasowniki regularne i nieregularne. Państwa świata – leksyka. Struktura i zastosowanie czasów przeszłych: czas przeszły ciągły - Past Continuous. Handel, biznes i komunikacja biznesowa – leksyka. Kontrastywne zastosowanie czasów przeszłych: Past Simple vs Past Continous. Systemy ustrojowe – leksyka. Struktura i zastosowanie czasów przeszłych: czas Past Perfect. Moda i ubrania – leksyka. Kontrastywne, kompleksowe zastosowanie wszystkich czasów przeszłych języka angielskiego.<br>***Semestr III***. Cyberbezpieczeństwo – leksyka. Struktura i zastosowanie czasów przyszłych: czas przyszły prosty - Will + infinitive. Konflikty- leksyka. Struktura i zastosowanie czasów przyszłych: wyrażenie "going to" - plany i przewidywanie przyszłości. Sport – leksyka. Struktura i zastosowanie czasów przyszłych: zaaranżowana przyszłość - Present Continuous for future. Życie na wsi i w mieście – leksyka. Kontrastywne zastosowanie czasów przyszłych: will = infinitive, going to, Present Continuous for future. Samorządy lokalne – leksyka. Kontrastywne, kompleksowe zastosowanie wszystkich czasów przyszłych języka angielskiego (z | |

| | | |
|---|---|---|
| | uwzględnieniem Future Continuous, Future Perfect i form opisowych).<br>***Semestr IV.*** Instytucje międzynarodowe – leksyka. Zdania złożone - struktura i zastosowanie - kompleksowe zastosowanie spójników. Prawo i systemy podatkowe – leksyka. Czasowniki frazowe - rozdzielne i nierozdzielne. Dyplomacja – leksyka. Czasowniki modalne - ich funkcje i formy. Analiza i tłumaczenie tekstów specjalistycznych z zakresu polityki i administracji. Mowa zależna w języku angielskim - zasady tworzenia i zastawania. Prezentacja wybranego tematu z zakresu polityki i administracji w języku angielskim - wypowiedź ustna. Kompleksowe zastosowanie rzeczowników, przymiotników, i przysłówków w różnych zdaniach z uwzględnieniem wszystkich czasów języka angielskiego (teraźniejszość, przeszłość, przyszłość). | |
| | | |
| **Kierunkowe efekty uczenia się** | **Język obcy (niemiecki)** | **ECTS: 9** |
| CYB_UK01<br>CYB_UK02<br>CYB_UK03 | ***Semestr I.*** Przymiotniki opisujące wygląd, osobowość i zachowanie człowieka. Rodzajnik określony i nieokreślony odmiana przez przypadki. Środowisko naturalne i ochrona przyrody – leksyka. Zaimek osobowy - odmiana przez przypadki. Zdrowie i ciało człowieka – leksyka. Rzeczownik niemiecki - odmiana przez przypadki - Nominativ, Genitiv, Dativ, Akkusativ. Turystyka, podróże i wakacje – leksyka. Czasowniki modalne, czasowniki haben i sein - odmiana i zastosowanie. Czas wolny człowieka: hobby, sport, rekreacja – leksyka. Przyimki niemieckie z Dativ i Akkusativ<br>***Semestr II.*** Pobyt w hotelu - problemy i ich rozwiązywanie – leksyka. Czas przeszły Perfekt z haben i sein - czasowniki słabe i mocne. Państwa świata – leksyka. Czas przeszły Praeteritum - odmiana czasowników. Handel, biznes i komunikacja biznesowa – leksyka. Czasowniki niemieckie wymagające przypadków Dativ i Akkusativ. Systemy ustrojowe – leksyka. Zdania złożone podrzędnie. Moda i ubrania – leksyka. Tryb rozkazujący języka niemieckiego.<br>***Semestr III.*** Cyberbezpieczeństwo – leksyka. Zdanie podrzędne dopełnieniowe i okolicznikowe celu (z dass i damit). Konflikty- leksyka. Stopniowanie przymiotników niemieckich. Sport – leksyka. Zdanie podrzędne warunkowe i przyczynowe (z wenn i weil). Laboratorium i sprzęt laboratoryjny – leksyka. Czasowniki zwrotne w Dativ i Akkusativ. Samorządy lokalne – leksyka. Zdanie podrzędne czasowe i ograniczające (z wenn, waehrend, obwohl).<br>***Semestr IV.*** Instytucje międzynarodowe – leksyka. Zaimki i zdania względne. Prawo i systemy podatkowe – leksyka. Tryb przypuszczający czasowników słabych i mocnych Konjunkitv II. Dyplomacja – leksyka. Strona bierna Passiv - wszystkie czasy. Analiza i tłumaczenie tekstów specjalistycznych z zakresu polityki i administracji. Czas przeszły Plusqamperfekt. Prezentacja wybranego tematu z zakresu polityki i administracji w języku angielskim - wypowiedź ustna. Czas przyszły Futur I i II | |
| | | |
| **Kierunkowe efekty uczenia się** | **Metodologia badań naukowych** | **ECTS: 4** |
| CYB_WG02<br>CYB_WG04<br>CYB_WG07<br>CYB_WK03 | Podstawy nauk społecznych - wprowadzenie w zasady dziedziny, wyjaśnienie podstawowych pojęć i kategorii. Dialektyka badań społecznych - wybrane zestawienia (indukcja, dedukcja, wyjaśnianie idiograficzne, nomotetyczne). Paradygmaty w naukach społecznych. Tradycyjny model nauki - zasady i założenia. Teoria indukcyjna i dedukcyjna - wyjaśnienie, teoria, przykłady, budowa. Pojęcie i kategoria przyczynowości w badaniach społecznych. Struktura procesu badawczego - plan badań, operacjonalizacja, konceptualizacja, pomiar. Typy obserwacji - eksperyment, badania sondażowe. Analiza danych jakościowych - odkrywanie prawidłowości, przetwarzanie danych. Podstawy analizy ilościowej. Etyka i polityka w badaniach społecznych - społeczny kontekst badań. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Prawoznawstwo** | **ECTS: 5** |
| CYB_WG02<br>CYB_WG04<br>CYB_WK03 | Charakterystyka prawoznawstwa- podstawowe zagadnienia prawa i prawoznawstwa: prawoznawstwo jako nauka; pojęcie prawa i jego funkcje; ogólna charakterystyka prawoznawstwa; dziedziny i metody badawcze prawoznawstwa; prawo jako przedmiot badań. Prawo a władza publiczna w państwie. Podstawowe zagadnienia tworzenia i stosowania prawa: prawo a inne regulatory zachowań - cechy głównych norm społecznych; podstawowe kierunki sporów o prawo, znaczenie komunikacji społecznej w pracy prawnika. Prawo w wymiarach: | |

| | | |
|---|---|---|
| | formalnym, aksjologicznym, realnym. Przepisy i normy prawne- podstawowe elementy prawa: charakterystyka struktury normy prawnej; przepisy, zasady prawne; język prawny i język prawniczy. Stanowienie prawa: formy tworzenia prawa; etapy stosowania prawa; akty normatywne; tryb tworzenia prawa, zasady technik prawodawczych; źródła prawa. Podstawowe pojęcia związane z wykładnią i wnioskowaniem: elementy teorii argumentacji; teorie wykładni prawa; koncepcja walidacyjna, derywacyjna, klaryfikacyjna; reguły interpretacyjne wykładni; podział wykładni ze względu na podmiot jej dokonujący; reguły wnioskowań prawniczych, toposy prawnicze. Stosunek prawny: fakty prawne, rodzaje i ich kwalifikacja; podmiot, treść i przedmiot stosunku prawnego. Obowiązywanie prawa, przestrzeganie prawa: w ujęciach: socjologicznym, aksjologicznym, formalnym (tetycznym). Odpowiedzialność prawna. System prawa i jego charakterystyka. Stosowanie prawa: modele stosowania prawa; proces stosowania prawa; tryby rozwiązywania sporów i konfliktów. Specyfika warsztatu pracy prawnika: w różnorodnych systemach prawnych, w wielokulturowym systemie; działalność między człowiekiem a społeczeństwem- państwa prawa; poza wiedzą, niezbędne są umiejętności praktyczne, wielopłaszczyznowe kwalifikacje; nabycie kompetencji komunikacyjnych; zawody prawnicze- prawnicy przyszłości. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Administracja publiczna** | **ECTS: 3** |
| CYB_WG02<br>CYB_WG03<br>CYB_WK03 | Istota i geneza oraz ewolucja administracji publicznej. Funkcje administracji publicznej. Podział terytorialny. Rada Ministrów RP. Kadry Administracji. Demokratyczne państwo prawa. Biurokracja. Źródła praw administracyjnego. Kontrola administracji. Administracja a polityka | |
| | | |
| **Kierunkowe efekty uczenia się** | **Zarządzanie projektami** | **ECTS: 3** |
| CYB_WG04<br>CYB_WG07<br>CYB_WK02<br>CYB_WK03 | Podstawowe pojęcia: projekt, portfel projektów, program, zakres projektu, interesariusze projektu, typowe problemy projektów, projekt w różnych typach organizacji. Procesy zarządzania projektem: procesy rozpoczęcia projektu, procesy planowania projektu, procesy realizacji projektu, procesy kontroli projektu, procesy zakończenia projektu. Obszary zarządzania projektami: zarządzanie integralnością projektu, zarządzanie zakresem, zarządzanie czasem, zarządzanie kosztami, zarządzanie jakością, zarządzanie zasobami ludzkimi, zarządzanie komunikacją, zarządzanie ryzykiem, zarządzanie zaopatrzeniem. Metody, techniki i narzędzia zarządzania projektami: zarządzanie cyklem życia projektu, matryca logiczna (struktura matrycy, logika pionowa oraz logika pozioma matrycy), etap analizy (interesariusze, strategia, cele, problemy) i etap planowania; Metodyka PMBOK (grupy procesów oraz obszary wiedzy), Metodyka zarządzania projektami Ten Step, Scrum, Adaptacyjne Zarządzanie Projektami (APD), Metodyka PRINCE2 (komponenty, techniki projektowe), struktura organizacyjna projektu i podziału pracy, metody sieciowe (PDM, PERT), metoda ścieżki krytycznej (CPM), metody estymacji kosztów, analiza jakościowa i ilościowa ryzyka, rejestry ryzyka, metryka ryzyka, rezerwy projektowe, kanały i plan komunikacji, zarządzanie dokumentacją projektu. Krytyczne czynniki sukcesu projektu, przyczyny porażek w realizacji projektów, zapobieganie niepowodzeniom. Budowanie zespołu projektowego: struktury zespołów projektowych, komunikacja w zespole projektowym, koncepcja ról zespołowych, kompetencje menedżera projektu, współpraca w zespole projektowym. Monitoring i ewaluacja projektów: system raportowania, elektroniczne bazy danych.. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Podstawy socjologii** | **ECTS: 5** |
| CYB_WG02<br>CYB_WG03<br>CYB_WG04<br>CYB_WK03 | Powstanie socjologii. Grupa społeczna;; .Kapitał społeczny i dylematy współzawodnictwa w życiu społecznym. Ład społeczny. Tożsamość społeczna. Role społeczne. Pojęcie socjalizacji. Zróżnicowanie społeczne: stratyfikacja i klasy społeczne; kultura społeczna. Zróżnicowanie społeczne: antropologia i płeć; Zróżnicowanie społeczne: bieda, wykluczenie i marginalizacja społeczna; Społeczeństwo obywatelskie; Kultura polityczna, Kontrola społeczna, Rodzina; | |
| | | |
| **Kierunkowe efekty uczenia się** | **Podstawy ekonomii** | **ECTS: 5** |

| | |
|---|---|
| CYB_WG02<br>CYB_WG03<br>CYB_WG04 | Charakterystyka osobliwości ekonomii jako nauki – analiza najważniejszych cech, język ekonomii, sposoby pozyskiwania danych źródłowych, kategorie ekonomiczne, modelowanie<br>Charakterystyka współczesnych kierunków rozwoju ekonomii (rys historyczny)<br>Analiza procesu badawczego w ekonomii (przedmiot badań ekonomii, schemat tworzenia wiedzy, metody badawcze)<br>Charakterystyka podmiotów ekonomicznych.<br>Treści programowe:<br>Kierunki rozwoju ekonomii jako nauki<br>Proces badawczy w ekonomii – proces wnioskowania w ekonomii, metody badawcze w ekonomii, wyjaśnianie i prognozowanie w ekonomii<br>Osobliwości ekonomii<br>Wewnętrzny podział ekonomii, subdyscypliny ekonomiczne<br>Ekonomia głównego nurtu i poza głównym nurtem<br>Teorie ludnościowe<br>Problem ubóstwa i wykluczenia zawodowego oraz problem aktywności zawodowej i bezrobocia<br>Wzrost i rozwój gospodarczy<br>Inflacja i deflacja |

## 2. KSZTAŁCENIE KIERUNKOWE

| | | |
|---|---|---|
| | | |
| **Kierunkowe efekty uczenia się** | **Wstęp do nauki o państwie i prawie** | **ECTS: 5** |
| CYB_WG02<br>CYB_WG04<br>CYB_WK01 | Pojęcie państwa. Geneza państwa. Typologiczna charakterystyka państwa. Państwo jako organizacja społeczna. Władza publiczna. Terytorium. Ludność. Pojęcie narodu i społeczeństwa. Państwo jako organizacja polityczna, hierarchiczna. Państwo jako organizacja suwerenna. Przymusowy charakter państwa. Aparat państwowy. Zasady ustroju państwa. Suwerenność państwa. Forma państwa a forma rządów. Funkcje państwa. Struktura prawna państwa. Reżim polityczny. System wyborczy. Pojęcie i funkcje prawa. Źródła prawa. Prawo jako zjawisko polityczne. System prawa i jego tworzenie. Obowiązywanie prawa. | |
| | | |
| | | |
| **Kierunkowe efekty uczenia się** | **Wprowadzenie do nauk o bezpieczeństwie** | **ECTS: 3** |
| CYB_WG02<br>CYB_WG03<br>CYB_WG06<br>CYB_WK01 | Przedmiot obejmuje teorię bezpieczeństwa narodowego, wieloaspektowości jego uwarunkowań oraz sektorów i kryteriów jego rozróżniania. Zawiera w sobie zagadnienia pozwalające rozpoznawać i identyfikować szanse, wyzwania i zagrożenia dla bezpieczeństwa narodowego oraz identyfikować sposoby mające na celu jego zapewnianie.<br>Treści kształceniaTerminologia nauk o bezpieczeństwie<br>Bezpieczeństwo jako potrzeba, wartość i prawo człowieka oraz grup społecznych<br>Psychologiczne aspekty bezpieczeństwa<br>Szanse, wyzwania i zagrożenia bezpieczeństwa<br>Podmiotowy wymiar bezpieczeństwa<br>Przedmiotowy wymiar bezpieczeństwa<br>Bezpieczeństwo państwa<br>Subiektywny i obiektywny charakter bezpieczeństwa<br>Czynniki percepcji zagrożeń bezpieczeństwa<br>Człowiek wobec zagrożeń bezpieczeństwa<br>Tradycyjne i współczesne pojmowanie bezpieczeństwa<br>Poziomy analizy bezpieczeństwa<br>Sektory bezpieczeństwa politycznego, militarnego i ekonomicznego<br>Sektory bezpieczeństwa kulturowo-tożsamościowego, ekologicznego i powszechnego | |
| | | |
| **Kierunkowe efekty uczenia się** | **Problemy bezpieczeństwa społeczeństwa informacyjnego** | **ECTS: 3** |
| CYB_WG02<br>CYB_WG03<br>CYB_WG07<br>CYB_UW02<br>CYB_UO01<br>CYB_KK01 | Społeczeństwo informacyjne. Współczesne potrzeby komunikacji społecznej w zakresie ochrony informacji niejawnych. Komunikacja międzykulturowa w zakresie informacji niejawnych. Podstawy organizacji ochrony informacji niejawnych. Grupy społeczne a bezpieczeństwo osobowe – problemy bezpieczeństwa społeczeństwa informacyjnego. Komunikacja społeczna w zakresie bezpieczeństwa teleinformatycznego – problemy bezpieczeństwa społeczeństwa informacyjnego. Komunikacja społeczna w zakresie bezpieczeństwa przemysłowego – problemy bezpieczeństwa społeczeństwa informacyjnego. Organizacja współczesnej komunikacji społecznej -dezinformacja. | |

| | | |
|---|---|---|
| **Kierunkowe efekty uczenia się** | **Wstęp do cyberbezpieczeństwa** | **ECTS: 5** |
| CYB_WG07<br>CYB_WK01<br>CYB_WK03 | Informacja i społeczeństwo informacyjne. Wprowadzenie do problematyki sieci. Strategie cyberbezpieczeństwa. Cyberwojny - nowe formy konfliktów. Narzędzia konfliktu w cyberprzestrzeni. Zarządzanie bezpieczeństwem informacji. Przestępczość w cyberprzestrzeni. Kultura bezpieczeństwa w cyberprzestrzeni | |
| | | |
| **Kierunkowe efekty uczenia się** | **Międzynarodowe stosunki polityczne** | **ECTS: 3** |
| CYB_WG01<br>CYB_WG02<br>CYB_WG03<br>CYB_WK03 | Miejsce i znaczenie dyscypliny nauki o politycznych stosunkach międzynarodowych. Czynniki wpływające na strukturę środowiska międzynarodowego. Pojęcie i ewolucja społeczności międzynarodowej. Formy relacji międzynarodowych. Typy więzi międzynarodowych. Funkcje nauki o stosunkach międzynarodowych. Typy i klasyfikacja uczestników stosunków międzynarodowych Polityka zagraniczna i dyplomacja - znaczenie, funkcje, czynniki zewnętrzne i wewnętrzne wpływające na realizację polityki zagranicznej. Rola i cechy ambasad, konsulatów, misji. Dyplomatyczne i niedyplomatyczne formy realizacji celów politycznych. Patologiczne formy międzynarodowych stosunków politycznych. Terroryzm, wojny i konflikty. Typy, klasyfikacje i cechy. Pojęcie i istota współpracy regionalnej. Geneza, cechy i funkcje. Nowy i stary regionalizm. Globalne problemy polityczne. Typy, istota, cechy. Sposoby rozwiązywania problemów globalnych w środowisku międzynarodowym. Wielkie koncepcje prognostyczne -F. Fukuyamy koniec historii i S.Huntingtona zderzenie cywilizacji. Pojęcie kolonizacji i neokolonizacji. Cele i funkcje. Geneza, przebieg, kierunki kolonizacji. Wpływ na globalny układ sił. Proces i przebieg dekolonizacji.. Społeczne i polityczne konsekwencje. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Systemy i technologie w cyberbezpieczeństwie** | **ECTS: 4** |
| CYB_WG03<br>CYB_WG07<br>CYB_UW01<br>CYB_UW04<br>CYB_UO01 | Technologie bezpieczeństwa stosowane w systemach informatycznych instytucji publicznych i prywatnych.<br>Elementy analizy zagrożeń oraz interpretacji danych z systemów bezpieczeństwa (SIEM, IDS, IAM).<br>Treści programowe:<br>Systemy bezpieczeństwa IT: funkcje, klasyfikacja, zastosowanie<br>SIEM i IDS – jak działają i jak interpretować dane z tych systemów<br>Skanowanie podatności i analiza luk – narzędzia OpenVAS, Nessus<br>Zarządzanie tożsamością i kontrola dostępu – IAM, MFA, SSO<br>Bezpieczeństwo w środowiskach chmurowych i kontenerowych (Docker, Kubernetes – wprowadzenie)<br>Przykłady incydentów i reakcji na nie – podstawy zarządzania incydentami<br>Współpraca między menedżerami a zespołami IT – modele komunikacji i odpowiedzialności | |
| | | |
| **Kierunkowe efekty uczenia się** | **Polityka cyberbezpieczeństwa państwa** | **ECTS: 3** |
| CYB_WG07<br>CYB_WK01<br>CYB_WK03<br>CYB_UW02<br>CYB_UO01<br>CYB_KK01 | Pojęcie cyberbezpieczeństwa, cyberprzestępstwa państwa a pojęcie bezpieczeństwa państwa. Wprowadzenie do problematyki bezpieczeństwa w cyberprzestrzeni. Kluczowe pojęcia w tematyce cyberbezpieczeństwa. Dynamika zagrożeń cybernetycznych. Zagrożenia cybernetyczne i ich wpływ na krajowe i międzynarodowe systemy bezpieczeństwa wewnętrznego państwa. Wojna informacyjna, cyberwywiad. Bezpieczeństwo infrastruktury krytycznej - wymiar teleinformatyczny. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Zarządzanie w sytuacjach kryzysowych** | **ECTS: 4** |

| | | |
|---|---|---|
| CYB_WG02<br>CYB_WG07<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_UW04<br>CYB_UK02<br>CYB_UO01<br>CYB_KO02 | Pojęcie i istota „sytuacji kryzysowej" – wymiar ekonomiczny, społeczny, polityczny i kulturowy. Sytuacja kryzysowa w sektorze prywatnym i publicznym – kluczowe rozróżnienia w uwagi na cel i skalę działania. Uniwersalne zasady i metody strategii zarządzania kryzysowego a modele zarządzania. Pojęcie państwowej kultury strategicznej. Zarządzanie w sytuacjach kryzysowych – poziom koncepcyjny. Zarządzanie w sytuacjach kryzysowych – poziom operacyjny. Zarządzanie w sytuacjach kryzysowych – poziom techniczno-organizacyjny. StratCom a sytuacje kryzysowe. Wykorzystanie cyberprzestrzeni w sytuacjach kryzysowych – HR, PR. Narzędzia i techniki oddziaływania defensywnego i ofensywnego.<br>Uzupełnienie przedmiotu o treści analiza przebiegu incydentu od momentu wykrycia do zamknięcia, role i odpowiedzialności poszczególnych uczestników procesu, zasady podejmowania decyzji na kolejnych etapach zdarzenia, kryteria eskalacji, współpracę między SOC, administratorem, właścicielem biznesowym i kadrą kierowniczą, podstawy komunikacji kryzysowej, prowadzenie dokumentacji operacyjnej oraz ćwiczenia oparte na case studies i symulacjach | |
| | | |
| **Kierunkowe efekty uczenia się** | **Zarządzanie bezpieczeństwem informacji** | **ECTS: 3** |
| CYB_WG03<br>CYB_WG04<br>CYB_WG07<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_UW04<br>CYB_UU01<br>CYB_KK01<br>CYB_KR01 | Organizacja, standardy i normy zarządzania bezpieczeństwem informacji (organizacja Security Operation Center, zarządzanie a zarządzanie bezpieczeństwem informacji, stosowanie i wdrażanie normy ISO27001, budowanie wartości przedsiębiorstwa z wykorzystaniem IT) Zarządzanie projektami w bezpieczeństwie informacji (zarządzanie projektami w zarządzaniu bezpieczeństwem informacji) Wdrażanie rozwiązań zarządzania bezpieczeństwem informacji (motywowanie pracowników w warunkach zmian, zarządzanie incydentami, zarządzanie zmianami, wdrażanie rozwiązań z zakresu bezpieczeństwa informacji) Ryzyko w bezpieczeństwie informacji (zarządzanie ryzykiem w projektach IT, zarządzanie ryzykiem w bezpieczeństwie informacji na podstawie normy ISO 27005) Technologiczne aspekty w bezpieczeństwie informacji (bezpieczeństwo infrastruktury krytycznej, Cloud Computing a bezpieczeństwo informacji, podstawowe aspekty techniczne dotyczące zarządzania bezpieczeństwem informacji, informatyka śledcza, zarządzanie bezpieczeństwem sprzętowym i sieci, kryptografia i mechanizmy bezpieczeństwa) Dobre praktyki w bezpieczeństwie informacji – ludzie i technologia (Człowiek a infrastruktura IT, dobre praktyki w zarządzaniu bezpieczeństwem informacji, zaufanie w systemach informatycznych) Prawne uwarunkowania bezpieczeństwa informacji (ochrona danych osobowych wg RODO, prawne aspekty cyberbezpieczeństwa – ochrona informacji niejawnych, przestępczość zorganizowana zagrożeniem dla bezpieczeństwa informacji, czarny rynek w zarządzaniu bezpieczeństwem informacji) Nowe wyzwania i monitorowanie skuteczności w zarządzaniu bezpieczeństwem informacji (nowe wyzwania związane z bezpieczeństwem informacji, audyt wewnętrzny w zakresie bezpieczeństwa, Planowanie Ciągłości Działania (BCM), ROI w obszarze bezpieczeństwa). | |
| | | |
| **Kierunkowe efekty uczenia się** | **Struktury bezpieczeństwa państwa** | **ECTS: 3** |
| CYB_WG02<br>CYB_WG03<br>CYB_WK03 | Polityka bezpieczeństwa państwa – wymiary: wewnętrzny i zewnętrzny, zagadnienia teoretyczne, Bezpieczeństwo wewnętrzne państwa polskiego w wymiarze politycznym – struktury i procesy decyzyjne. Struktury w systemie bezpieczeństwa Polski (Policja, Straż Graniczna, Służba Ochrony Państwa, i inne służby stosujące przymus bezpośredni). Służby specjalne – Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Centralne Biuro Antykorupcyjne, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego. Zagrożenia bezpieczeństwa wewnętrznego Polski: zorganizowana przestępczość, korupcja i przestępstwa finansowe, cyberprzestępczość, nielegalna imigracja, i.in. Bezpieczeństwo Polski w wymiarze konstytucyjnym: stany nadzwyczajne w Polsce: klęski żywiołowej, wyjątkowy, wojenny. Polityka bezpieczeństwa Polski w wymiarze militarnym: siły zbrojne RP, siły specjalne, Narodowe siły rezerwowe, Wojska Obrony Terytorialnej. Istota misji i operacji Wojska Polskiego. Rola Polski we wspólnej polityce bezpieczeństwa i obrony Unii Europejskiej oraz w NATO | |
| | | |
| **Kierunkowe efekty uczenia się** | **Współczesny terroryzm polityczny** | **ECTS: 3** |

| | | |
|---|---|---|
| CYB_WG03<br>CYB_WG04<br>CYB_WG07<br>CYB_WK01 | Terroryzm współczesny – istota, zasadnicze rozróżnienia, klasyfikacje; Ewolucja i uwarunkowania działalności terrorystycznej (geopolityczne, ideologiczne, religijne, kulturowe); Psychologia terroryzmu – proces stawania się terrorystą i internalizacja terroryzmu; Psychologiczne aspekty terroryzmu samobójczego; Terroryzm w kontekście płci społecznej; Terroryzm etniczno-narodowy; Terroryzm społeczno – rewolucyjny; Terroryzm islamski; Terroryzm państwowy; Koncepcje przyszłości terroryzmu – poszukiwania nowego paradygmatu. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Praktyka zawodowa I (DW)** | **ECTS:28** |
| CYB_WG06<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_UW03<br>CYB_UO01<br>CYB_KK01<br>CYB_KO02<br>CYB_KR01 | **Praktyka w obszarze organizacji bezpieczeństwa informacji i cyberbezpieczeństwa**<br>Charakterystyka miejsca odbywania praktyki oraz zapoznanie się z profilem działalności organizacji, jej strukturą organizacyjną, podstawami prawnymi działania, warunkami pracy oraz zakresem zadań realizowanych w obszarze bezpieczeństwa informacji i cyberbezpieczeństwa. Poznanie zasad funkcjonowania komórek organizacyjnych odpowiedzialnych za bezpieczeństwo teleinformatyczne, ochronę informacji, zarządzanie dostępem, ochronę danych oraz ciągłość działania. Zapoznanie się z podstawową dokumentacją, procedurami i standardami bezpieczeństwa obowiązującymi w organizacji, w tym polityką bezpieczeństwa informacji, zasadami zarządzania incydentami, instrukcjami użytkowania systemów oraz procedurami ochrony danych. Udział w wybranych zadaniach związanych z identyfikowaniem zagrożeń, analizą ryzyka, oceną podatności organizacyjnych i technicznych oraz przygotowywaniem materiałów, zestawień, notatek lub raportów wspierających procesy decyzyjne. Obserwacja i analiza roli specjalisty do spraw cyberbezpieczeństwa w organizacji. Przygotowanie sprawozdania z praktyki, obejmującego opis zadań, wnioski oraz propozycje usprawnień w zakresie bezpieczeństwa informacji. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Praktyka zawodowa II (DW)** | **ECTS: 28** |
| CYB_WG05<br>CYB_WG06<br>CYB_WK01<br>CYB_UW01<br>CYB_UW02<br>CYB_UW03<br>CYB_UW04<br>CYB_UK02<br>CYB_UO01<br>CYB_KK01<br>CYB_KO01<br>CYB_KR01 | **Praktyka w obszarze analizy zagrożeń, incydentów i ryzyka cybernetycznego**<br><br>Zapoznanie się z działalnością organizacji w zakresie monitorowania zagrożeń, reagowania na incydenty, analizy ryzyka oraz ochrony systemów informacyjnych. Poznanie podstawowych procedur identyfikowania, klasyfikowania i dokumentowania incydentów bezpieczeństwa oraz zasad obiegu informacji w sytuacjach wymagających reakcji organizacyjnej lub technicznej. Udział w zadaniach pomocniczych związanych z analizą zagrożeń, analizą źródeł informacji, oceną ryzyka, przeglądem komunikatów bezpieczeństwa, monitorowaniem podatności oraz przygotowywaniem zestawień i raportów. Obserwacja sposobu współpracy między zespołami technicznymi, analitycznymi, prawnymi, administracyjnymi i menedżerskimi w sytuacjach zagrożenia. Poznanie znaczenia informacji, technologii cyfrowych i komunikacji cyfrowej w procesach bezpieczeństwa. Przygotowanie sprawozdania, notatki analitycznej lub prezentacji dotyczącej wybranego problemu zaobserwowanego podczas praktyki. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Praktyka zawodowa III (DW)** | **ECTS: 28** |
| CYB_WG04<br>CYB_WG06<br>CYB_WK02<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_UW04<br>CYB_UK01<br>CYB_UK02<br>CYB_UO01<br>CYB_KK01 | **Praktyka w obszarze ochrony danych, zgodności i regulacji cyberbezpieczeństwa**<br><br>Zapoznanie się ze strukturą organizacyjną i zakresem działania podmiotu przyjmującego na praktykę, ze szczególnym uwzględnieniem obszarów ochrony danych, bezpieczeństwa informacji, zgodności regulacyjnej i odpowiedzialnego korzystania z technologii cyfrowych. Poznanie podstawowych aktów wewnętrznych, procedur, regulaminów, polityk bezpieczeństwa, zasad ochrony danych osobowych, zasad zarządzania dostępem oraz standardów etycznych obowiązujących w organizacji. Udział w czynnościach pomocniczych związanych z analizą dokumentacji, oceną zgodności działań organizacji z procedurami, przygotowywaniem zestawień, notatek, projektów komunikatów, instrukcji lub materiałów informacyjnych. Poznanie zasad odpowiedzialnego korzystania ze źródeł informacji, ochrony własności intelektualnej, prawa autorskiego, poufności i bezpieczeństwa danych. Analiza wybranych problemów organizacyjnych, prawnych lub etycznych związanych z cyberbezpieczeństwem oraz przygotowanie propozycji | |

| | | |
|---|---|---|
| CYB_KO02<br>CYB_KR01 | działań usprawniających. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Praktyka zawodowa IV (DW)** | **ECTS: 28** |
| CYB_WG02<br>CYB_WG05<br>CYB_WK01<br>CYB_WK02<br>CYB_UW01<br>CYB_UW02<br>CYB_UK01<br>CYB_UK02<br>CYB_UO01<br>CYB_UU01<br>CYB_KK01<br>CYB_KO01<br>CYB_KO02<br>CYB_KR01 | **Praktyka w obszarze projektów, edukacji i komunikacji w cyberbezpieczeństwie**<br><br>Zapoznanie się z działalnością organizacji realizującej projekty, działania edukacyjne, komunikacyjne, szkoleniowe lub informacyjne dotyczące cyberbezpieczeństwa, bezpieczeństwa cyfrowego, ochrony danych, higieny cyfrowej albo odpowiedzialnego korzystania z technologii. Poznanie struktury organizacyjnej, zasad pracy zespołowej, sposobów planowania i realizacji projektów oraz form komunikacji z odbiorcami. Udział w przygotowywaniu materiałów edukacyjnych, informacyjnych, prezentacyjnych, promocyjnych lub szkoleniowych dotyczących zagrożeń cyfrowych, ochrony informacji, bezpieczeństwa użytkowników, dezinformacji, cyberhigieny lub odpowiedzialnego korzystania z nowych technologii. Współpraca przy organizacji wydarzeń, warsztatów, kampanii informacyjnych lub projektów społecznych. Analiza potrzeb odbiorców, przygotowanie prostych rekomendacji komunikacyjnych oraz ocena skuteczności wybranych działań. Przygotowanie sprawozdania z praktyki, zawierającego opis wykonanych zadań, ocenę zastosowanych narzędzi komunikacji oraz propozycje usprawnień. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Inżynieria informacji w przestrzeni publicznej** | **ECTS: 3** |
| CYB_WG03<br>CYB_WK01<br>CYB_WK03<br>CYB_UW02<br>CYB_UW04<br>CYB_KO02<br>CYB_KR01 | Teoria informacji i systemy informacyjne. Źródła danych i informacji. Metody pozyskiwania danych i informacji. Zasoby i infrastruktura systemów informacyjnych. Metody i technologie wyszukiwania informacji. Modelowanie danych i informacji. Metody wizualizacji danych i informacji. Metody ochrony danych i bezpieczeństwo teleinformatyczne. Metody walidacji i wyceny informacji . Analiza danych społecznych, biznesowych i osobowych. Informacja w zarządzaniu kryzysowym, bezpieczeństwie. Cyberbezpieczeństwo, wywiad, wywiad gospodarczy. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Wojna informacyjna i hybrydowa** | **ECTS: 3** |
| CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_UW04<br>CYB_KK01 | Zagrożenia asymetryczne, informacyjne i hybrydowe w teorii stosunków międzynarodowych oraz w nauce o bezpieczeństwie. Podmioty stosunków międzynarodowych stanowiące zagrożenie w bezpieczeństwie informacji. Procesy globalizacyjne i postęp technologiczny a konflikty zbrojne<br>Wojny hybrydowe. Terroryzm międzynarodowy i cyberterroryzm jako przykład zagrożenia asymetrycznego. Dezinformacja jako forma walki politycznej. Wymiar instytucjonalny i jej rola w stosunkach międzynarodowych. Współczesna wojna informacyjna/ wojna kognitywna a wojna „hybrydowa. Propaganda w mediach krajów niedemokratycznych i demokratycznych oraz mediów międzynarodowych. Nowe media a dezinformacja. Konflikt na Ukrainie jako przykład wojny informacyjnej. Konflikt na Bliskim Wschodzie jako przykład wojny informacyjnej. Medialny wizerunek przywódcy w Ameryce Łacińskiej - wybrane przykłady | |
| | | |
| **Kierunkowe efekty uczenia się** | **Geoinformacja i geolokalizacja** | **ECTS: 3** |
| CYB_WG07<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_UW04<br>CYB_KO02<br>CYB_KR01 | Podstawy systemów informacji przestrzennej. Geolokalizacja: systemy, odniesienia, dokładność. Globalne i lokalne ziemskie układy odniesienia, zasady transformacji między układami odniesienia, wysokościowe systemy i układy odniesienia i ich realizacje. Modelowanie kartograficzne i geowizualizacja. Algorytm – podstawowe pojęcia, algorytmy i struktury, pojęcie algorytmu, kryteria analizy algorytmów, poprawność. Oprogramowanie typu CAD - wykorzystanie, wymiana oraz wizualizacji informacji. Technologie pozyskiwania danych przestrzennych. Analizy przestrzenne w modelu wektorowym i rastrowym. Geokodowanie: definicja, dane referencyjne, proces geokodowania, charakterystyka ewentualnych błędów i możliwości ich poprawy, obszary zastosowań wyników geokodowania.. Teledetekcja z elementami cyfrowego przetwarzania sygnału. Modelowanie informacji urbanistycznej oraz procesu inwestycyjnego w technologii BIM. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Cyberkultura w XXI w.** | **ECTS: 3** |

| | | |
|---|---|---|
| CYB_WG03<br>CYB_WG06<br>CYB_WK03 | Wstęp do zagadnienia cyberkultury. Przedstawienie historycznego tła zjawiska. Wprowadzenie kluczowych pojęć i definicji. Przedstawienie i analiza pól funkcjonowania cyberkultury. związków kultury z technologią (cyberkultura a technokultura). Omówienie wyzwań jakie stanowi powstanie nowego zjawiska w postaci cyberkultury. Sztuka życia w cyberkulturze – jako konieczność znalezienia równowagi w czasach nadpodaży technologii i informacji. Teoretyczne omówienie idei społeczeństwa sieciowego. Przedstawienie miejsca sztuki w cyberprzestrzeni i cyberkulturze – metamedialne i postmedialne tendencje w cybersztuce. Nurty współczesnej sztuki mediów cyfrowych. Teoria i praktyka dokumentowania i prezentacji sztuki mediów cyfrowych. Omówienie roli archiwum w przestrzeni cyfrowej oraz sieciowych bibliotek, galerii i magazynów. Rola artystów w nowej rzeczywistości – ich nowe wyzwania i pola aktywności. Społeczne skutki zachodzących zmian. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Zarządzanie ryzykiem w polityce** | **ECTS: 3** |
| CYB_WG02<br>CYB_WG03<br>CYB_WK01<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_UK02<br>CYB_UO01<br>CYB_KO02<br>CYB_KR01 | Ryzyko w działalności politycznej, jego źródła i ogólna systematyka. Pojęcie i istota „sytuacji kryzysowej” – wymiar ekonomiczny, społeczny, polityczny i kulturowy. Uniwersalne zasady i metody strategii zarządzania kryzysowego. Cele i rodzaje zarządzania ryzykiem w polityce. Zarządzanie ryzykiem w polityce poprzez jego monitorowanie, eliminacje i ograniczanie. Identyfikacja zagrożeń. Analiza ryzyka i tworzenie mapy ryzyka. Źródła ryzyka w działalności politycznej. Korzystanie z informacji źródłowych w zarządzaniu ryzykiem w polityce. Komunikowanie w zarządzaniu ryzykiem w polityce. | |
| | | |
| | | |
| **Kierunkowe efekty uczenia się** | **Zarządzanie ryzykiem IT** | **ECTS: 3** |
| CYB_WG03<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_UW04<br>CYB_KO02<br>CYB_KR01 | Podstawowe pojęcia i definicje..Psychologia ryzyka. Czynniki osobowe w procesie zarządzania ryzykiem. Podstawowe przepisy i normy dotyczące zarządzania ryzykiem. Zarządzanie ryzykiem – proces i jego ewaluacja. Modele zarządzania ryzykiem. Analiza występowania ryzyka w procesach IT. Audyt bezpieczeństwa w procesach IT. Metody wpływu na ryzyko. Elementy bezpieczeństwa w procesie IT. | |
| **Kierunkowe efekty uczenia się** | **Zachowania przestępcze w cyberprzestrzeni** | **ECTS: 2** |
| CYB_WG02<br>CYB_WG04<br>CYB_WK01<br>CYB_UW01<br>CYB_UW02<br>CYB_UW04<br>CYB_UO01<br>CYB_KO02<br>CYB_KR01 | Definicje i typologie cyberprzestępstw (hacking, phishing, cyberstalking, grooming, DDoS, ransomware)<br>Cyberprzestępczość a przestępczość tradycyjna – punkty wspólne i różnice<br>Statystyki i trendy przestępczości cyfrowej w Polsce i na świecie<br>Krajowe ramy prawne (Kodeks karny, ustawa o zwalczaniu nieuczciwej konkurencji, RODO)<br>Międzynarodowe instrumenty prawne (Konwencja budapeszteńska, dyrektywy UE, prawo ONZ)<br>Organy ścigania i procedury dochodzeniowe w sprawach cyberprzestępstw<br>Motywacje sprawców cyberprzestępstw (np. zysk, ideologia, zaburzenia osobowości)<br>Społeczna percepcja przestępczości w sieci – zjawisko normalizacji<br>Cyberprzemoc i jej skutki społeczne – ofiary, świadkowie, społeczne milczenie<br>Dobre praktyki w ochronie przed cyberzagrożeniami (edukacja, zarządzanie hasłami, cyfrowa higiena)<br>Rola instytucji publicznych i organizacji pozarządowych w prewencji<br>Kampanie społeczne i edukacyjne<br>Studium przypadków: cyberataki na instytucje publiczne, oszustwa internetowe, sextortion | |
| | | |
| **Kierunkowe efekty uczenia się** | **Elementy kryptografii** | **ECTS: 3** |

| | | |
|---|---|---|
| CYB_WG04<br>CYB_WK03<br>CYB_UW01<br>CYB_UW04<br>CYB_UO01<br>CYB_KO02 | Wprowadzenie. Elementarne pojęcia.. Bezpieczeństwo systemów IT – ogólne pojęcia. Analiza i audyt bezpieczeństwa IT. Historia kryptografii.. Algorytmy szyfrowania symetrycznego.. Algorytmy szyfrowania asymetrycznego. Skrót – funkcje skrótu i ich rodzaje. Kryptonanaliza. Zastosowanie kryptografii w praktyce. Inne rodzaje zabezpieczeń. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Audyt bezpieczeństwa sieci teleinformatycznych** | **ECTS: 4** |
| CYB_WG07<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_UW04<br>CYB_UU01<br>CYB_KK01<br>CYB_KO02 | Wprowadzenie. Elementarne pojęcia. Informacja we współczesnym świecie. Przepisy prawne dotyczące informacji. Techniki i metody analizy informacji. Wybrane zagrożenia bezpieczeństwa sieciowego i ich charakterystyka. Inżynieria bezpieczeństwa, strategia oraz polityka bezpieczeństwa. Bezpieczeństwo fizyczne i środowiskowe. Środki, plany i procedury bezpieczeństwa IT. Zarządzanie bezpieczeństwem IT i ocena ryzyka. Audyt bezpieczeństwa sieci. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Metodyka przygotowania projektu** | **ECTS: 3** |
| CYB_WG04<br>CYB_WG07<br>CYB_WK02<br>CYB_UW04<br>CYB_UO01<br>CYB_UU01<br>CYB_KO02 | Projekt - istota, cele, fazy realizacji. Źródła możliwe do wykorzystania przy planowaniu i realizacji projektu. Sposoby dokumentowania wykorzystanych źródeł z poszanowaniem praw własności intelektualnej. Identyfikacja obszarów problemowych z zakresu finansów i rachunkowości mogących stanowić przedmiot projektu. Ustalanie tematu i celów projektu, grupy docelowej oraz przewidywanych skutków projektu. Ustalanie działań projektowych, ich harmonogramu, budżetu oraz ewentualnych źródeł finansowania. Szczegółowa koncepcja projektu - zasady opracowania. Źródła wiedzy o różnej wartości i wiarygodności naukowej. Przeszukiwanie baz danych. Zasady ochrony własności intelektualnej, rodzaje systemów cytowań i prawidłowa dokumentacja wykorzystanych źródeł. Identyfikacja ryzyk związanych z realizacją projektu oraz sposobów ich minimalizacji. Szczegółowe zaplanowanie poszczególnych działań projektowych. Sposoby dokumentowania działań projektowych Metody ewaluacji działań projektowych oraz całości projektu. Zasady modyfikacji założeń i działań projektowych w przypadku wystąpienia okoliczności uniemożliwiających ich realizację. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Cyberbezpieczeństwo w sektorze publicznym** | **ECTS: 3** |
| CYB_WG02<br>CYB_WG04<br>CYB_WK01<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_UW04<br>CYB_UK01<br>CYB_KO02 | Jednostki samorządu terytorialnego jako podmioty narażone na cyberataki; Ramy prawne cyberbezpieczeństwa w jednostkach samorządu terytorialnego; Najbardziej rozpowszechnione rodzaje cyberataków w JST; Przetwarzanie i ochrona danych osobowych w kontekście cyberbezpieczeństwa; Krajowy system cyberbezpieczeństwa. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Cyberbezpieczeństwo w organizacjach międzynarodowych** | **ECTS: 3** |
| CYB_WG02<br>CYB_WG03<br>CYB_WG04<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_UW04<br>CYB_UO01<br>CYB_KK01<br>CYB_KO02 | Polityka cyberbezpieczeństwa wybranych państw i organizacji międzynarodowych; Bezpieczeństwo w erze wielkich zbiorów danych przykładowe zagrożenia prawa do prywatności, prawo do bycia zapomnianym, oraz systemy algorytmicznej oceny obywatela; Cyberprzestrzeń jako wymiar rywalizacji oraz współpracy międzypaństwowej; Wywiad cybernetyczny, rywalizacja gospodarcza/wywiad gospodarczy; Cyberwojna i działalność w sferze nie-wojny a stosowalność prawa międzynarodowego w cyberprzestrzeni | |

| | | |
|---|---|---|
| **Kierunkowe efekty uczenia się** | **Przestępczość w sieci** | **ECTS: 3** |
| CYB_WG03<br>CYB_WG04<br>CYB_WG07<br>CYB_WK01<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_UO01<br>CYB_KK01<br>CYB_KO02 | Podstawowe pojęcia: informacja, dane komputerowe, program komputerowy, społeczeństwo informacyjne, cyberprzestrzeń, cyberprzestępstwo, klasyfikacja cyberprzestępstw; Składniki sieci: sprzęt komputerowy, medium sieciowe, urządzenie sieciowe, oprogramowanie komputerowe; Podział sieci komputerowych ze względu na zasięg oraz na sposób konfiguracji. Typologie sieciowe; Wąskopasmowe i szerokopasmowe technologie dostępowe; Modele sieci; Przesyłanie danych siecią. Protokoły sieciowe, adresy, routing, nazwy komputerów i adresy URL.; Usługi sieciowe. Sieci P2P; Złośliwe oprogramowanie; Podsłuch komputerowy; Łamanie haseł; Spoofing (ARP i DNS); Ataki odmowy usług (DoS, DDoS, DRDoS); Wykorzystanie luk i błędów w aplikacjach; Techniczne aspekty cyberprzestępczości: grooming, cyberstalking, phishing, pharming, drive-b-pharming; blue-jacking, blue-hacking, skimming, wymiana plików w sieci, metody anonimizacji (tor, serwery proxy, VPN); Międzynarodowe inicjatywy mające na celu zwalczanie przestępczości | |
| | | |
| **Kierunkowe efekty uczenia się** | **Bezpieczeństwo dzieci i młodzieży online** | **ECTS: 3** |
| CYB_WG02<br>CYB_WG03<br>CYB_WG04<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_UW04<br>CYB_KO02<br>CYB_KR01 | Internet w życiu młodych ludzi; Zagrożenia wobec dzieci i młodzieży online Cyberprzestępstwa; Międzynarodowe standardy ochrony dzieci online; Polskie standardy ochrony dzieci online; Podstawowe narzędzia zapewniające bezpieczeństwo dzieci online; Diagnoza bezpieczeństwa dziecka online; Sposoby reakcji na zaistniałe zagrożenie dziecka online; Specyfika mediów społecznościowych; Reklama i marketing skierowany do dzieci | |
| | | |
| **Kierunkowe efekty uczenia się** | **Ochrona danych osobowych: ujęcie krajowe i międzynarodowe** | **ECTS: 3** |
| CYB_WG02<br>CYB_WG07<br>CYB_WK02<br>CYB_WK03 | Wprowadzenie do problematyki prawa do prywatności oraz prawa ochrony danych osobowych; Regulacje międzynarodowe oraz wspólnotowe; Zakres podmiotowy i przedmiotowy stosowania ustawy o ochronie danych osobowych; Zasady przetwarzania danych osobowych; Dane osobowe w systemach informatycznych: numer telefonu, numer IP, login, Nick. adres poczty elektronicznej. Wykonywanie obowiązku informacyjnego usługodawców internetowych; Inteligentne urządzenia mobilne – analiza ryzyka naruszeń prywatności; Technologie komputerowe wykorzystywane do kradzieży danych; Standardy bezpiecznego przetwarzani danych osobowych w systemach teleinformatycznych; Odpowiedzialność za naruszenie danych osobowych i prywatności; Organy nadzorcze i ich zadania | |
| | | |
| **Kierunkowe efekty uczenia się** | **Ramy prawne białego i czarnego wywiadu** | **ECTS: 3** |
| CYB_WG04<br>CYB_WG06<br>CYB_WK01<br>CYB_WK03 | Wprowadzenie. Elementarne pojęcia. Informacja we współczesnym świecie. Przepisy prawne dotyczące informacji. Techniki i metody analizy informacji. Czarny i biały wywiad. Ochrona prawna własności przemysłowej. Prawo autorskie. Szpiegostwo gospodarcze. Informatyczne metody i środki ochrony zasobów informacyjnych jednostki organizacyjnej (podmiotu gospodarczego). Techniczne środki ochrony zasobów informacyjnych jednostki organizacyjnej (podmiotu gospodarczego). Znaczenie działalności wywiadowczej w przyszłości. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Zwalczanie dezinformacji w Internecie** | **ECTS: 3** |

| | | |
|---|---|---|
| CYB_WG02<br>CYB_WG04<br>CYB_WG07<br>CYB_WK02<br>CYB_WK03<br>CYB_UW01<br>CYB_UW04<br>CYB_UO01<br>CYB_KO02 | Wprowadzenie. Elementarne pojęcia. Informacja we współczesnym świecie.. Przepisy prawne dotyczące informacji.. Techniki i metody analizy informacji.. Czarny i biały wywiad. Ochrona prawna własności przemysłowej. Prawo autorskie. Szpiegostwo gospodarcze. Informatyczne metody i środki ochrony zasobów informacyjnych jednostki organizacyjnej (podmiotu gospodarczego). Techniczne środki ochrony zasobów informacyjnych jednostki organizacyjnej (podmiotu gospodarczego). Znaczenie działalności wywiadowczej w przyszłości. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Techniki eksploracji Internetu** | **ECTS: 3** |
| CYB_WG07<br>CYB_WK01<br>CYB_WK02<br>CYB_WK03<br>CYB_UW04<br>CYB_KO02 | Wprowadzenie. Elementarne pojęcia. Informacja we współczesnym świecie. Internet jako źródło informacji. Eksploracja danych masowych i hurtowni danych. Przeglądanie zasobów Internetu. Wyszukiwanie w sieci. Optymalizacja i przetwarzanie zapytań. Wprowadzanie do sieci semantycznych. Pozycjonowanie witryn internetowych. Systemy rekomendacyjne. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Bezpieczeństwo informacji w obrocie gospodarczym** | **ECTS: 3** |
| CYB_WG04<br>CYB_WK02<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_UW04<br>CYB_UO01<br>CYB_KO02 | Wprowadzenie. Elementarne pojęcia.. Bezpieczeństwo systemów IT – ogólne pojęcia.. Analiza i audyt bezpieczeństwa IT. Pojęcie i rodzaje obrotu gospodarczego. Znaczenie pojęć bezpieczeństwo i pewność obrotu. Instrumenty ochronne wynikające z ograniczeń swobody działalności gospodarczej.. Proces szacowania ryzyka w odniesieniu do bezpieczeństwa informacji.. Zarządzanie incydentami bezpieczeństwa informacji.. Zasady wykorzystania podpisu elektronicznego i elektronicznych instrumentów płatniczych w obrocie gospodarczym.. Gwarancje bezpieczeństwa obrotu instrumentami finansowymi.. Wymagania prawne (krajowe i międzynarodowe) dotyczące ochrony informacji. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Bezpieczeństwo informacji w administracji rządowej** | **ECTS: 3** |
| CYB_WG02<br>CYB_WG03<br>CYB_WG04<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_KK01<br>CYB_KO02 | Istota i geneza pojęcia informacja. Zakres pojęcia informacji, klasyfikacja i istota informacji. Koncepcja społeczeństwa informacyjnego. Kategorie społeczeństwa informacyjnego. Zagrożenie bezpieczeństwa informacyjnego. Informacja i dezinformacja jako instrumenty konfrontacji informacyjnej. Ochrona informacji i bezpieczeństwa informacyjnego. Zakres pojęciowy. Pojmowanie bezpieczeństwa informacyjnego. Zarządzanie ryzykiem w bezpieczeństwie informacyjnym. Zarządzanie potencjałem informacyjnym. Wyzwania dla bezpieczeństwa informacyjnego. Bezpieczeństwo informacyjne i bezpieczeństwo informacji. Ochrona informacji i obiektów w sieciach teleinformacyjnych. Modele ochrony informacji. Przetwarzanie informacji. Zapewnienie informacyjnej ciągłości działania. Analiza ryzyka i identyfikacja zagrożeń. Informacyjny aspekt bezpieczeństwa. Przestrzeń informacyjna jako płaszczyzna komunikacji. Bezpieczeństwo społeczeństw informacyjnych. Instrumenty prawne ochrony informacji. Administracja rządowa wobec potrzeby zapewnienia bezpieczeństwa informacji. Zarządzanie kryzysowe. Ochrona danych osobowych. Ochrona informacji niejawnych. Wymogi prawa unijnego. Wizja europejskiego społeczeństwa europejskiego. Obrót wiedzy w społeczeństwie informacyjnym. Radiofonia i telewizja jako elementy społeczeństwa informacyjnego. Internet a bezpieczeństwo informacji. Walka informacyjna i jej elementy. Uczestnicy walki informacyjnej. Narzędzia walki informacyjnej. Sfera materialna walki informacyjnej. Sfera duchowa (psychologiczna) walki informacyjnej. Kontrola społeczeństwa. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Projekt społeczny** | **ECTS: 5** |

| | | |
|---|---|---|
| CYB_WG03<br>CYB_WG04<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_UW04<br>CYB_KK01<br>CYB_KO02 | Techniki, narzędzia i etapy przygotowania projektu. Omówienie merytoryczne indywidualnych projektów studentów. Raport z realizacji działań projektowych. Raport końcowy z realizacji projektu - zasady, wymagania, sposób przygotowania, zakres treści. Prezentacja przebiegu i wyników projektu - jako przykład wystąpienia publicznego. Zasady wystąpień publicznych. Prezentacja multimedialna - jako narzędzie pomocnicze w wystąpieniu publicznym. Zasady prawidłowego przygotowania prezentacji multimedialnych. Cechy dobrych prezentacji i najczęstsze błędy w prezentacjach multimedialnych. Analiza przykładowych prezentacji. Omówienie merytoryczne indywidualnych projektów studentów. Omówienie merytoryczne raportów końcowych indywidualnych projektów studentów. Omówienie merytoryczne prezentacji multimedialnych poszczególnych studentów. Ćwiczenia w ustnym omawianiu swojego projektu z jednoczesnym wykorzystaniem prezentacji multimedialnej - na forum grupy. Bezpośrednie przygotowanie do egzaminu dyplomowego - omówienie jego przebiegu i zasad | |
| | | |
| **Kierunkowe efekty uczenia się** | **Bezpieczeństwo metropolii i społeczności lokalnych** | **ECTS: 5** |
| CYB_WG03<br>CYB_WG04<br>CYB_WK01<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_KO02<br>CYB_KR01 | Zapoznanie z podstawowymi pojęciami w zakresie bezpieczeństwa metropolii i społeczności lokalnych. Aktualna polityka państwa w zakresie bezpieczeństwa społeczności lokalnych. Zadania samorządu w kontekście bezpieczeństwa społeczności lokalnych. Zagrożenia dla bezpieczeństwa metropolii i społeczności lokalnych Lokalny system wsparcia dla ofiar przemocy . Współdziałanie obywateli z organami ścigania w środowisku lokalnych. Współpraca instytucji bezpieczeństwa publicznego z władzami lokalnymi. System nadzoru. | |
| | | |
| **3. KSZTAŁCENIE INFORMATYCZNE** | | |
| | | |
| **Kierunkowe efekty uczenia się** | **Wstęp do programowania** | **ECTS: 5** |
| CYB_WG07<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_KK01 | Przedstawienie roli programisty we współczesnych projektach informatycznych. Omówienie typowych obowiązków, a także przedstawienie kluczowych kompetencji, jakie programista powinien posiąść w celu osiągnięcia sukcesu zawodowego; Rodzaje paradygmatów programowania ze szczególnym uwzględnieniem programowania obiektowego; Metody uruchamiania aplikacji w języku Java - kompilacja i uruchamianie w konsoli, zastosowanie środowiska programistycznego, kompilacja w środowiskach internetowych; Podstawowe pojęcia programistyczne: zmienne, stałe, typy danych, funkcje, instrukcje proste i złożone, moduły, typy wyliczeniowe, tablice; Programowanie obiektowe. Pojęcie klasy i obiektu. Konstruktory. Modyfikatory dostępu. Dziedziczenie. Typy referencyjne a typy wartości (prymitywne). Polimorfizm. Enkapsulacja. Tworzenie klas JavaBeans; Zaawansowane programowanie obiektowe. Interfejsy i klasy abstrakcyjne. Konstrukcje statyczne. Słowa kluczowe this i super. Przeciążanie a przesłanianie metod. Klasy finalne; Kolekcje jako kluczowe struktury danych w Javie. Listy, zbiory, słowniki. Kolekcje sortowane. Metody hashCode() i equals().; Klasy strumieni na przykładzie obsługi systemu plików z wykorzystaniem elementów przestrzeni nazw java.io.; Tworzenie prostych aplikacji z interfejsem graficznym na przykładzie technologii JavaFX. | |
| | | |
| **Kierunkowe efekty uczenia się** | **Architektura systemów komputerowych** | **ECTS: 5** |
| CYB_WG07<br>CYB_WK03<br>CYB_UW01<br>CYB_UO01<br>CYB_KO02 | Wprowadzenie do architektury systemów komputerowych: pojęcia organizacji i architektury komputerów, ich struktura, działanie oraz rozwój. Systemy liczbowe (binarny, ósemkowy, szesnastkowy), konwersje liczb całkowitych i ułamkowych, arytmetyka binarna, liczby zmiennoprzecinkowe i standard IEEE-754, kodowanie znaków oraz kod BCD. Podstawy układów cyfrowych: zmienne i operacje logiczne, algebra Boole'a, prawa de Morgana, funkcje i ich minimalizacja, tablice prawdy, mapy Karnaugha, układy kombinacyjne i sekwencyjne, w tym przerzutniki, rejestry, liczniki i układy programowalne. Architektura komputera typu von Neumana, podstawowe cechy mikroprocesorów, formaty rozkazów, tryby adresowania, rejestry, operacje arytmetyczne, logiczne i przesunięć, skoki, makra, procedury, przerwania oraz obsługa wejścia-wyjścia w środowisku MASM32. Typy i hierarchia pamięci, pamięć podręczna, RAM, ROM, DMA oraz architektury CISC i RISC, systemy równoległe, klasyfikacja Flynna i komputery wektorowe. Weryfikacja działania układów i realizacja prostych zadań programistycznych z użyciem symulatorów oraz assemblera. | |
| | | |

| Kierunkowe efekty uczenia się | Technologie sieciowe | ECTS: 4 |
|---|---|---|
| CYB_WG07<br>CYB_WK03<br>CYB_UW01<br>CYB_UW02<br>CYB_KK01 | Wprowadzenie do tematyki sieci komputerowych..Ewolucja sieci komputerowych. Praca w intresieci (internetworking). Adresacja IP. Modele warstwowe protokołów sieciowych: 7-warstwowy model ISO, model TCP/IP . Protokół IP. Budowa nagłówka datagramu IP. Rola warstwy łączy danych. Budowa ramki ethernetowej. Problem odwzorowania adresów. Protokół ARP. Sieci dostępowe. Zasady routing w sieciach TCP/IP. Budowa tablicy routingu. Dodawanie tras statycznych do tabeli routingu. Trasa domyślna. Protokoły routingu dynamicznego. Protokół RIP. Zasady tworzenia tabel routingu w RIP. Konfiguracja protokołu RIP. Protokół OSPF. Komunikaty ICMP. Typy i kody komunikatów ICMP. Wykorzystanie ICMP w diagnostyce sieci. Narzędzie ping.. Sieci szerokopasmowe Sieci dostępowe. Technologie sieci dostępowych . Rola warstwy transportowej. Przesyłanie danych niezawodnymi strumieniami – protokół TCP. Protokół UDP. Rola warstwy aplikacji Usługa sieciowa DNS. Struktura nazw domenowych. Rekordy zasobów. Format komunikatów DNS. Sieciowe programy użytkowe :sftp, ssh, nfs. Cechy protokołu IPv6. Format nagłówka<br>IPv6. Analiza składniowa datagramu IPv6 | |
| | | |
| **Kierunkowe efekty uczenia się** | **Systemy operacyjne** | **ECTS: 4** |
| CYB_WG01<br>CYB_WG07<br>CYB_WK03<br>CYB_UW02<br>CYB_UK02<br>CYB_KO02 | Procesy i wątki: pojęcie procesu, stany procesu, struktura i atrybuty procesu. Powoływanie nowych procesów, wykorzystanie funkcji fork i exec. Pojęcie wątku. Operacje na wątkach s. Synchronizowanie procesów: problem sekcji krytycznej, mechanizmy synchronizacji, klasyczne problemy synchronizacji, semafory, sygnały, zamki, zmienne warunkowe. Komunikacja międzyprocesowa: pamięć dzielona, kolejki komunikatów, potoki, kolejki fifo Planowanie przydziału procesora: algorytmy planowania, ocena algorytmów, przykłady implementacji. Zakleszczenia: model systemu, charakterystyka zakleszczenia, sposoby postępowania z zakleszczeniami. Zarządzanie pamięcią: logiczna i fizyczna przestrzeń adresowa, wiązanie adresów, mechanizm wymiany, przydział obszarów pamięci głównej, stronicowanie, segmentacja. Pamięć wirtualna, błąd strony, zastępowanie stron, algorytmy zastępowania, szamotanie, model zbioru roboczego Zarządzanie pamięcią pomocniczą: pliki, metody dostępu do plików, katalogi, implementacje systemów plików, metody przydziału miejsca na dysku, zarządzanie obszarami wolnymi, pamięć podręczna, planowanie dostępu do dysku. Ochrona i bezpieczeństwo: uwierzytelnienie i kontrola dostępu. Konfigurowanie systemu, podstawowe polecenia, system pomocy Polecenia operowania systemem plików. Prawa dostępu. Sterowanie procesami, przekierowanie strumieni, potoki. | |

## Stosowane metody dydaktyczne oraz sposoby weryfikacji i oceny efektów uczenia się osiągniętych przez studenta w trakcie całego cyklu kształcenia

Treści programowe na kierunku *cyberbezpieczeństwo,* studia pierwszego stopnia o profilu praktycznym, zostały dobrane w sposób zapewniający realizację zakładanych efektów uczenia się w odniesieniu do wiedzy, umiejętności oraz kompetencji społecznych. Ich osiągnięcie jest zapewniane poprzez odpowiednio dobrane metody dydaktyczne. Weryfikacja realizacji efektów uczenia się odbywa się za pomocą metod odpowiednio dobranych do ich specyfiki, a także specyfiki przedmiotu, formy jego realizacji oraz możliwości ich weryfikacji.

W celu osiągnięcia zakładanych efektów uczenia się na kierunku *cyberbezpieczeństwo* są stosowane przede wszystkim następujące formy prowadzenia zajęć dydaktycznych: wykłady, ćwiczenia, warsztaty, laboratoria, konwersatoria oraz konsultacje.

Wykłady wykorzystują metody podawcze i są ukierunkowane na tworzenie zasobów wiedzy studiujących przy jednoczesnym zachęcaniu ich do dyskusji. Stosowane są także metody interaktywne i pomoce wizualne podnoszące efektywność procesu kształcenia.

Ćwiczenia, warsztaty czy laboratoria koncentrują się przede wszystkim na budowaniu umiejętności i kompetencji społecznych poprzez rozwiązywanie zadań, przykładów, studiów przypadku, interakcję z wykładowcą i pozostałymi studentami. Te formy zajęć mają na celu osiąganie efektów uczenia się przez doświadczanie rzeczywistości gospodarczej w sali ćwiczeniowej lub laboratorium komputerowym.

Konwersatoria wymagają zarówno elementów wykładowych, jak i ćwiczeń. W szczególności, istotnym elementem konwersatoriów są dyskusje pomiędzy prowadzącym zajęcia i studentami oraz pomiędzy studentami w odniesieniu prezentowanych treści kształcenia oraz prezentacji wyników badań z jednoczesną interpretacją teoretyczną oraz nastawieniem na ich wykorzystanie w praktyce. Służą temu zwłaszcza dyskusje skoncentrowane na studiach przypadków i innych materiałach źródłowych, z którymi studiujący zapoznają się w trakcie zajęć lub w ramach pracy własnej, studiując literaturę przedmiotu. Przygotowanie studentów do zajęć pozwala na skonfrontowanie opinii i wiedzy teoretycznej z dyskutowanym problemem. Zagadnienie, którego dotyczy dyskusja wzbogacana jest przez wykorzystywanie debat.

Konsultacje uzupełniają metody dydaktyczne, pozwalając na rozwinięcie wiedzy, umiejętności i kompetencji społecznych poprzez pracę własną studenta i interakcję z prowadzącym zajęcia oraz członkami grupy zajęciowej.

Część efektów uczenia się jest realizowana poprzez zastosowanie kilku metod dydaktycznych. Prowadzący przedmiot dokonuje wyboru optymalnej kombinacji metod kształcenia z uwzględnieniem formy zajęć, treści programowych oraz specyfiki efektów uczenia się, których osiągnięcie powinno zostać zapewnione. Dla każdej z zaprojektowanych form zajęć (wykład, ćwiczenia, warsztaty, laboratoria, konwersatoria, konsultacje), w odniesieniu do poszczególnych przedmiotów stosuje się następujący katalog metod kształcenia (Tabela 1).

**Tabela 1. Metody kształcenia z podziałem na formy prowadzenia zajęć**

| **Wykłady** | **Ćwiczenia, Warsztaty, Laboratoria** | **Konwersatoria** | **Konsultacje** |
|---|---|---|---|
| **Metody podające:** | **Metody aktywizujące:** | **Metody dialogowe i problemowe:** | **Metody indywidualne i wspierające:** |
| Wykład klasyczny<br>Wykład problemowy<br>Wykład z prezentacją multimedialną<br>Wykład interaktywny | Rozwiązywanie problemów (zadań, przykładów) - indywidualnie lub w zespole zadaniowym<br>Analiza studiów przypadku<br>Dyskusja moderowana<br>Burza mózgów<br>Symulacje<br>Praca w grupach | Dyskusja panelowa<br>Debata<br>Analiza literatury i tekstów źródłowych,<br>Krytyczna ocena i formułowanie opinii<br>Wspólne wypracowanie rozwiązań poprzez wymianę doświadczeń<br>Wykład interaktywny | Konsultacje problemowe<br>Konsultowanie prac indywidualnych<br>Mentoring, mentoring online<br>Wskazywanie dodatkowych materiałów do samodzielnej nauki |

Weryfikacja i ocena osiągnięcia efektów uczenia się jest przeprowadzana w ramach zajęć w oparciu o zadania i metody weryfikacji określone w sylabusach. Zróżnicowanie sposobów weryfikacji w ramach zajęć, w tym realizowanych z wykorzystaniem metod i technik kształcenia na odległość, jak i całego programu pozwala na całościowe monitorowanie procesu zdobywania wiedzy, umiejętności i kompetencji społecznych przez studentów. Do weryfikacji i oceny efektów uczenia się są stosowane przede wszystkim w zakresie:

- wiedzy – egzaminy pisemne, w tym testy, egzaminy ustne oraz kolokwia pisemne i ustne, a także prace pisemne;
- umiejętności – prace pisemne indywidualne i grupowe, projekty, studia przypadku oraz prezentacje;
- kompetencji społecznych – prezentacje, studium przypadku i zadania wykonywane w czasie lub poza zajęciami oraz obserwacja (np. aktywności studentów w czasie zajęć).

W uczelni obowiązuje zasada, iż weryfikacja efektów uczenia się na zajęciach prowadzonych w formie wykładów jest dokonywana w drodze egzaminu końcowego na ocenę (w czasie sesji egzaminacyjnej), a pozostałe formy zajęć pozwalają zarówno na bieżącą weryfikację efektów uczenia się w trakcie trwania semestru, jak też na koniec semestru i kończą się wystawieniem zaliczenia na ocenę. W przypadku studentów z niepełnosprawnościami, w zależności od ich indywidualnych potrzeb, są ustalane alternatywne metody weryfikacji efektów uczenia się, które uwzględniają indywidualne potrzeby tych osób.

Tabela 2 przedstawia katalog stosowanych sposobów weryfikacji efektów uczenia się w odniesieniu do formy prowadzonych zajęć dydaktycznych, który może zostać poszerzony jako efekt wdrażania działań projakościowych i korygujących.

| Tabela 2. Sposoby weryfikacji osiągnięcia efektów uczenia się z podziałem na kategorie efektów uczenia się i formy prowadzenia zajęć | | | |
|---|---|---|---|
| **Formy prowadzenia zajęć** | **Kategorie efektów uczenia się** | | |
| | **Wiedza** | **Umiejętności** | **Kompetencje społeczne** |
| **Wykłady** | Test wiedzy (*otwarty, zamknięty – jednokrotnego, wielokrotnego wyboru, pytania typu prawda/fałsz, dopasowanie itp*.)<br>Odpowiedź pisemna na pytania otwarte<br>Odpowiedź ustna – egzamin ustny | | |
| **Ćwiczenia**<br>**Laboratoria**<br>**Warsztaty** | Kolokwium pisemne<br>Kolokwium ustne | Aktywność na zajęciach (*punkty przyznawane za aktywność na zajęciach - dla najbardziej aktywnych, wyróżniających się jakością udzielanych odpowiedzi lub ocena poziomu samodzielnie wykonywanych zadań podczas zajęć wg zdefiniowanych kryteriów*)<br>Praca pisemna (*opinia, raport, ekspertyza, esej itp.*)<br>Projekt (*pisemny wraz z prezentacją lub bez prezentacji*)<br>Referat (*z prezentacją lub bez prezentacji*)<br>Dyskusja, debata (*punkty przyznawane za udział w dyskusji lub debacie; ocena jakości wypowiadanych argumentów wg przyjętych kryteriów)*<br>Praca w grupach (*punkty przyznawane za wykonanie zadania w grupach podczas zajęć wg ustalonych kryteriów*)<br>Krytyczna analiza tekstu<br>Analiza studium przypadku i/lub opracowanie studium przypadku (*indywidualnie lub zespołowo, na zajęciach i/lub poza zajęciami*)<br>Rozwiązywanie zadań i przykładów w czasie zajęć | |
| **Konwersatoria** | Kolokwium pisemne w formie testu zamkniętego lub z pytaniami otwartymi<br>Wypowiedź pisemna na zadany temat<br>Odpowiedź ustna – zaliczenie ustne | Aktywność na zajęciach (*punkty przyznawane za aktywność na zajęciach - dla najbardziej aktywnych, wyróżniających się jakością udzielanych odpowiedzi lub ocena poziomu samodzielnie wykonywanych zadań podczas zajęć wg zdefiniowanych kryteriów*)<br>Praca pisemna (*opinia, raport, ekspertyza, esej itp.*)<br>Projekt (*pisemny wraz z prezentacją lub bez prezentacji*)<br>Referat (*z prezentacją lub bez prezentacji*)<br>Dyskusja, debata (*punkty przyznawane za udział w dyskusji lub debacie; ocena jakości wypowiadanych argumentów wg przyjętych kryteriów)*<br>Praca w grupach (*punkty przyznawane za wykonanie zadania w grupach podczas zajęć wg ustalonych kryteriów*)<br>Krytyczna analiza tekstu<br>Analiza studium przypadku i/lub opracowanie studium przypadku (*indywidualnie lub zespołowo, na zajęciach i/lub poza zajęciami*)<br>Rozwiązywanie zadań i przykładów w czasie zajęć | |

Przy weryfikacji efektów uczenia się przyjmuje się założenie, że uzyskanie pozytywnej oceny z egzaminu lub zaliczenia kończącego przedmiot oraz egzaminu dyplomowego potwierdza osiągnięcie wszystkich efektów

uczenia się ustalonych dla elementów procesu uczenia się. Poziom uzyskania efektów uczenia się wynika z wystawionej oceny. Przy zaliczeniach i egzaminach stosuje się następującą skalę ocen: celujący (6,0), bardzo dobry (5), dobry plus (4,5), dobry (4), dostateczny plus (3,5), dostateczny (3), niedostateczny (2). Egzamin dyplomowy jest oceniany z zastosowaniem tej samej skali ocen. W przypadku zajęć kończących się zaliczeniem bez oceny stosuje się zapis: niezaliczony (nzal), zaliczony (zal).

Tabela 3 przedstawia skalę ocen stosowaną w uczelni, odzwierciedlającą stopień osiągnięcia efektów uczenia się.

**Tabela 3. Kryteria oceny w procesie weryfikacji efektów uczenia się**

| Ocena | Opis wymagań | Wymagany procent osiągniętych efektów uczenia się dla przedmiotu |
|---|---|---|
| celujący (6,0) | Zakładane efekty uczenia się zostały osiągnięte w pełni i w bardzo zaawansowanym stopniu. Dodatkowo osoba studiująca opanowała treści kształcenia wykraczające poza zakres przewidziany w sylabusie przedmiotu, samodzielnie określa i rozwiązuje problemy, proponuje twórcze i oryginalne rozwiązania problemów, potrafi wykorzystać wiedzę w nowych sytuacjach, poprawnie i swobodnie posługuje się terminologią, samodzielnie i twórczo rozwija własne uzdolnienia. | 96-100% |
| bardzo dobry (5,0) | Zakładane efekty uczenia się zostały osiągnięte w zaawansowanym stopniu. Osoba studiująca osiągnęła bardzo wysoki poziom opanowania treści kształcenia, wykorzystywania wiedzy w nowych, nieznanych sytuacjach, rozwiązuje problemy teoretyczne i praktyczne na wysokim poziomie, poprawnie posługuje się terminologią. | 90-95% |
| dobry plus (4,5) | Zakładane efekty uczenia się zostały osiągnięte w stopniu więcej niż średnim, ale mniej niż zaawansowanym. | 85-89% |
| dobry (4,0) | Zakładane efekty uczenia się zostały osiągnięte w stopniu średnim. Osoba studiująca opanowała większość treści określonych programem kształcenia dla przedmiotu, rozwiązuje typowe zadania teoretyczne i praktyczne, ujmuje w terminach naukowych i zawodowych podstawowe pojęcia i prawa. | 70-84% |
| dostateczny plus (3,5) | Zakładane efekty uczenia się zostały osiągnięte w stopniu więcej niż podstawowym, ale w mniej niż średnim. | 65-69% |
| dostateczny (3,0) | Zakładane efekty uczenia się zostały osiągnięte w stopniu podstawowym. Osoba studiująca opanowała podstawowe wiadomości i umiejętności określone programem kształcenia dla przedmiotu, rozwiązuje typowe zadania teoretyczne i praktyczne o średnim stopniu trudności, popełnia niewielkie błędy terminologiczne, a wiadomości przekazuje językiem zbliżonym do potocznego. | 50-64% |
| niedostateczny (2.0) | Zakładane efekty uczenia się nie zostały osiągnięte. Osoba studiująca nie opanowała treści kształcenia, nie potrafi rozwiązać zadań o niewielkim stopniu trudności, popełnia rażące błędy terminologiczne, a styl jego wypowiedzi jest nieporadny. | mniej niż 50% |
| nzal – zakładane efekty uczenia się nie zostały osiągnięte<br>zal – zakładane efekty uczenia się zostały osiągnięte | | |

Metodą weryfikacji efektów uczenia się uzyskanych z całości cyklu kształcenia na poziomie studiów pierwszego stopnia jest **egzamin dyplomowy**. Jest on przeprowadzany po złożeniu przez osobę studiującą zaliczeń i egzaminów z wynikiem pozytywnym ze wszystkich zajęć przewidzianych w toku studiów oraz uzyskaniu co najmniej 180 punktów ECTS. Na studiach o profilu praktycznym egzamin dyplomowy obejmuje część teoretyczną, część praktyczną oraz prezentację projektu.

(1) w ramach części teoretycznej osoba studiująca odpowiada na pytanie wylosowane z puli pytań kierunkowych

(2) część praktyczna egzaminu dyplomowego ma charakter aplikacyjny i polega na analizie przypadków zdarzeń, czy rozwiązania problemów z zakresu kierunku studiów. W trakcie realizacji części praktycznej egzaminu weryfikacji podlegają również umiejętności i kompetencje społeczne osób studiujących, w szczególności: zdolność do komunikacji, podejmowania decyzji adekwatnych do sytuacji, odpowiedzialność za proponowane działania oraz świadomość ograniczeń własnych kompetencji.

(3) prezentacja wykonanego i zaliczonego w czasie VI semestru studiów projektu społecznego zawiera propozycję rozwiązania wybranego problemu społecznego z wykorzystaniem odpowiednich metod i narzędzi oraz wiedzy i umiejętności z zakresu studiów, a także udzielenie odpowiedzi na pytanie sformułowane przez komisję egzaminacyjną dotyczące przedstawionego projektu,

Z ustnego egzaminu dyplomowego sporządza się protokół, w którym są zapisywane pytania wylosowane i zadane osobie studiującej z obu części egzaminu, oceny za udzielone odpowiedzi, ocena ostateczna egzaminu dyplomowego oraz końcowy wynik studiów. Protokół jest podpisywany elektronicznie w systemie informatycznym uczelni przez wszystkich członków komisji, a jego wydruk jest archiwizowany w teczce osobowej osoby studiującej.

Absolwent studiów otrzymuje dyplom ukończenia studiów wyższych pierwszego stopnia na kierunku *cyberbezpieczeństwo* o profilu praktycznym, potwierdzający uzyskanie tytułu zawodowego licencjata.

## Zasady i forma odbywania praktyk zawodowych

Ogólne zasady organizacji praktyk zawodowych, wzory niezbędnych dokumentów, zadania opiekunów praktyk oraz tryb zaliczania praktyk określa uczelniany Regulamin Praktyk Zawodowych w Uniwersytecie VIZJA. Natomiast szczegółowe zasady realizacji praktyk na kierunku *cyberbezpieczeństwo*, w tym ich cel, efekty uczenia się, treści programowe, umiejscowienie w planie studiów, wymiar, metody weryfikacji efektów uczenia się, sposób dokumentowania przebiegu praktyk, kryteria dotyczące podmiotów przyjmujących na praktyki, zasady zatwierdzania miejsca praktyk oraz warunki kwalifikowania studenta na praktyki, określa Program Praktyk Zawodowych na kierunku *cyberbezpieczeństwo* zatwierdzony przez dziekana.

Uczelnia zapewnia miejsca praktyk i zawiera porozumienia z podmiotami przyjmującymi osoby studiujące na praktyki. Osoba studiująca może również samodzielnie wskazać miejsce odbywania praktyk, pod warunkiem jego wcześniejszego zatwierdzenia przez uczelnię poprzez wystawienie skierowania na praktyki. Dopuszczalne jest także zaliczenie praktyki na podstawie wykonywanej pracy zawodowej, udziału w programie ERASMUS+, działalności w studenckim kole naukowym, pracy wykonywanej w Uniwersytecie VIZJA lub działalności wolontariackiej, o ile forma ta umożliwia osiągnięcie wszystkich efektów uczenia się przewidzianych dla praktyk.

Praktyki zawodowe na kierunku *cyberbepieczeństwo* mają charakter obowiązkowy. Są realizowane:

- na trzecim semestrze (2 rok studiów) – Praktyka zawodowa w wymiarze 180 godz.,
- na czwartym semestrze (2 rok studiów) – Praktyka zawodowa w wymiarze 180 godz.,
- na piątym semestrze (3 rok studiów) – Praktyka zawodowa w wymiarze 180 godz.,
- na szóstym semestrze (3 rok studiów) – Praktyka zawodowa w wymiarze 180 godz.

Łączny wymiar praktyk wynosi **720 godzin**, za które student uzyskuje **28 punktów ECTS**. Osoba studiująca rozpoczyna realizację praktyk na trzecim semestrze, jednak w uzasadnionych przypadkach może wystąpić do dziekana z wnioskiem o wcześniejsze rozpoczęcie praktyki.
Celem praktyk zawodowych jest umożliwienie osobie studiującej weryfikacji dotychczas zdobytej wiedzy teoretycznej oraz nabycie praktycznych umiejętności jej wykorzystania w pracy w obszarze administracji. Praktyki służą także rozwijaniu umiejętności pracy w zespole,

kształtowaniu etyki zawodowej oraz przygotowaniu do wykonywania praktycznych czynności zawodowych.

Osoba studiująca wybiera miejsce praktyk zgodnie z profilem kierunku studiów. Treści programowe realizowane podczas praktyki powinny odpowiadać specyfice zadań wykonywanych w danej jednostce. W trakcie praktyki osoba studiująca poznaje zasady bezpieczeństwa i higieny pracy obowiązujące w placówce, cele i zadania realizowane przez organizację, jej strukturę organizacyjną, zakres obowiązków poszczególnych komórek i pracowników oraz stosowaną dokumentację, procedury, regulaminy, akty prawne, metodyki, programy komputerowe i inne narzędzia pracy.

Szczególne znaczenie ma poznanie metod i narzędzi charakterystycznych dla pracy w administracji oraz nabycie umiejętności ich praktycznego stosowania pod nadzorem zakładowego opiekuna praktyk. W zależności od specyfiki miejsca praktyk osoba studiująca może wykonywać zadania o charakterze:

- analitycznym – związane ze zbieraniem, weryfikowaniem i przetwarzaniem informacji oraz formułowaniem wniosków,
- prognostycznym – związane z przewidywaniem zdarzeń i procesów prawno-administracyjnych w obszarze cyberbezpieczeństwa
- rekrutacyjnym – związane z wykonywaniem zadań wymagających wykorzystania kompetencji administracyjnych w procesach rekrutacyjnych dla obszarów cyberbezpieczeństwa
- administracyjnym – związane z realizacją zadań prawno-administracyjnych właściwych dla danej jednostki wykonującej działania w obszarze cyberbezpieczeństwa
- opiniodawczym – polegające na sporządzaniu opinii na zlecenie podmiotu przyjmującego na praktykę.

Podczas praktyki osoba studiująca powinna zostać zapoznana z zasadami wykonywania obowiązków zawodowych, regułami współpracy z przełożonymi, współpracownikami i klientami, a także z kulturą organizacyjną instytucji. Powinna również poznać normy etyczne i przepisy prawne regulujące funkcjonowanie danej placówki oraz stopniowo uczestniczyć w jej bieżącej działalności. Dzięki temu rozwija umiejętność obserwowania i rozumienia środowiska pracy, zasad formalnych i nieformalnych oraz relacji interpersonalnych występujących w organizacji.

**Kryteria doboru miejsca praktyki i metody weryfikacji i oceny efektów uczenia się**

Praktyka zawodowa na kierunku *cyberbezpieczeństwo* może być realizowana w czterech profilach: organizacji bezpieczeństwa informacji i cyberbezpieczeństwa, analizy zagrożeń i ryzyka cybernetycznego, ochrony danych i zgodności regulacyjnej oraz projektów, edukacji i komunikacji w cyberbezpieczeństwie. Zróżnicowanie profili praktyk wynika z interdyscyplinarnego charakteru kierunku oraz z potrzeby umożliwienia osobom studiującym osiągania efektów uczenia się w różnych środowiskach zawodowych: technicznych, organizacyjnych, analitycznych, administracyjnych, prawno-regulacyjnych, edukacyjnych i projektowych. Każdy wariant praktyki umożliwia zastosowanie wiedzy i umiejętności w rzeczywistych warunkach pracy oraz rozwija odpowiedzialność, krytyczne podejście, współpracę zespołową i gotowość do etycznego pełnienia ról zawodowych w obszarze cyberbezpieczeństwa.

Praktyki zawodowe na kierunku *cyberbezpieczeństwo* umożliwiają realizacje następujących efektów uczenia się:

**Wiedza:** CYB_WG02, CYB_WG04, CYB_WG05, CYB_WG06, CYB_WK01, CYB_WK02, CYB_WK03

**Umiejętności:** CYB_UW01, CYB_UW02, CYB_UW03, CYB_UW04, CYB_UK01, CYB_UK02, CYB_UO01, CYB_UU01

Kompetencje społeczne: CYB_KK01, CYB_KO01, CYB_KO02 CYB_KR01

Zaproponowane efekty uczenia się dla praktyk zawodowych na kierunku *cyberbezpieczeństwo* uwzględniają założenia, iż osoba studiująca może realizować praktyki w:

- działach IT i cyberbezpieczeństwa przedsiębiorstw;
- zespołach bezpieczeństwa informacji;
- centrach monitorowania bezpieczeństwa i reagowania na incydenty;
- jednostkach administracji publicznej;
- instytucjach odpowiedzialnych za ochronę danych osobowych;
- działach compliance, audytu i zarządzania ryzykiem;
- bankach, instytucjach finansowych i ubezpieczeniowych;
- firmach technologicznych i informatycznych;
- firmach konsultingowych z obszaru bezpieczeństwa, IT, danych i zgodności;
- podmiotach infrastruktury krytycznej;
- centrach zarządzania kryzysowego;
- organizacjach pozarządowych prowadzących działania edukacyjne lub społeczne w zakresie bezpieczeństwa cyfrowego;
- instytucjach edukacyjnych i szkoleniowych;

- jednostkach prowadzących projekty z zakresu cyfryzacji, bezpieczeństwa informacji, przeciwdziałania dezinformacji i ochrony użytkowników technologii cyfrowych.

Weryfikacji osiągnięcia efektów uczenia się dokonuje każdorazowo zakładowy opiekun praktyk lub osoba bezpośrednio nadzorująca czynności wykonywane przez osobę studiującą. Osoba studiująca prowadzi na bieżąco *Dzienniczek praktyk*, w którym codziennie zapisuje wykonywane czynności i zadania oraz przyporządkowuje im odpowiednie kody efektów uczenia się. Do jednej czynności może być przypisany więcej niż jeden efekt uczenia się. Zakładowy opiekun praktyk nadzoruje poprawność tych przyporządkowań oraz potwierdza osiągnięcie albo nieosiągnięcie poszczególnych efektów poprzez wpisanie w dzienniczku odpowiednio: zal. lub nzal.

Zakładowy opiekun praktyk ma obowiązek powierzać osobie studiującej taki zakres zadań, który:

- jest zgodny z programem praktyk,
- odpowiada specyfice pracy w administracji w danym podmiocie,
- umożliwia osiągnięcie wszystkich efektów uczenia się przewidzianych dla praktyki.

Po zakończeniu praktyki zakładowy opiekun praktyk sporządza końcową opinię dotyczącą osoby studiującej i przebiegu praktyki.

Nadzór nad realizacją praktyk sprawuje również uczelniany opiekun praktyk, który analizuje zakres zrealizowanych zadań, odbywa z osobą studiującą rozmowę podsumowującą, sprawdza poprawność dokumentacji, liczbę zrealizowanych godzin, prawidłowość przypisania efektów uczenia się oraz ocenia, czy osoba studiująca osiągnęła wszystkie wymagane efekty. Analizuje także opinię końcową zakładowego opiekuna praktyk i w razie wątpliwości wyjaśnia je z osobą studiującą lub opiekunem zakładowym. Na tej podstawie podejmuje decyzję o zaliczeniu albo niezaliczeniu praktyki i wpisuje ją do protokołu. Następnie przekazuje dokumentację do **Biura Obsługi Studenta**

**Sposób dokumentowania przebiegu praktyk**

Do obowiązkowej dokumentacji praktyk należą:

- Skierowanie na praktyki,
- Porozumienie o przeprowadzenie praktyki studenckiej,
- *Dzienniczek praktyk*,
- Protokół zaliczenia praktyki.

Podstawowym dokumentem potwierdzającym przebieg praktyki jest *Dzienniczek praktyk*. Powinien on zawierać:

- datę rozpoczęcia i zakończenia praktyki,
- nazwę jednostki, w której student odbywa praktykę,
- dane zakładowego opiekuna praktyk,
- dane uczelnianego opiekuna praktyk,
- wykaz efektów uczenia się wraz z kodami,
- zakres powierzonych studentowi zadań i obowiązków,
- dzienny zapis wykonywanych czynności wraz z przypisanymi efektami uczenia się i potwierdzeniem ich realizacji,
- końcową opinię zakładowego opiekuna praktyk.

**Warunki kwalifikowania osoby studiującej na praktykę**

Osoba studiująca zgłasza się do uczelnianego opiekuna praktyk i wskazuje proponowane miejsce oraz termin realizacji praktyki. Uczelniany opiekun praktyk ocenia adekwatność tej propozycji na podstawie regulaminu praktyk i programu praktyk dla kierunku prawo, a następnie podejmuje decyzję o zakwalifikowaniu osoby studiującej na praktykę.

Osoba studiująca jest przyjmowana na praktykę na podstawie:

a) Porozumienia o przeprowadzenie praktyki zawodowej zawartego pomiędzy uczelnią a jednostką przyjmującą,

b) Indywidualnego skierowania na praktyki.

Oba dokumenty podpisuje w imieniu uczelni uczelniany opiekun praktyk, działający na podstawie pełnomocnictwa udzielonego przez Rektora.

Szczegółowe dokumenty dotyczące kryteriów, zasad realizacji i ewaluacji praktyk zawodowych dla kierunku *cyberbezpieczeństwo* są dostępne na stronie internetowej uczelni oraz w zarządzeniach dziekańskich dotyczących organizacji i hospitacji praktyk zawodowych.