Załącznik
do Uchwały nr …
Senatu MWSLiT we Wrocławiu
z dnia …

MIĘDZYNARODOWA WYŻSZA SZKOŁA LOGISTYKI I TRANSPORTU WE WROCŁAWIU

PROGRAM STUDIÓW

C Y B E R B E Z P I E C Z E Ń S T W O

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: 2353 godz.** **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 47,8%** **Nauki o bezpieczeństwie 30,6%** **Informatyka techniczna i telekomunikacja 21,7%**
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**Studia stacjonarne: 90,6 (50,3%)** **Studia niestacjonarne: 63,7 (35,4%)**
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć kształtujących umiejętności praktyczne	**100,7 pkt. ECTS (55,9%)**
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*** *W tym za zajęcia/grupy zajęć: Wprowadzenie do filozofii
Liczba punktów ECTS przyporządkowana zajęciom lub grupom zajęć do wyboru	**58 pkt. ECTS (32,2%)**
Wymiar praktyk zawodowych oraz liczba punktów ECTS, jaką student musi uzyskać w ramach tych praktyk	**6 miesięcy** **720 godz.** **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	24
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

4. Fakultatywne (nieobowiązkowe) moduły kształcenia ogólnego *				
Moduł I				
L.p.	**Nazwa zajęć**	**ECTS**	**Liczba godzin zajęć dydaktycznych ogółem**	
			Studia stacjonarne	**Studia niestacjonarne**
1.	Język obcy specjalistyczny I	**3**	30	16
2.	Kulturowe dziedzictwo Europy	**3**	30	16
3.	Praktyczna nauka języka (leksyka i czytanie) **(DW)**	**5**	60	32
4.	Praktyczna nauka języka (gramatyka praktyczna) **(DW)**	**5**	60	32
5.	Praktyczna nauka języka (konwersacje) **(DW)**	**5**	60	32
6.	Praktyczna nauka języka (pisanie i stylistyka) **(DW)**	**5**	60	32
7.	Praktyczna nauka języka (umiejętności zintegrowane) **(DW)**	**4**	30	16
	Razem	**30**	**330**	**176**
Moduł II				
L.p.	**Nazwa zajęć**	**ECTS**	**Liczba godzin zajęć dydaktycznych ogółem**	
			Studia stacjonarne	**Studia niestacjonarne**
1.	Język obcy specjalistyczny II	**3**	30	16
2.	Kulturowe dziedzictwo Polski	**3**	30	16
3.	Praktyczna nauka języka (leksyka i czytanie) **(DW)**	**5**	60	32
4.	Praktyczna nauka języka (gramatyka praktyczna) **(DW)**	**5**	60	32
5.	Praktyczna nauka języka (konwersacje) **(DW)**	**5**	60	32
6.	Praktyczna nauka języka (pisanie i stylistyka) **(DW)**	**5**	60	32
7.	Praktyczna nauka języka (umiejętności zintegrowane) **(DW)**	**4**	30	16
	Razem	**30**	**330**	**176**

***** Zajęcia kształcenia kulturowego i językowego, realizowane w ramach semestru lub roku wstępnego (tzw. *foundation programme*), przeznaczone w szczególności dla cudzoziemców lub osób o niewystarczających kompetencjach w zakresie języka, w którym realizowany jest program studiów.

5. Fakultatywne (nieobowiązkowe) zajęcia kształcenia dodatkowego – zajęcia swobodnego wyboru w j. angielskim**				
Semestr I				
L.p.	**Nazwa zajęć**	**ECTS**	**Liczba godzin zajęć dydaktycznych ogółem**	
			Studia stacjonarne	**Studia niestacjonarne**
1.	Przedmiot (-y) dodatkowe (fakultatywne) w liczbie od 1 do 3	**maks. 9**	maks. 90	---
Semestr II				
L.p.	**Nazwa zajęć**	**ECTS**	**Liczba godzin zajęć dydaktycznych ogółem**	
			Studia stacjonarne	**Studia niestacjonarne**
1.	Przedmiot (-y) dodatkowe (fakultatywne) w liczbie od 1 do 3	**maks. 9**	maks. 90	---
	Razem	**maks. 18**	**maks. 180**	**---**

** Fakultatywne (nieobowiązkowe) zajęcia dodatkowe swobodnego wyboru w j. angielskim są przeznaczone dla studentów I roku studiów stacjonarnych I stopnia lub jednolitych studiów magisterskich. Student może zrealizować od jednego do trzech przedmiotów w semestrze. Lista przedmiotów jest ogłaszana na początek roku akademickiego.

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	15	8	**1,3**
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**	**100,7**

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 stopniu zaawansowanym charakter, miejsce i rolę współczesnych dyscyplin nauk społecznych, w tym z zakresu nauk o bezpieczeństwie oraz nauk o polityce i administracji, zachodzące między nimi wzajemne zależności, a także ich zastosowania praktyczne.	P6U_W	P6S_WG
	CYB_WG02	Zna w zaawansowanym stopniu różne rodzaje struktur i instytucji społecznych (kulturowych, politycznych, prawnych, ekonomicznych) oraz ich istotne elementy, w tym związane z systemem bezpieczeństwa cyfrowego.	P6U_W	P6S_WG
	CYB_WG03	Posiada w stopniu zaawansowanym podstawową wiedzę o relacjach między strukturami oraz instytucjami społecznymi i politycznymi w skali krajowej, międzynarodowej i międzykulturowej.	P6U_W	P6S_WG
	CYB_WG04	Zna i rozumie w stopniu zaawansowanym rodzaje więzi społecznych oraz rządzące nimi prawidłowości, w tym znaczenie komunikacji za pomocą technologii cyfrowych.	P6U_W	P6S_WG
	CYB_WG05	Posiada w stopniu zaawansowanym wiedzę w wymiarze polskim, europejskim i światowym o państwie, władzy, polityce, administracji oraz prawie, także o zasadach funkcjonowania systemu politycznego.	P6U_W	P6S_WG
	CYB_WG06	Zna w zaawansowanym stopniu metody i narzędzia, w tym techniki pozyskiwania danych, pozwalające opisywać różnego rodzaju struktury oraz instytucje, a także procesy w nich i między nimi zachodzące.	P6U_W	P6S_WG
	CYB_WG07	Posiada zaawansowaną wiedzę o normach i regułach (prawnych, organizacyjnych, moralnych, etycznych) organizujących struktury i instytucje społeczne, gospodarcze i polityczne, a także o rządzących nimi prawidłowościach oraz o ich źródłach, naturze, zmianach i sposobach działania ze szczególnym uwzględnieniem norm reguł i instytucji w strukturach bezpieczeństwa.	P6U_W	P6S_WG
	CYB_WG08	Posiada zaawansowaną wiedzę o procesach zmian struktur i instytucji społecznych, gospodarczych i politycznych oraz ich elementów, o przyczynach, przebiegu, skali i konsekwencjach tych zmian.	P6U_W	P6S_WG
	CYB_WG09	Zna w stopniu zaawansowanym poglądy na temat struktur instytucji społecznych, gospodarczych i politycznych oraz rodzajów więzi społecznych i o ich historycznej ewolucji.	P6U_W	P6S_WG
	CYB_WG10	Zna i rozumie kierunki rozwoju i kompetencje członków społeczeństwa informacyjnego, orientuje się w jego kodach	P6U_W	P6S_WG

		kulturowych i komunikacyjnych.		
	CYB_WG11	Zna i rozumie znaczenie informacji jako multidyscyplinarnego klucza kulturowego współczesnego społeczeństwa, jej wagi w procesach społecznych i gospodarczych.	P6U_W	P6S_WG
WIEDZA - kontekst				
	CYB_WK01	Zna i rozumie mechanizmy rządzenia i podejmowania decyzji politycznych, w tym oddziałujących na bezpieczeństwo i zakres właściwego stosowania nowych technologii cyfrowych.	P6U_W	P6S_WK
	CYB_WK02	Zna fundamentalne zasady zarządzania zasobami własności intelektualnej oraz podstawowe pojęcia i zasady z zakresu ochrony własności przemysłowej i prawa autorskiego.	P6U_W	P6S_WK
	CYB_WK03	Ma uporządkowaną i pogłębioną wiedzę specjalistyczną z zakresu studiów, obejmującą teorię i zastosowania praktyczne tej wiedzy.	P6U_W	P6S_WK
	CYB_WK04	Zna i rozumie zasady etyczno-moralne obowiązujące podczas wykonywania czynności i praktyki zawodowej, zna kodeks etyczno zawodowy politologa i eksperta z zakresu cyberbezpieczeństwa.	P6U_W	P6S_WK
	CYB_WK05	Zna podstawowe zasady tworzenia i rozwoju różnych form przedsiębiorczości oraz rozumie społeczne uwarunkowania tych procesów, w tym powstawania inicjatyw z obszarze technologii cyfrowych.	P6U_W	P6S_WK
	CYB_WK06	Rozumie różnorodne uwarunkowania ekonomiczne, prawne, społeczne i etyczne wykonywania roli zawodowej z zakresu cyberbezpieczeństwa.	P6U_W	P6S_WK
W ZAKRESIE UMIEJĘTNOŚCI				
UMIEJĘTNOŚCI – wykorzystanie wiedzy				
	CYB_UW01	Potrafi prawidłowo wykorzystywać w praktyce zawodowej posiadaną wiedzę i interpretować nietypowe problemy oraz zjawiska społeczne z dyscyplin naukowych właściwych dla studiowanego kierunku.	P6U_U	P6S_UW
	CYB_UW02	Potrafi pozyskiwać informacje do analizowania w działalności zawodowej procesów oraz zjawisk społeczno-politycznych, szczególnie związanych z problematyką bezpieczeństwa i cyberbezpieczeństwa.	P6U_U	P6S_UW
	CYB_UW03	Potrafi wykorzystać zdobytą wiedzę do rozstrzygania nietypowych dylematów pojawiających się w praktyce zawodowej.	P6U_U	P6S_UW
	CYB_UW04	Potrafi przeprowadzić analizę proponowanych i nietypowych rozwiązań konkretnych problemów i zaproponować w tym zakresie odpowiednie rozstrzygnięcia.	P6U_U	P6S_UW
	CYB_UW05	Potrafi odczytać i zinterpretować dane do badań społecznych z zakresu nauk społecznych i informatycznych.	P6U_U	P6S_UW
	CYB_UW06	Ma umiejętność posługiwania się w praktyce technologią informatyczną i komunikacyjną właściwą dla studiowanego kierunku.	P6U_U	P6S_UW
UMIEJĘTNOŚCI – komunikowanie się				
	CYB_UK01	Potrafi posługiwać się wybranym językiem obcym na poziomie co najmniej B2 Europejskiego Opisu Kształcenia Językowego.	P6U_U	P6S_UK
	CYB_UK02	Posługuje się w praktyce specjalistyczną terminologią, także w języku obcym, z zakresu bezpieczeństwa i cyberbezpieczeństwa.	P6U_U	P6S_UK
	CYB_UK03	Potrafi sporządzać komunikaty, ekspertyzy, doniesienia i inne formy wypowiedzi pisemnych z przeprowadzonych przez siebie prac analitycznych z zakresu studiowanej dyscypliny.	P6U_U	P6S_UK
	CYB_UK04	Posiada kompetencje do krytycznej analizy materiałów źródłowych i potrafi zakomunikować swoje stanowisko i poglądy w odpowiedniej formie.	P6U_U	P6S_UK
	CYB_UK05	Posiada odpowiedni zasób kompetencji umożliwiających rozumienie procesów informatycznych i ich właściwy opis.	P6U_U	P6S_UK

UMIEJĘTNOŚCI – organizacja pracy				
	CYB_UO01	Potrafi pracować i wykorzystać podstawową wiedzę w zespołach interdyscyplinarnych do analizowania konkretnych procesów i zjawisk w ramach współczesnych procesów technologicznych oraz cyfryzacji życia publicznego i społecznego.	P6U_U	P6S_UO
	CYB_UO02	Potrafi współdziałać z innymi osobami w ramach prac zespołowych, w szczególności w zespołach projektujących postępowanie diagnostyczne i pomocowe w różnych zastosowaniach cyberbezpieczeństwa.	P6U_U	P6S_UO
UMIEJĘTNOŚCI – uczenie się				
	CYB_UU01	Potrafi samodzielnie korzystać z różnorodnych źródeł informacji, w tym w języku obcym, niezbędnych do wykorzystania wybranych teorii i koncepcji w praktyce, głównie w analizie zjawisk i procesów dotyczących współczesnych problemów z zakresu cyberbezpieczeństwa.	P6U_U	P6S_UU
W ZAKRESIE KOMPETENCJI SPOŁECZNYCH				
KOMPETENCJE – oceny – krytyczne podejście				
	CYB_KK01	Jest gotowy do krytycznej oceny wiarygodności różnych źródeł i odbieranych treści, w szczególności do różnicowania treści o różnym stopniu pewności zawodowej, a także potrafi odpowiedzialnie ocenić granice swoich kompetencji zawodowych i rozumie potrzebę zasięgania opinii innych ekspertów, w przypadku trudności z samodzielnym rozwiązywaniem problemów zawodowych.	P6U_K	P6S_KK
	CYB_KK02	Jest gotowy do uznawania znaczenia wiedzy w rozwiązywaniu problemów o charakterze praktycznym, pojawiających się w działalności eksperta w dziedzinie bezpieczeństwa cyfrowego	P6U_K	P6S_KK
	CYB_KK03	Ma świadomość potrzeby aktywnego uczestnictwa w projektach opisujących i analizujących najważniejsze determinanty współczesnych stosunków politycznych oraz społecznych ze szczególnym uwzględnieniem czynnika cyfryzacji współczesnych relacji społecznych.	P6U_K	P6S_KK
KOMPETENCJE - odpowiedzialność				
	CYB_KO01	Ujawnia wysoką odpowiedzialność za wypełnianie zobowiązań społecznych wynikających z działalności zawodowej, a także jest gotowy do współorganizowania, uzupełniania i doskonalenia nabytej wiedzy w zakresie pozyskiwania danych niezbędnych do opisu i analizy rzeczywistości krajowej oraz międzynarodowej.	P6U_K	P6S_KO
	CYB_KO02	Inicjuje działania na rzecz interesu publicznego w zakresie bezpieczeństwa cyfrowego, potrafi odpowiednio zbudować listę priorytetów w celu optymalnej realizacji zadań własnych lub zleconych z zakresu spraw politycznych, społecznych oraz bezpieczeństwa w skali krajowej i międzynarodowej.	P6U_K	P6S_KO
	CYB_KO03	Jest gotów do wspierania innych w formie doradztwa lub innych oddziaływań w zakresie podejmowania i rozwijania aktywności przedsiębiorczej w dobie cyfryzacji życia społecznego.	P6U_K	P6S_KO
KOMPETENCJE – rola zawodowa				
	CYB_KR01	Zdaje sobie sprawę z powagi konsekwencji wynikających z własnych działań zawodowych dla grup społecznych, w związku z tym ujawnia wysoki stopień odpowiedzialności za efekty i konsekwencje swoich poczynań zawodowych, w tym wydawanych opinii i decyzji, a także wypowiedzi publicznych.	P6U_K	P6S_KR
	CYB_KR02	Zdaje sobie sprawę, że zawód wykonywany w obszarze cyberbezpieczeństwa jest zawodem zaufania publicznego, a zatem przestrzega zasad etyki zawodowej poprzez odpowiedzialne dążenie w swoim życiu zawodowym i osobistym do realizowania wysokich standardów.	P6U_K	P6S_KR
	CYB_KR03	Docenia dotychczasowy dorobek w dziedzinie nowych technologii i ich bezpieczeństwa oraz przejawia kreatywność i inicjatywy w działaniu w tej dziedzinie w przyszłości.	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**
CYB_WK04 CYB_WK03 CYB_UW04 CYB_KR01	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 CYB_UW01 CYB_UU01 CYB_UW06 CYB_UO02 CYB_UW02 CYB_KK01 CYB_KK02	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 CYB_WG07 CYB_WK06 CYB_UW01 CYB_KK01 CYB_KK02	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 CYB_WG04 CYB_WG06 CYB_WK03 CYB_UW02 CYB_UW04 CYB_UK04 CYB_UW01 CYB_KO03 CYB_KR03 CYB_KK02 CYB_KO01	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 CYB_WG10 CYB_WK02 CYB_WK04 CYB_UW02 CYB_UU01 CYB_KO02	Wprowadzenie do pojęcia własności intelektualnej: zakres, podział, znaczenie społeczne i gospodarcze Prawa autorskie: autorskie prawa osobiste i majątkowe, czas trwania ochrony, pola eksploatacji Dozwolony użytek edukacyjny i prywatny – gdzie leżą granice legalnego korzystania Plagiat, autoplagiat, uczciwość akademicka – standardy etyczne i prawne Własność przemysłowa: wynalazki, znaki towarowe, wzory przemysłowe, know-how Cyfrowe środowisko pracy i twórczości: otwarte zasoby edukacyjne, AI i prawo, ochrona danych	
Kierunkowe efekty uczenia się	**Zajęcia sportowo-rekreacyjne**	**ECTS: 0**
CYB_WK04 CYB_UO01 CYB_UO02 CYB_KR01	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_WG06 CYB_WG06 CYB_WK03 CYB_UK01 CYB_UK02 CYB_UK01 CYB_UK02 CYB_UK03 CYB_UU01 CYB_KR03 CYB_KR01	***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. ***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. ***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). ***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_WG06 CYB_WG06 CYB_WK03 CYB_UK01 CYB_UK02 CYB_UK01 CYB_UK02 CYB_UU01 CYB_KR03 CYB_KR01	***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 ***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. ***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). ***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_WK03 CYB_WG06 CYB_WK03 CYB_WG07 CYB_WG08 CYB_UW05 CYB_UK01 CYB_UO01 CYB_UW06 CYB_UK02 CYB_KK01 CYB_KR01 CYB_KO01 CYB_KO02 CYB_KO03 CYB_KR02 CYB_KR03	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_WG05 CYB_WG07 CYB_WG08 CYB_WK03 CYB_UW02 CYB_UK03 CYB_UU01 CYB_UW01	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	

CYB_UK04 CYB_KK03 CYB_KK02 CYB_KO02 CYB_KR01 CYB_KR02	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_WG03 CYB_WG04 CYB_WG02 CYB_WG02 CYB_WK03 CYB_UW01 CYB_UW04 CYB_UU01 CYB_KK02 CYB_KO02	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_WG07 CYB_WK03 CYB_WK05 CYB_WG06 CYB_UW02 CYB_UW04 CYB_UO01 CYB_UO02 CYB_KK02 CYB_KK01	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_WG08 CYB_WK03 CYB_WG07 CYB_WG04 CYB_WG09 CYB_UW04 CYB_UW03 CYB_UU01 CYB_KK02 CYB_KO01	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 CYB_WG07 CYB_WG08 CYB_WG09 CYB_UW01 CYB_UW02 CYB_KK02 CYB_KK01	Charakterystyka osobliwości ekonomii jako nauki – analiza najważniejszych cech, język ekonomii, sposoby pozyskiwania danych źródłowych, kategorie ekonomiczne, modelowanie Charakterystyka współczesnych kierunków rozwoju ekonomii (rys historyczny) Analiza procesu badawczego w ekonomii (przedmiot badań ekonomii, schemat tworzenia wiedzy, metody badawcze) Charakterystyka podmiotów ekonomicznych. Treści programowe: Kierunki rozwoju ekonomii jako nauki Proces badawczy w ekonomii – proces wnioskowania w ekonomii, metody badawcze w ekonomii, wyjaśnianie i prognozowanie w ekonomii Osobliwości ekonomii Wewnętrzny podział ekonomii, subdyscypliny ekonomiczne Ekonomia głównego nurtu i poza głównym nurtem Teorie ludnościowe Problem ubóstwa i wykluczenia zawodowego oraz problem aktywności zawodowej i bezrobocia Wzrost i rozwój gospodarczy Inflacja i deflacja

2. KSZTAŁCENIE KIERUNKOWE

Kierunkowe efekty uczenia się	**Wstęp do nauki o państwie i prawie**	**ECTS: 5**
CYB_WG05 CYB_WG07 CYB_WK01 CYB_UW03 CYB_UW04 CYB_KK01 CYB_KK02 CYB_KO03	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 CYB_WG03 CYB_WG08 CYB_WG11 CYB_WK01 CYB_WG10 CYB_UK05 CYB_UW01 CYB_UO01 CYB_UO02 CYB_UU01 CYB_KK01 CYB_KK02 CYB_KO01 CYB_KO02 CYB_KR01 CYB_KR02	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. Treści kształcenia: Terminologia nauk o bezpieczeństwie Bezpieczeństwo jako potrzeba, wartość i prawo człowieka oraz grup społecznych Psychologiczne aspekty bezpieczeństwa Szanse, wyzwania i zagrożenia bezpieczeństwa Podmiotowy wymiar bezpieczeństwa Przedmiotowy wymiar bezpieczeństwa Bezpieczeństwo państwa Subiektywny i obiektywny charakter bezpieczeństwa Czynniki percepcji zagrożeń bezpieczeństwa Człowiek wobec zagrożeń bezpieczeństwa Tradycyjne i współczesne pojmowanie bezpieczeństwa Poziomy analizy bezpieczeństwa Sektory bezpieczeństwa politycznego, militarnego i ekonomicznego Sektory bezpieczeństwa kulturowo-tożsamościowego, ekologicznego i powszechnego	
Kierunkowe efekty uczenia się	**Problemy bezpieczeństwa społeczeństwa informacyjnego**	**ECTS: 3**
CYB_WG02 CYB_WG04 CYB_WG06 CYB_UK05 CYB_UK04 CYB_UW02	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	

CYB_UW06 CYB_UO01 CYB_UO02 CYB_KR02 CYB_KR03 CYB_KK01 CYB_KO03	społecznej -dezinformacja.	
Kierunkowe efekty uczenia się	**Wstęp do cyberbezpieczeństwa**	**ECTS: 5**
CYB_WG11 CYB_WG08 CYB_WG06 CYB_WK01 CYB_WK03 CYB_WG10 CYB_UW01 CYB_UW04 CYB_UO01 CYB_UW02 CYB_KK02 CYB_KK01 CYB_KR01 CYB_KR02	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 CYB_WK03 CYB_WG02 CYB_WG03 CYB_WG05 CYB_WK03 CYB_UW01 CYB_UW02 CYB_UW03 CYB_UW04 CYB_UW06 CYB_UO01 CYB_UO02 CYB_UU02 CYB_KK01 CYB_KO01 CYB_KO02 CYB_KO03 CYB_KR01 CYB_KR02 CYB_KR03	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_WG06; CYB_WG03, CYB_UW01, CYB_UW04, CYB_UW06, CYB_UK05, CYB_UO01, CYB_KK02	Technologie bezpieczeństwa stosowane w systemach informatycznych instytucji publicznych i prywatnych. Elementy analizy zagrożeń oraz interpretacji danych z systemów bezpieczeństwa (SIEM, IDS, IAM). Treści programowe: Systemy bezpieczeństwa IT: funkcje, klasyfikacja, zastosowanie SIEM i IDS – jak działają i jak interpretować dane z tych systemów Skanowanie podatności i analiza luk – narzędzia OpenVAS, Nessus Zarządzanie tożsamością i kontrola dostępu – IAM, MFA, SSO Bezpieczeństwo w środowiskach chmurowych i kontenerowych (Docker, Kubernetes – wprowadzenie) Przykłady incydentów i reakcji na nie – podstawy zarządzania incydentami Współpraca między menedżerami a zespołami IT – modele komunikacji i odpowiedzialności

Kierunkowe efekty uczenia się	**Polityka cyberbezpieczeństwa państwa**	**ECTS: 3**
CYB_WG08 CYB_WG06 CYB_WK01 CYB_WK03 CYB_WG10 CYB_UO01 CYB_UW02 CYB_KK02 CYB_KK01 CYB_KR02	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_WK03 CYB_WG08 CYB_WG05 CYB_WG06 CYB_WK05 CYB_UW01 CYB_UW02 CYB_UW04 CYB_UO01 CYB_UW03 CYB_UK03 CYB_KO02 CYB_KO03 CYB_KK02	Współczesny zakres pojęcia „zarządzanie" w kontekście ewolucji środowiska bezpieczeństwa. Perspektywa podmiotowa i przedmiotowa.. 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.	

Kierunkowe efekty uczenia się	**Zarządzanie bezpieczeństwem informacji**	**ECTS: 3**
CYB_WK03 CYB_WK04 CYB_WG03 CYB_WG06 CYB_WG07 CYB_UW01 CYB_UW02 CYB_UU01 CYB_UW04	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	

CYB_KK01 CYB_KR01 CYB_KR02 CYB_KR03	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_WK03 CYB_WG02 CYB_UW02 CYB_UW03 CYB_UW04 CYB_UO01 CYB_KK02 CYB_KK01 CYB_KK03	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 CYB_WG07 CYB_WG06 CYB_UW03 CYB_UW04 CYB_UW01 CYB_UO01 CYB_KK01 CYB_KK02 CYB_KR01	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**	**ECTS: 28**
CYB_WK04 CYB_WG06 CYB_WK06 CYB_UW02 CYB_UW03 CYB_UW05 CYB_UW06 CYB_UO01 CYB_UO02 CYB_KO01 CYB_KK02 CYB_KK03	Charakterystyka miejsca odbywania praktyki, zapoznanie z charakterem działalności prowadzonej przez organizację, w której odbywa się praktyka. Poznanie struktury organizacyjnej, podstaw prawnych, warunków pracy oraz charakterystyki prac specyficznych dla organizacji, ze szczególnym uwzględnieniem roli specjalisty do spraw cyberbezpieczeństwa. Charakterystyka najważniejszych działów funkcjonujących w organizacji, w której odbywa się praktyka. Poznanie zasad i przestrzegania przepisów bezpieczeństwa i higieny pracy obowiązujących na stanowiskach, na których odbywa się praktyka. Charakterystyka sposobów realizowania zasad, stosowanych metod, technik pracy i wyposażenia, w tym techniczno-technologicznego. Charakterystyka zakresu czynności wykonywanych w organizacji, szczególnie na stanowiskach przydatnych z punktu widzenia cyberbezpieczeństwa np. procesy pracy, sposób działań menedżerskich, zasady organizacji działalności biznesowej. Zapoznanie się z dokumentami wiodącymi dla wykonywania zadań w czasie praktyki. Aktywne uczestnictwo w czynnościach związanych z wykonywanymi zadaniami podczas praktyki. Aktywne uczestnictwo w pracach w zakresie zarządzania. Omówienie zmian zachodzących w wyniku zmian w otoczeniu organizacji. Przygotowanie sprawozdań i prezentacji specyficznych dla realizowanych zadań w danej organizacji. Opracowanie własnych opinii i spostrzeżeń, poddanie pod dyskusję propozycji rozwiązania zaobserwowanych problemów.	
Kierunkowe efekty uczenia się	**Inżynieria informacji w przestrzeni publicznej**	**ECTS: 3**
CYB_WG03 CYB_WK03 CYB_WG10	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	

CYB_WK01 CYB_UW05 CYB_UW04 CYB_UW02 CYB_UK04 CYB_KK02 CYB_KO01 CYB_KR01	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_WG10 CYB_WG11 CYB_WK03 CYB_WG08 CYB_UW02 CYB_UW01 CYB_UW06 CYB_UW04 CYB_UW05 CYB_KK02 CYB_KK01 CYB_KK03	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 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_WK03 CYB_WG06 CYB_UW01 CYB_UW02 CYB_UW03 CYB_UW06 CYB_UW04 CYB_KO02 CYB_KR01 CYB_KO01	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_WG04 CYB_WG10 CYB_WK03 CYB_UW03 CYB_UW06 CYB_UW01 CYB_KK02 CYB_KO01 CYB_KK01	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_WG03 CYB_WK01 CYB_WG05 CYB_WK03 CYB_WG08 CYB_UW01 CYB_UW02 CYB_UK03 CYB_UO01 CYB_KO01 CYB_KR01 CYB_KR03	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_WK03 CYB_WG04 CYB_WG03 CYB_UW02 CYB_UK04 CYB_UW01 CYB_UW04 CYB_KO01 CYB_KO02 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 CYB_WG05 CYB_WG07 CYB_WG08 CYB_WG10 CYB_WK01 CYB_WK06 CYB_UW02 CYB_UW03 CYB_UW04 CYB_UW05 CYB_UO01 CYB_UO02 CYB_KK02 CYB_KK03 CYB_KO01 CYB_KR01 CYB_KR02	Definicje i typologie cyberprzestępstw (hacking, phishing, cyberstalking, grooming, DDoS, ransomware) Cyberprzestępczość a przestępczość tradycyjna – punkty wspólne i różnice Statystyki i trendy przestępczości cyfrowej w Polsce i na świecie Krajowe ramy prawne (Kodeks karny, ustawa o zwalczaniu nieuczciwej konkurencji, RODO) Międzynarodowe instrumenty prawne (Konwencja budapeszteńska, dyrektywy UE, prawo ONZ) Organy ścigania i procedury dochodzeniowe w sprawach cyberprzestępstw Motywacje sprawców cyberprzestępstw (np. zysk, ideologia, zaburzenia osobowości) Społeczna percepcja przestępczości w sieci – zjawisko normalizacji Cyberprzemoc i jej skutki społeczne – ofiary, świadkowie, społeczne milczenie Dobre praktyki w ochronie przed cyberzagrożeniami (edukacja, zarządzanie hasłami, cyfrowa higiena) Rola instytucji publicznych i organizacji pozarządowych w prewencji Kampanie społeczne i edukacyjne Studium przypadków: cyberataki na instytucje publiczne, oszustwa internetowe, sextortion	
Kierunkowe efekty uczenia się	**Elementy kryptografii**	**ECTS: 3**
CYB_WK03 CYB_WG07 CYB_WG11 CYB_UO01 CYB_UW03 CYB_UW04 CYB_UW05 CYB_KO03 CYB_KO01 CYB_KK03	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_WK03 CYB_WG11 CYB_WG06 CYB_UW04 CYB_UW05 CYB_UU01 CYB_UW01 CYB_UW02 CYB_KO02 CYB_KO03 CYB_KK01	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_WG06 CYB_WG07 CYB_WK02 CYB_WK05 CYB_UW04 CYB_UW06 CYB_UU01 CYB_UO01 CYB_UO02 CYB_KK02 CYB_KO01 CYB_KO03	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_WG07 CYB_WK03 CYB_WG08 CYB_WK01 CYB_WG02 CYB_UW01 CYB_UW02 CYB_UW03 CYB_UW04 CYB_UK02 CYB_UW06 CYB_KO01 CYB_KO03 CYB_KK02	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_WG03 CYB_WG05 CYB_WK03 CYB_WG07 CYB_UW02 CYB_UW01 CYB_UW03 CYB_UW04 CYB_UO01 CYB_UO02 CYB_KO03 CYB_KO02 CYB_KK01	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_WK03 CYB_WG06 CYB_WG04 CYB_WG07 CYB_WK01 CYB_UW01 CYB_UW02 CYB_UW03 CYB_UK04 CYB_UO01 CYB_KK01 CYB_KO02 CYB_KR02 CYB_KK02	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_WK03 CYB_WG02 CYB_WG04 CYB_WG07 CYB_UW01 CYB_UW02 CYB_UW04 CYB_UW03 CYB_KO02 CYB_KO01 CYB_KR01 CYB_KK02	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_WK03 CYB_WG09 CYB_WG05 CYB_WG06 CYB_WK02 CYB_UW01 CYB_UW04 CYB_UO01 CYB_UU01 CYB_KR03 CYB_KK01 CYB_KK02 CYB_KK03	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_WG10 CYB_WG07 CYB_WK01 CYB_WK03 CYB_UW01 CYB_UW02 CYB_UW03 CYB_UW06 CYB_UK04 CYB_KK01 CYB_KO01 CYB_KR01	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_WK03 CYB_WG06 CYB_WG07 CYB_WK02 CYB_WG02 CYB_WG08 CYB_UW01 CYB_UW04 CYB_UW03 CYB_UO02 CYB_KK02 CYB_KO01 CYB_KR03	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_WK03 CYB_WG11 CYB_WK02 CYB_WG06	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.	

CYB_WG08 CYB_UW05 CYB_UW06 CYB_WK01 CYB_WK02 CYB_UW04 CYB_UW05 CYB_KO01 CYB_KO03 CYB_KR03 CYB_KR02		
Kierunkowe efekty uczenia się	**Bezpieczeństwo informacji w obrocie gospodarczym**	**ECTS: 3**
CYB_WK03 CYB_WG07 CYB_WK02 CYB_WK05 CYB_UW01 CYB_UW02 CYB_UW04 CYB_UK04 CYB_UO01 CYB_KK02 CYB_KO01 CYB_KO02 CYB_KR03	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_WK03 CYB_WG07 CYB_WG03 CYB_WG08 CYB_WG05 CYB_UW02 CYB_UW01 CYB_UW03 CYB_UK04 CYB_KK01 CYB_KR02 CYB_KO01 CYB_KK02	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_WG04 CYB_WG03 CYB_WG07 CYB_WK03 CYB_UW01 CYB_UW02 CYB_UW03 CYB_UW04 CYB_UK04 CYB_KK01 CYB_KK02 CYB_KO01	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_WG07 CYB_WK01 CYB_WG03 CYB_WG08 CYB_WK03 CYB_UW01 CYB_UW02 CYB_UW03 CYB_UW01 CYB_KO01 CYB_KK02 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_WK03 CYB_WG06 CYB_WK03 CYB_UW01 CYB_UW06 CYB_UW02 CYB_UW03 CYB_KK01 CYB_KR03	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_WG11 CYB_WK03 CYB_WG06 CYB_UW01 CYB_UW03 CYB_UW06 CYB_UO01 CYB_UW01 CYB_UW03 CYB_KO02 CYB_KK02 CYB_KR03	Wprowadzenie do tematyki architektura systemów komputerowych. Pojęcia organizacja i architektura komputerów. Struktura i działanie. Ewolucja systemów liczących oraz rozwój systemów komputerowych. Systemy liczbowe. System binarny, ósemkowy, heksagonalny. Konwersje liczb całkowitych i ułamkowych dziesiętnych na kody binarne. Operacje arytmetyczne na liczbach binarnych. Liczby zmiennoprzecinkowe. Standard zapisu liczb zmiennoprzecinkowych IEEE-754. Kodowanie znaków. Podstawy działania układów cyfrowych. Zmienne i operacje logiczne. Aksjomaty algebry Boole'a i prawa de Morgana. Funkcje logiczne. Minimalizacja funkcji boolowskich. Realizacja funkcji logicznych. Podział na układy kombinacyjne i sekwencyjne. Kombinacyjne układy cyfrowych. Kombinacyjne układy cyfrowych. Projektowania kombinacyjnych układów logicznych opartą na analizie tablic Karnaugha. Budowa złożonych układów kombinacyjnych. Sekwencyjne układy cyfrowe. Abstrakcyjny model sekwencyjnych układów cyfrowych. Zasadnicze typy układów sekwencyjnych: przerzutniki, rejestry, liczniki. Programowalne układy cyfrowe zawierające zarówno układy kombinacyjne jak i sekwencyjne. Struktura blokowa komputera typu von Neumana. Podstawowe cechy architekturalne i techniczne mikroprocesorów. Model programowy komputera typu von Neumana: format rozkazów, tryby adresowania, wykonywanie programów, MASM32 – przykład asemblera dla procesorów 32 bitowych. Obsługa standardowego wejścia-wyjścia. Szkielet programu w języku assembler w środowisku MASM32. Rejestry procesora 32 bitowego. Realizacja rozkazów arytmetycznych, logicznych, przesłań, przesunięć. Skoki i rozgałęzienia. Budowanie makr. Przesyłanie i zarzadzanie danymi. Przerwania. Układy i operacje wejścia-wyjścia. Typy i hierarchia pamięci. Organizacja i architektura systemów pamięci. Pamięć podręczna. Pamięci dynamiczne RAM. Pamięci ROM. Układy DMA. Architektury podstawowych typów procesorów: CISC i RISC. Procesory RISC i systemy równoległe. Klasyfikacja Flynna systemów komputerowych.. Komputery wektorowe. Podstawowe systemy liczbowe: binarne, o różnych podstawach 3,4, 8 oraz heksagonalny. Konwersje liczb dziesiętnych całkowitych i ułamkowych na kody binarne i heksagonalny. Operacje arytmetyczne na liczbach zapisanych w kodach binarnych. Kodowanie liczb wymiernych w formacie	

	zmiennoprzecinkowym IEEE754. Operacje arytmetyczne na liczbach w formacie zmiennoprzecinkowym . Kodowanie znaków. Konwersje liczb dziesiętnych całkowitych na kod BCD. Maski bitowe. Metody opisu i minimalizacji funkcji boolowskich: tablica prawdy, formuła koniunkcyjno-alternatywna, formuła alternatywno-koniunkcyjnia. Tworzenie prostych układów kombinacyjnych przy pomocy symulatora Multimedia Logic (lub Digital Works) i weryfikacja ich działania. Mapy Karnaugh'a. Sekwencyjne układy cyfrowe. Abstrakcyjny model sekwencyjnych układów cyfrowych. Zasadnicze typy układów sekwencyjnych: przerzutniki, rejestry, liczniki. Wprowadzenie do środowiska masm32, kompilacja, łączenie. Uruchomianie programu w masm32. Ustawianie flag procesora w języku asembler. Samodzielna realizacja zadania programistycznego z zakresu ustawiania flag procesora. Skoki i rozgałęzienia. Realizacja zadania programistycznego ze skokami i instrukcjami warunkowymi. Procedury i makra. Przerwania. Pamięć podręczna. Realizacja zadania programistycznego pobrania i wysłania danych do pamięci.	
Kierunkowe efekty uczenia się	**Technologie sieciowe**	**ECTS: 4**
CYB_WK03 CYB_WG06 CYB_WG08 CYB_UW01 CYB_UW06 CYB_UW03 CYB_UW02 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 IPv6. Analiza składniowa datagramu IPv6	
Kierunkowe efekty uczenia się	**Systemy operacyjne**	**ECTS: 4**
CYB_WG01 CYB_WG06 CYB_WK03 CYB_UW02 CYB_UW05 CYB_UK03 CYB_KO01 CYB_KR03	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.	

Sposoby weryfikacji i oceny efektów uczenia się osiągniętych przez studenta w trakcie całego cyklu kształcenia

Do metod weryfikacji efektów uczenia się uzyskiwanych w procesie kształcenia zalicza się:

1) egzaminy – ustne, pisemne (opisowe, testowe);
2) zaliczenia – ustne, pisemne (opisowe, testowe);
3) kolokwium;
4) przygotowanie indywidualnie lub zespołowo referatu, eseju itp.;
5) przygotowanie indywidualnie lub zespołowo projektu;
6) wykonanie sprawozdań, raportów, zadanych prac domowych itp. – indywidualnie lub zespołowo;
7) rozwiązywanie zadań problemowych w trakcie oraz poza zajęciami – indywidualnie lub zespołowo;
8) prezentacje multimedialne prowadzone i przygotowywane indywidualnie lub zespołowo;
9) wypowiedzi ustne, aktywność w trakcie zajęć, udział w dyskusji;
10) analizy przypadków;
11) egzamin dyplomowy;
12) inne, specyficzne i szczególne formy weryfikacji zakładanych efektów uczenia się wskazane w kartach poszczególnych przedmiotów (sylabusach).

Ocena stopnia osiągnięcia założonych efektów uczenia się obejmuje wszystkie kategorie efektów uczenia się (wiedzę, umiejętności, kompetencje społeczne). Wybór metod weryfikacji powinien uwzględniać specyfikę poszczególnych kategorii efektów uczenia się, a także specyfikę przedmiotu oraz współczesne uwarunkowania społeczne i możliwości technologiczne ich weryfikacji.

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.

Metodą weryfikacji efektów uczenia się uzyskanych z całości cyklu kształcenia na poziomie studiów jest egzamin dyplomowy.

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.

Regulamin studiów określa skalę stosowanych ocen w ramach procesu weryfikacji efektów uczenia się, a Zarządzenie Rektora określa wewnętrzny system oceniania, będący zbiorem zasad dotyczących oceniania studentów w zakresie opanowania przez nich efektów uczenia się oraz kryteria ogólne wystawienia danej oceny z przedmiotu (por. Tabela). W Regulaminie studiów przewidziane są także zaliczenia na: zaliczony/niezaliczony (odpowiednio: zal/nzal). Dotyczy to głównie zajęć niewymagających weryfikacji efektów uczenia się na ocenę (np. zajęcia sportowo-rekreacyjne, BHP).

Kryteria ocen w procesie weryfikacji efektów uczenia się

Ocena	Opis wymagań	Wymagany procent osiągniętych efektów uczenia się dla przedmiotu
celujący (6,0)	Student osiągnął efekty uczenia ilościowo lub jakościowo wykraczające poza zakres przewidziany programem kształcenia dla przedmiotu, w szczególności: posiada wiedzę znacznie przekraczającą zakres określony programem kształcenia dla przedmiotu, samodzielnie określa i rozwiązuje problemy teoretyczne i praktyczne, potrafi wykorzystać wiedzę w nowych sytuacjach problemowych, poprawnie i swobodnie posługuje się terminologią naukową oraz zawodową.	> 90% oraz dodatkowe osiągnięcia wykraczające ilościowo lub jakościowo poza te przewidziane na ocenę bardzo dobrą
bardzo dobry (5,0)	Student opanował pełen zakres wiedzy i umiejętności określony w programie kształcenia dla przedmiotu, samodzielnie rozwiązuje problemy teoretyczne i praktyczne, potrafi wykorzystać wiedzę w nowych sytuacjach problemowych, poprawnie posługuje się terminologią naukową oraz zawodową.	min. 90%
dobry plus (4,5)	Student osiągnął efekty uczenia się powyżej wymagań dla oceny dobrej, ale niewystarczające dla oceny bardzo dobrej.	min. 85%
dobry (4,0)	Student opanował większość wiadomości i umiejętności określonych programem kształcenia dla przedmiotu, rozwiązuje typowe zadania teoretyczne i praktyczne, ujmuje w terminach naukowych i zawodowych podstawowe pojęcia i prawa.	min. 70%
dostateczny plus (3,5)	Student osiągnął efekty uczenia się powyżej wymagań dla oceny dostatecznej, ale niewystarczające dla oceny dobrej.	min. 65%
dostateczny (3,0)	Student opanował 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.	min. 50%
niedostateczny (2.0)	Student nie opanował niezbędnego minimum podstawowych wiadomości i umiejętności określonych programem kształcenia dla przedmiotu, nie potrafi rozwiązać zadań o niewielkim stopniu trudności, popełnia rażące błędy terminologiczne, a styl jego wypowiedzi jest nieporadny.	mniej niż 50%

Ocena osiągnięcia efektów uczenia się przeprowadzana jest w następujących etapach:

- w trakcie realizacji efektów uczenia się w ramach danego przedmiotu/modułu oraz po jej zakończeniu poprzez weryfikację efektów uczenia się dokonaną dla każdego studenta przez prowadzącego zajęcia/egzaminatora;
- po zrealizowaniu programu danego przedmiotu/modułu poprzez weryfikację efektów uczenia się dokonaną przez prowadzącego zajęcia/koordynatora przedmiotu/modułu;
- po zakończeniu każdego semestru poprzez weryfikację efektów uczenia się uzyskanych przez studentów kierunku;
- po zakończeniu praktyk zawodowych;
- na egzaminie dyplomowym poprzez weryfikację efektów uczenia się dokonaną dla każdego studenta przez egzaminatorów biorących udział w egzaminie dyplomowym;
- na bieżąco poprzez ocenę realizacji efektów uczenia się dokonaną przez hospitujących zajęcia;
- po zakończeniu każdego cyklu kształcenia poprzez weryfikację efektów uczenia się według mierników ilościowych oraz w drodze monitorowania losów absolwentów i oceny ich funkcjonowania na rynku pracy.

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 Akademii Ekonomiczno-Humanistycznej w Warszawie. W Regulaminie praktyk zapisano m.in., iż Uczelnia zapewnia miejsca praktyk dla studentów i zawiera w tej sprawie porozumienie z praktykodawcą lub zatwierdza miejsca odbywania praktyk, w przypadku samodzielnego ich wskazania przez studenta, poprzez wystawienie skierowania na praktyki. Poza tym, student może zrealizować praktykę na podstawie wykonywanej pracy zawodowej (o ile umożliwia ona osiągnięcie efektów uczenia się przewidzianych dla praktyk), w ramach programu ERASMUS+, działalności studenckiego koła naukowego, w AEH w Warszawie oraz w ramach wolontariatu. Obowiązkowym sposobem dokumentacji przebiegu praktyki i realizowanych w jej trakcie zadań jest prowadzony przez studenta „Dzienniczek praktyk".

Szczegółowe zasady realizacji praktyk na kierunku cyberbezpieczeństwo, w tym: cel praktyk, efekty uczenia się, treści programowe, umiejscowienie praktyk w planie studiów, wymiar praktyk, metody weryfikacji i oceny osiągnięcia przez studentów efektów uczenia się zakładanych dla praktyk, sposób dokumentowania przebiegu praktyk i realizowanych w ich trakcie zadań, kryteria, które muszą spełniać placówki, w których odbywają się praktyki, reguły zatwierdzania miejsca praktyki samodzielnie wybranego przez studenta oraz warunki kwalifikowania studenta na praktyki określa Program praktyk zawodowych na kierunku cyberbezpieczeństwo.

Praktyki zawodowe realizowane przez studentów kierunku cyberbezpieczeństwo mają umożliwić im zweryfikowanie dotychczas nabytej wiedzy teoretycznej oraz nabycie praktycznych umiejętności wykorzystania tej wiedzy w pracy politologa lub analityka. Mają także na celu wykształcenie w studencie umiejętności pracy w grupie, poczucia etyki zawodowej oraz znaczenia realizowania praktycznych czynności zawodowych.

Praktyki na kierunku cyberbezpieczeństwo mają charakter zajęć obowiązkowych i planowane są do realizacji:

- 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 realizowanych w okresie 6 miesięcy. Student uzyskuje 28 punktów ECTS za zrealizowane praktyki zawodowe.

Treści programowe realizowane podczas praktyki zawodowej powinny odzwierciedlać specyfikę zadań powierzanych politologom oraz analitykom w danej placówce. Student podczas odbywania praktyk zawodowych odbywa zajęcia praktyczne w jednostkach o zróżnicowanym charakterze z uwagi na szeroki zakres zadań zawodowych specjalisty ds. cyberbezpieczeństwa. Mogą one obejmować zadania:

1. Analityczne – student wykorzystuje i rozwija swoje zdolności zbierania i przetwarzania informacji w zakresie odpowiednim dla placówki, w której realizuje swoje praktyki zawodowe. Weryfikuje prawdziwość informacji, wyciąga wnioski oraz podejmuje decyzje mające przyczynić się do realizacji powierzonych mu zadań.
2. Prognostyczne – student wykorzystuje i rozwija swoje zdolności przewidywania zdarzeń i procesów w zakresie odpowiednim dla placówki, w której realizuje swoje praktyki zawodowe.

3. Rekrutacyjne – student wykorzystuje i rozwija swoje umiejętności perswazji do powierzonych mu zadań o charakterze rekrutacyjnym.

4. Administracyjne – student sprawnie i skutecznie realizuje powierzone mu zadania administracyjne właściwe dla placówki, w której realizuje swoje praktyki zawodowe.

5. Sporządzanie opinii i ekspertyz – student przygotowuje opinie oraz ekspertyzy powiązane z tematami właściwymi dla miejsca, w którym realizuje swoje praktyki zawodowe.

6. Badania – student dąży do ustawicznego aktualizowania swojej wiedzy, aktywnie uczestniczy w badaniach oraz przygotowuje opracowania na tematy związane z obszarem zainteresowań.

7. Inne zadania

Treści programowe realizowane podczas praktyki zawodowej odzwierciedlają specyfikę zadań powierzanych specjaliście ds. cyberbezpieczeństwa w danej placówce. Podczas odbywania praktyki student nabywa wiedzę, umiejętności i kompetencje w następującym zakresie tematycznym: charakterystyka miejsca odbywania praktyki, charakterystyka najważniejszych działów funkcjonujących w danej jednostce, poznanie zasad przepisów bezpieczeństwa i higieny pracy. W zależności od charakteru jednostki, student uczy się pracować w specyficznych warunkach miejsca pracy – powinien zostać zapoznany z zasadami obowiązującymi go podczas wykonywania zadań zawodowych, zasadami profesjonalnego kontaktu z klientami, pacjentami i współpracownikami. Student powinien poznać specyficzne dla pracy specjalisty ds. cyberbezpieczeństwa stosowane metody oraz narzędzia i nauczyć się ich poprawnego stosowania w zależności od charakteru miejsca praktyk, a w przyszłości miejsca pracy.

Miejscem praktyk może być placówka dająca możliwość odbywania praktyk pod opieką/nadzorem zakładowego opiekuna praktyk lub osoby sprawującej bezpośredni nadzór nad czynnościami wykonywanymi przez studenta podczas praktyk. Typ umowy zatrudnienia opiekuna praktyk w danej instytucji lub firmie nie jest istotny (może to być umowa o pracę, umowa zlecenia, samozatrudnienie itp.), ważne jest natomiast, by wymiar jego zatrudnienia umożliwiał sprawowanie bieżącej opieki nad studentem, obserwację jego pracy i weryfikację osiągnięcia zakładanych dla praktyki efektów uczenia się.