UCHWAŁA NR 22/2026

Senatu Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie

z dnia 29 kwietnia 2026 roku

w sprawie zmiany programu studiów rozpoczętego w roku akademickim 2025/2026 na kierunku

Cyberbezpieczeństwo, studia I stopnia, profil praktyczny

Działając na podstawie art. 28 ust. 1 pkt 11 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2024 r. poz. 1571 z późn. zm.), § 9 ust.2 pkt. 1 rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów (Dz.U. 2023.2787 t.j.) oraz § 8 ust. 1 pkt 12 Statutu Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie Senat Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie uchwala, co następuje:

§ 1

1. Senat Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie dokonuje zmiany programu studiów rozpoczętego w roku akademickim 2025/2026 na kierunku **Cyberbezpieczeństwo, studia I stopnia, profil praktyczny.**

2. Program studiów na kierunku **Cyberbezpieczeństwo** stanowi załącznik do niniejszej uchwały.

§ 2

1. Uchwała wchodzi w życie z dniem jej podjęcia.

Przewodniczący Senatu

/ wersja podpisana do wglądu w Biurze Rektora /

dr hab. Radosław Wiśniewski, prof. UAFM

Załącznik
do Uchwały nr 22/2026
Senatu Uniwersytetu Andrzeja
Frycza Modrzewskiego w Krakowie
z dnia 29 kwietnia 2026 r.

UNIWERSYTET
Andrzeja Frycza Modrzewskiego
w Krakowie

PROGRAM STUDIÓW

CYBERBEZPIECZEŃSTWO

STUDIA I STOPNIA

PROFIL PRAKTYCZNY

Rok akademicki rozpoczęcia cyklu kształcenia: 2025/2026

Kraków 2026

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: 2398 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 55%** **Nauki o bezpieczeństwie 20%** **Informatyka techniczna i telekomunikacja 25%**
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	**Studia stacjonarne: 92,4 (51,3%)** **Studia niestacjonarne: 63,7 (35,4%)**
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć kształtujących umiejętności praktyczne	**107,5 pkt. ECTS (60,3%)**
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	**56 pkt. ECTS (31,1%)**
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.	Wychowanie fizyczne	**0**	60	0
3.	Język obcy **(DW)**	**9**	120	64
4.	Umiejętności akademickie	**1**	15	8
5.	Wstęp do nauk o państwie i prawie	**5**	30	24
6.	Wprowadzenie do filozofii	**5**	35	20
7.	Podstawy komunikacji społecznej	**4**	30	24
8.	Własność intelektualna	**5**	30	24
9.	Podstawy ekonomii	**5**	30	24
10.	Metodologia badań naukowych	**4**	30	16
11.	Prawoznawstwo	**5**	30	24
12.	Podstawy socjologii	**4**	30	16
13.	Zarządzanie projektami	**3**	30	16
	Razem	**50**	**478**	**268**
2. Kształcenie kierunkowe				
14.	Wprowadzenie do nauk o bezpieczeństwie	**3**	60	32
15.	Administracja publiczna	**4**	30	24
16.	Międzynarodowe stosunki polityczne	**3**	30	24
17.	Polityka cyberbezpieczeństwa państwa / Problem bezpieczeństwa społeczeństwa informacyjnego **(DW)**	**3**	30	16
18.	Wstęp do cyberbezpieczeństwa	**5**	30	16
19.	Zarządzanie w sytuacjach kryzysowych	**4**	60	32
20.	Przestępczość w cyberprzestrzeni	**3**	30	16
21.	Systemy bezpieczeństwa państwa	**3**	30	16
22.	Operacje informacyjne i oddziaływanie kognitywne	**3**	30	16
23.	Bezpieczeństwo sieci komputerowych/ Podstawy pentestingu **(DW)**	**4**	60	32
24.	Dostęp do informacji publicznej i ochrona informacji niejawnych/ Zarzadzanie bezpieczeństwem informacji w przedsiębiorstwie **(DW)**	**3**	30	16
25.	Systemy i technologie w cyberbezpieczeństwie	**4**	60	32
26.	Ethical Hacker	**3**	30	16
27.	Audyt bezpieczeństwa sieci teleinformatycznych	**4**	60	32
28.	Prawo ochrony danych osobowych/ Zarzadzanie bezpieczeństwem informacji w administracji publicznej **(DW)**	**3**	30	16
29.	Metodyka przygotowania projektu	**3**	30	16
30.	Formy prowadzenia działalności gospodarczej / Podstawy finansów prywatnych i publicznych **(DW)**	**3**	30	16

31.	Informatyka śledcza	**4**	60	32
32.	Cyberkultura w XXI w.	**2**	30	16
33.	Współczesny terroryzm polityczny	**3**	30	16
34.	OPSEC w internecie – podstawy anonimizacji w sieci	**3**	30	16
35.	Wojna hybrydowa	**3**	30	16
36.	Projekt społeczny	**5**	30	16
37.	Praktyka zawodowa	**28**	720	720
	Razem	**106**	**1590**	**1200**
	3. Kształcenie informatyczne			
38.	Architektura systemów komputerowych i systemy operacyjne	**4**	60	32
39.	Wstęp do programowania	**4**	60	32
40.	Bezpieczeństwo aplikacji	**4**	60	32
41.	Programowanie	**3**	30	16
42.	Technologie sieciowe	**3**	30	16
43.	Elementy kryptologii	**4**	60	32
44.	Podstawy technologii chmurowych/ Podstawy technologii mobilnych i internetu rzeczy (IoT) **(DW)**	**3**	30	16
	Razem	**25**	**330**	**176**
	Ogółem w całym toku studiów	**180**	**2398**	**1620**

DW – zajęcia do wyboru

Zajęcia lub grupy zajęć kształtujących umiejętności praktyczne

Nazwa zajęć lub grupy zajęć	Forma/formy zajęć	Łączna liczba godzin		Liczba punktów ECTS
		Studia stacjonarne	Studia niestacjonarne	
Język obcy **(DW)**	lektoraty	120	64	9
Wprowadzenie do nauk o bezpieczeństwie	ćwiczenia	30	16	1,5
Polityka cyberbezpieczeństwa państwa / Problem bezpieczeństwa społeczeństwa informacyjnego **(DW)**	konwersatorium	30	16	3
Zarządzanie w sytuacjach kryzysowych	ćwiczenia	30	16	2
Architektura systemów komputerowych i systemy operacyjne	laboratorium	30	16	2
Przestępczość w cyberprzestrzeni	konwersatorium	30	16	3
Systemy bezpieczeństwa państwa	konwersatorium	30	16	3
Operacje informacyjne i oddziaływanie kognitywne	konwersatorium	30	16	3
Wstęp do programowania	laboratorium	30	16	2
Bezpieczeństwo aplikacji	laboratorium	30	16	2
Bezpieczeństwo sieci komputerowych/ Podstawy pentestingu **(DW)**	laboratorium	30	16	2
Programowanie	laboratorium	30	16	3
Dostęp do informacji publicznej i ochrona informacji niejawnych/ Zarzadzanie bezpieczeństwem informacji w przedsiębiorstwie **(DW)**	konwersatorium	30	16	3
Systemy i technologie w cyberbezpieczeństwie	laboratorium	30	16	2
Technologie sieciowe	laboratorium	30	16	3
Elementy kryptologii	ćwiczenia	30	16	2
Podstawy technologii chmurowych/ Podstawy technologii mobilnych i internetu rzeczy (IoT) **(DW)**	konwersatorium	30	16	3
Ethical Hacker	warsztaty	30	16	3
Audyt bezpieczeństwa sieci teleinformatycznych	ćwiczenia	30	16	2
Prawo ochrony danych osobowych/ Zarzadzanie bezpieczeństwem informacji w administracji publicznej **(DW)**	konwersatorium	30	16	3
Metodyka przygotowania projektu	konwersatorium	30	16	3
Formy prowadzenia działalności gospodarczej / Podstawy finansów prywatnych i publicznych **(DW)**	konwersatorium	30	16	3
Informatyka śledcza	laboratorium	30	16	2
Cyberkultura w XXI w.	konwersatorium	30	16	2
Współczesny terroryzm polityczny	konwersatorium	30	16	3
OPSEC w internecie – podstawy anonimizacji w sieci	laboratorium	30	16	3
Wojna hybrydowa	konwersatorium	30	16	3
Projekt społeczny	konwersatorium	30	16	5
Praktyka zawodowa	praktyki	720	720	28
	Razem	**1650**	**1216**	**108,5**

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 (DW)	lektoraty	120	64	9
Polityka cyberbezpieczeństwa państwa / Problem bezpieczeństwa społeczeństwa informacyjnego (DW)	konwersatorium	30	16	3
Bezpieczeństwo sieci komputerowych/ Podstawy pentestingu **(DW)**	wykład, laboratorium	60	32	4
Dostęp do informacji publicznej i ochrona informacji niejawnych/ Zarzadzanie bezpieczeństwem informacji w przedsiębiorstwie (DW)	konwersatorium	30	16	3
Podstawy technologii chmurowych/ Podstawy technologii mobilnych i internetu rzeczy (IoT) **(DW)**	konwersatorium	30	16	3
Prawo ochrony danych osobowych/ Zarzadzanie bezpieczeństwem informacji w administracji publicznej **(DW)**	konwersatorium	30	16	3
Formy prowadzenia działalności gospodarczej / Podstawy finansów prywatnych i publicznych **(DW)**	konwersatorium	30	16	3
Praktyka zawodowa (DW)	praktyki	720	720	28
	Razem	**1050**	**896**	**56**

Zajęcia, które <u>mogą być</u> prowadzone z wykorzystaniem metod i technik kształcenia na odległość

NAZWA ZAJĘĆ	WYKŁADY - ilość godzin		ECTS – w części realizowanej na odległość
	Studia stacjonarne	Studia niestacjonarne	
Umiejętności akademickie	15	8	1
Wstęp do nauki o państwie i prawie	30	24	5
Wprowadzenie do filozofii	35	20	5
Podstawy komunikacji społecznej	30	24	4
Własność intelektualna	30	24	5
Wprowadzenie do nauk o bezpieczeństwie	30	16	2
Podstawy ekonomii	30	24	5
Metodologia badań naukowych	30	16	4
Prawoznawstwo	30	24	5
Podstawy socjologii	30	16	4
Administracja publiczna	30	24	4
Zarzadzanie projektami	30	16	3
Międzynarodowe stosunki polityczne	30	24	3
Wstęp do cyberbezpieczeństwa	30	16	5
Zarządzanie w sytuacjach kryzysowych	30	16	2
Architektura systemów komputerowych i systemy operacyjne	30	16	2
Wstęp do programowania	30	16	2
Bezpieczeństwo aplikacji	30	16	2
Bezpieczeństwo sieci komputerowych/Podstawy penstestingu (DW)	30	16	2
Systemy i technologie w cyberbezpieczeństwie	30	16	2
Elementy kryptologii	30	16	2
Audyt bezpieczeństwa sieci teleinformatycznych	30	16	2
Informatyka śledcza	30	16	2
Razem	**680**	**420**	**73**

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 (t.j. Dz. U. z 2024 r. poz. 1606) 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, kontekst				
	CYB_WG01	Zna i rozumie w stopniu zaawansowanym charakter, miejsce i rolę współczesnych dyscyplin z dziedziny nauk społecznych, w szczególności nauk o polityce i administracji oraz nauk o bezpieczeństwie, 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 powiązaniu z ich miejscem i znaczeniem w systemie cyberbezpieczeństwa. Posiada w stopniu zaawansowanym wiedzę o państwie, władzy, polityce, administracji oraz prawie i zasadach funkcjonowania systemu politycznego, rozumie znaczenie norm i instytucji bezpieczeństwa narodowego i międzynarodowego.	P6U_W	P6S_WG
	CYB_WG03	Ma wiedzę na temat regulacji prawnych związanych z cyberbezpieczeństwem i zapewnieniem ochrony danych osobowych, informacji, zna zasady funkcjonowania krajowego systemu cyberbezpieczeństwa oraz rozwiązań międzynarodowych w tym zakresie, a także zna ich zastosowania praktyczne.	P6U_W	P6S_WG
	CYB_WG04	Zna i rozumie kierunki rozwoju i kompetencje członków społeczeństwa informacyjnego, orientuje się w jego kodach kulturowych i komunikacyjnych. Zna i rozumie zagrożenia, wyzwania wynikające z funkcjonowania w świecie cyfrowym i ich wpływ na współczesne państwa, społeczeństwo, jednostki oraz organizacje publiczne i prywatne.	P6U_W	P6S_WG
	CYB_WG05	Zna i rozumie w stopniu zaawansowanym znaczenie komunikacji za pomocą technologii cyfrowych dla bezpieczeństwa narodowego i międzynarodowego. Ma zaawansowaną wiedzę na temat przygotowania i prowadzenia, a także przeciwdziałania skutkom operacji informacyjnych w cyberprzestrzeni.	P6U_W	P6S_WG
	CYB_WG06	Ma wiedzę na temat programowania, zapewniania bezpieczeństwa sieci i systemów komputerowych, operacyjnych oraz aplikacji. Zna i rozumie zasady zarządzania bezpieczeństwem informacji i danych osobowych, w różnych systemach bezpieczeństwa, a także rozumie ich zastosowania w praktyce zawodowej.	P6U_W	P6S_WG

	CYB_WG07	Zna zasady tworzenia i rozwoju różnych form przedsiębiorczości, ochrony własności intelektualnej oraz zarządzania bezpieczeństwem w działalności zawodowej.	P6U_W	P6S_WG P6S_WK
	CYB_WG08	Zna i rozumie zasady etyczne związane z działalnością zawodową specjalisty z zakresu nauk o polityce i administracji, bezpieczeństwie i informatyce.	P6U_W	P6S_WG P6S_WK
W ZAKRESIE UMIEJĘTNOŚCI				
UMIEJĘTNOŚCI – wykorzystanie wiedzy, komunikowanie się, uczenie się				
	CYB_UW01	Potrafi wykorzystywać posiadaną wiedzę, identyfikując i rozwiązując problemy w działalności zawodowej, w obszarach związanych z naukami o polityce i administracji, naukami o bezpieczeństwie i informatyce.	P6U_U	P6S_UW
	CYB_UW02	Potrafi, korzystając z właściwych metod i narzędzi, w tym zaawansowanych technik informacyjno-komunikacyjnych, pozyskiwać informacje z właściwych źródeł, dokonywać ich oceny, krytycznej analizy i syntezy, w celu rozwiązania złożonych problemów związanych z działalnością zawodową w obszarze cyberbezpieczeństwa.	P6U_U	P6S_UW
	CYB_UK03	Potrafi komunikować się z otoczeniem, w tym posługiwać się w praktyce specjalistyczną terminologią z zakresu bezpieczeństwa i cyberbezpieczeństwa w działalności zawodowej.	P6U_U	P6S_UK
	CYB_UK04	Potrafi przygotować i przedstawić wypowiedź pisemną na temat związany z kierunkiem studiów, potrafi zabrać głos w debacie przedstawiając swoją opinię, stanowisko oraz dyskutować o nich.	P6U_U	P6S_UK
	CYB_UK05	Potrafi posługiwać się wybranym językiem obcym na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego.	P6U_U	P6S_UK
	CYB_UO06	Potrafi planować i organizować pracę indywidualną oraz w ramach zespołu, w tym gotów jest współdziałać z innymi w zespołach, także o charakterze interdyscyplinarnym.	P6U_U	P6S_UO
	CYB_UU07	Potrafi samodzielnie planować i realizować własne uczenie się przez całe życie w celu podnoszenia kompetencji zawodowych i społecznych.	P6U_U	P6S_UU
W ZAKRESIE KOMPETENCJI SPOŁECZNYCH				
KOMPETENCJE – oceny – krytyczne podejście, odpowiedzialność, rola zawodowa				
	CYB_KK01	Jest gotowy do krytycznej oceny wiarygodności różnych źródeł informacji, a także potrafi odpowiedzialnie ocenić granice swoich kompetencji zawodowych i rozumie potrzebę zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązywaniem problemów zawodowych.	P6U_K	P6S_KK
	CYB_KK02	Jest świadomy granic swoich kompetencji oraz konieczności ciągłego rozwijania się poprzez poszerzanie swojej wiedzy, nawiązywanie nowych relacji oraz ustawiczne udoskonalanie umiejętności w zakresie bezpieczeństwa cyfrowego	P6U_K	P6S_KK
	CYB_KO03	Jest świadomy społecznej roli absolwenta tego kierunku studiów, w szczególności odpowiedzialności za konsekwencje swojej działalności zawodowej. Rozumie potrzebę przekazywania społeczeństwu informacji na temat cyberbezpieczeństwa, a także jest gotowy do działania na rzecz interesu publicznego w zakresie bezpieczeństwa cyfrowego.	P6U_K	P6S_KO
	CYB_KO04	Potrafi myśleć i działać w sposób przedsiębiorczy w obszarze cyberbezpieczeństwa.	P6U_K	P6S_KO
	CYB_KR05	Ma świadomość znaczenia pracy własnej i konieczności przestrzegania zasad etyki zawodowej, wymaga tego również od innych. Jest gotowy do podejmowania działań w celu zachowania dorobku i tradycji zawodu.	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** *Occupational Health & Safety Training*	**ECTS: 0**
CYB_WG01 CYB_UW01 CYB_UU07 CYB_KK02	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** *Academic Skills*	**ECTS: 1**
CYB_WG01 CYB_UW02 CYB_UK04 CYB_KK01 CYB_KO03	System edukacji w Polsce, funkcjonowanie uczelni wyższych w Polsce. Charakterystyka uczelni, struktura i pracownicy. Omówienie statutu uczelni oraz regulaminu studiów. Sposoby pozyskiwania informacji oraz komunikowania się na uczelni (w tym sporządzanie podstawowych pism, e–maili), zachowanie się na uczelni. Przygotowanie referatu, prezentacji, projektu, kazusu, eseju, pracy projektowej lub dyplomowej, w tym wyjaśnienie różnicy pomiędzy cytowaniem a bezprawnym wykorzystaniem cudzego tekstu. Dbałość o prawa autorskie i prawa pokrewne.	
Kierunkowe efekty uczenia się	**Wstęp do nauki o państwie i prawie** *Introduction to the study of state and law*	**ECTS: 5**
CYB_WG02 CYB_WG03 CYB_UW01 CYB_KR05	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 filozofii**	**ECTS: 5**

	Foundations of Philosophy	
CYB_WG01 CYB_WG08 CYB_UW01 CYB_KK01	Przedmiot i działy filozofii. Źródła filozofii. Różnice i podobieństwa pomiędzy filozofią a zdrowym rozsądkiem, religią, ideologią, sztuką. Filozofia europejska a orientalna myśl filozoficzna. Historia filozofii. Podstawowe problemy filozoficzne. Omówienie przedmiotu i zakresu ontologii, epistemologii, aksjologii i antropologii filozoficznej. Podstawowe lektury filozoficzne.	
Kierunkowe efekty uczenia się	**Podstawy komunikacji społecznej** *Foundations of Social Communication*	**ECTS: 4**
CYB_WG01 CYB_WG04 CYB_WG05 CYB_UK03 CYB_KO03	Zdefiniowanie podstawowych pojęć. Schemat aktu komunikowania i jego elementy. Rodzaje komunikacji społecznej. Poziomy komunikowania. Funkcje komunikowania. Komunikacja w organizacji, komunikacja w zespole. Komunikowanie a inkluzja. Zasady budowania dostępności informacyjno-komunikacyjnej. Media i komunikowanie masowe. Stare i nowe media. Edukacja medialna, kompetencje medialne.	
Kierunkowe efekty uczenia się	**Własność intelektualna** Intellectual Property	**ECTS: 5**
CYB_WG03 CYB_WG07 CYB_UW02 CYB_KR05	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	**Podstawy ekonomii** *Fundamentals of Economics*	**ECTS: 5**
CYB_WG01 CYB_WG02 CYB_UW01 CYB_KO04	Podstawowe kategorie ekonomiczne. Ograniczoność zasobów i rzadkość ekonomiczna. Klasyfikacja dóbr i czynników produkcji. Krzywa możliwości produkcyjnych. Podmioty gospodarcze. Gałęzie ekonomii. Ekonomia pozytywna i normatywna. Historia myśli ekonomicznej. Współczesne nurty ekonomii. Problemy społeczne w gospodarce. Wzrost i rozwój gospodarczy: mierniki i modele. Wyzwania współczesnej ekonomii: globalizacja, cyfryzacja, zrównoważony rozwój i nierówności; przyszłość nauk ekonomicznych oraz ich wymiar etyczny.	
Kierunkowe efekty uczenia się	**Wychowanie fizyczne** *Physical education*	**ECTS: 0**
CYB_WG01 CYB_UU07 CYB_KK02	Zasady BHP na zajęciach wychowania fizycznego. Regulamin korzystania z obiektu sportowego. Trening zdrowotny. Formy aktywności ruchowej przy muzyce - aerobik, TBC, joga. Ćwiczenia kształtujące sylwetkę z wykorzystaniem sprzętu fitness. Zespołowe gry sportowe. Zajęcia aerobowe. Rodzaje zajęć aerobowych. Tenis stołowy - nauka i doskonalenie wykonania podstawowych elementów technicznych. Elementy tańca towarzyskiego.	
Kierunkowe efekty uczenia się	**Język obcy – Język angielski** *Foreign Language – English*	**ECTS: 9**
CYB_UK04 CYB_UK05 CYB_UO06	Liczba godzin poświęcona poszczególnym sprawnościom, umiejętnościom i podsystemom języka będzie uzależniona od indywidualnych potrzeb grupy. Ogólny zakres leksykalny. Tematyka tekstów oraz zadań językowych w ramach nauki ogólnego języka obcego: dane osobowe; dom, mieszkanie, otoczenie; życie codzienne, czas wolny, rozrywka; podróżowanie i turystyka; stosunki międzyludzkie; zdrowie i higiena; edukacja; praca;	

	kultura; sport; nauka i technika; świat przyrody; zakupy i usługi; żywienie; państwo i społeczeństwo; język. Funkcje językowe. Rozwijanie różnych funkcji językowych, a w szczególności: opisywanie; opowiadanie; wyrażanie opinii; pytanie o informacje, udzielanie informacji; rozwiązywanie nieporozumień (wyjaśnianie); udzielanie rad, ostrzeżeń; telefonowanie; przepraszanie; wydawanie poleceń; wyrażanie próśb; instruowanie; zwroty grzecznościowe. Zagadnienia gramatyczne. Zagadnienia gramatyczne odrębne dla każdego nauczanego języka, typowe dla poziomu B2. Sprawności językowe. Rozwijanie czterech podstawowych sprawności językowych w sposób częściowo zintegrowany: słuchanie, mówienie, czytanie, pisanie.	
Kierunkowe efekty uczenia się	**Język obcy – Język niemiecki** *Foreign Language – German*	**ECTS: 9**
CYB_UK04 CYB_UK05 CYB_UO06	Liczba godzin poświęcona poszczególnym sprawnościom, umiejętnościom i podsystemom języka będzie uzależniona od indywidualnych potrzeb grupy. Ogólny zakres leksykalny. Tematyka tekstów oraz zadań językowych w ramach nauki ogólnego języka obcego: dane osobowe; dom, mieszkanie, otoczenie; życie codzienne, czas wolny, rozrywka; podróżowanie i turystyka; stosunki międzyludzkie; zdrowie i higiena; edukacja; praca; kultura; sport; nauka i technika; świat przyrody; zakupy i usługi; żywienie; państwo i społeczeństwo; język. Funkcje językowe. Rozwijanie różnych funkcji językowych, a w szczególności: opisywanie; opowiadanie; wyrażanie opinii; pytanie o informacje, udzielanie informacji; rozwiązywanie nieporozumień (wyjaśnianie); udzielanie rad, ostrzeżeń; telefonowanie; przepraszanie; wydawanie poleceń; wyrażanie próśb; instruowanie; zwroty grzecznościowe. Zagadnienia gramatyczne. Zagadnienia gramatyczne odrębne dla każdego nauczanego języka, typowe dla poziomu B2. Sprawności językowe. Rozwijanie czterech podstawowych sprawności językowych w sposób częściowo zintegrowany: słuchanie, mówienie, czytanie, pisanie.	
Kierunkowe efekty uczenia się	**Metodologia badań naukowych** *Methodology of Scientific Research*	**ECTS: 4**
CYB_WG01 CYB_UW02 CYB_KK01	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** *Jurisprudence*	**ECTS: 5**
CYB_WG02 CYB_WG03 CYB_UW01 CYB_KR05	Pojęcie nauk prawnych, jurysprudencji, teorii i filozofii prawa oraz prawoznawstwa. Specyfika przedmiotu, problemów i metod badawczych w naukach prawnych. Prawo a moralność. Prawo a inne normy społeczne. Funkcje prawa. Funkcja performatywna języka prawnego. Koncepcja prawa naturalnego - założenia ogólne. Koncepcja pozytywizmu prawniczego - założenia ogólne. Znaczenie logiki formalnej w legislacji i rozumowaniach prawniczych. Teoria argumentacji prawniczej. Ekonomiczna analiza prawa. Charakterystyka i budowa norm prawnych. Norma prawna a przepis prawa. Zasady techniki prawodawczej. Pojęcie systemu prawa. Struktura systemu prawa. Niezgodność formalna w systemie praw. Luka w prawie. Wykładnia prawa. Teorie wykładni. Wykładnia prawa a wnioskowania prawnicze. Domniemania prawnicze i rola. Źródła prawa. Źródła poznania prawa; źródła powstania prawa. Źródła prawa UE. Godność, jako prawnonaturalne źródło praw i wolności w Konstytucji RP	
Kierunkowe efekty uczenia się	**Podstawy socjologii** *Fundamentals of Sociology*	**ECTS: 4**
CYB_WG01 CYB_UW01 CYB_KK02	Socjologia, podstawowe terminy: struktura społeczna, status, rola. Stratyfikacja społeczna i klasy społeczne, podklasa, deprywacja społeczna. Czym jest nowoczesność i późna nowoczesność, patologie nowoczesności. Globalizacja i jej konsekwencje. Socjologiczne pojęcie kultury. Zmiana społeczno-kulturowa. Co oznacza życie w społeczeństwie wielokulturowym. Rasa i etniczność. Naród i nacjonalizm. Religia we współczesnym świecie. Przemiany rodziny. Osobowość i kultura. Rola tożsamości. Nowe i stare ruchy społeczne. Socjologia edukacji..	

Kierunkowe efekty uczenia się	**Zarządzanie projektami** *Project Management*	**ECTS: 3**
CYB_WG05 CYB_WG07 CYB_UK03 CYB_UO06 CYB_KO04 CYB_KR05	Podstawowe pojęcia: projekt, portfel projektów, program, zakres projektu, interesariusze projektu, typowe problemy projektów, projekt w różnych typach organizacji. Procesy zarządzania projektem. Etyka w zarządzaniu projektami. Obszary zarządzania projektami. Krytyczne czynniki sukcesu projektu, przyczyny porażek w realizacji projektów, zapobieganie niepowodzeniom. Budowanie zespołu projektowego. Monitoring i ewaluacja projektów: system raportowania, elektroniczne bazy danych.	

2. KSZTAŁCENIE KIERUNKOWE

Kierunkowe efekty uczenia się	**Wprowadzenie do nauk o bezpieczeństwie** *Introduction to Security Studies*	**ECTS: 5**
CYB_WG01 CYB_WG02 CYB_UK03 CYB_UK04 CYB_UO06 CYB_KK01	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	**Administracja publiczna** *Public Administration*	**ECTS: 5**
CYB_WG02 CYB_UW01 CYB_UK04 CYB_UO06 CYB_UK03 CYB_KK02	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	**Polityka cyberbezpieczeństwa państwa** *The state's cybersecurity policy*	**ECTS: 3**
CYB_WG03 CYB_WG08 CYB_UW01 CYB_UK04 CYB_UO06 CYB_KO03	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	**Problemy bezpieczeństwa społeczeństwa informacyjnego** *Problems of information society security*	**ECTS: 4**
CYB_WG03 CYB_WG08 CYB_UW01 CYB_UK04 CYB_UO06 CYB_KO03	Społeczeństwo informacyjne. Współczesne potrzeby komunikacji społecznej w zakresie ochrony informacji niejawnych. Komunikacja międzykulturowa w zakresie informacji niejawnych. Podstawy organizacji ochrony informacji niejawnych. Grupy społeczne a bezpieczeństwo osobowe – problemy bezpieczeństwa społeczeństwa informacyjnego. Komunikacja społeczna w zakresie bezpieczeństwa teleinformatycznego – problemy bezpieczeństwa społeczeństwa informacyjnego. Komunikacja społeczna w zakresie bezpieczeństwa przemysłowego – problemy bezpieczeństwa społeczeństwa informacyjnego. Organizacja współczesnej komunikacji społecznej -dezinformacja.	
Kierunkowe efekty uczenia się	**Międzynarodowe stosunki polityczne** *International Political Relations*	**ECTS: 4**
CYB_WG02 CYB_UW01 CYB_KK01	Przedmiot i zakres międzynarodowych stosunków politycznych. Uczestnicy międzynarodowych stosunków politycznych. Ewolucja ładu międzynarodowego w XXI wieku. Główne wyzwania i zagrożenia w międzynarodowych stosunkach politycznych. Prawnoinstytucjonalne ramy i aktywności na rzecz bezpieczeństwa międzynarodowego. Kultura i zagadnienia społeczne w międzynarodowych stosunkach politycznych. Procesy globalizacji a stosunki międzynarodowe. Regionalizm w stosunkach międzynarodowych. Główni aktorzy stosunków międzynarodowych.	
Kierunkowe efekty uczenia się	**Wstęp do cyberbezpieczeństwa** *Introduction to Cybersecurity*	**ECTS: 4**
CYB_WG03 CYB_WG07 CYB_UU07 CYB_KK02	Informacja i społeczeństwo informacyjne. Wprowadzenie do problematyki sieci. Strategie cyberbezpieczeństwa. Cyberwojny - nowe formy konfliktów. Narzędzia konfliktu w cyberprzestrzeni. Zarządzanie bezpieczeństwem informacji. Kultura bezpieczeństwa w cyberprzestrzeni	
Kierunkowe efekty uczenia się	**Zarządzanie w sytuacjach kryzysowych** *Management in crisis situations*	**ECTS: 4**
CYB_WG02 CYB_WG05 CYB_WG07 CYB_UW02 CYB_UK04 CYB_UO06 CYB_KO03	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	**Architektura systemów komputerowych i systemy operacyjne** *Computer Systems Architecture and Operating Systems*	**ECTS: 4**
CYB_WG06 CYB_WG08 CYB_UW02 CYB_UK04	Podstawy architektury systemów komputerowych (modele, struktura i działanie systemu komputerowego). Reprezentacja danych i systemy liczbowe (binarny, oktalny, heksadecymalny, IEEE-754). Podstawy logiki cyfrowej (algebra Boole'a, funkcje logiczne, minimalizacja). Układy cyfrowe (kombinacyjne i sekwencyjne – przerzutniki, rejestry, liczniki). Architektura i działanie mikroprocesorów (rejestry, tryby adresowania, wykonywanie rozkazów). Programowanie niskopoziomowe (assembler, operacje na danych, sterowanie programem, przerwania). Organizacja i zarządzanie pamięcią	

CYB_UO06 CYB_UU07 CYB_KR05	(hierarchia pamięci, pamięć wirtualna, stronicowanie, segmentacja). Podstawy systemów operacyjnych (procesy, wątki, zarządzanie zasobami). Synchronizacja i komunikacja międzyprocesowa (semafory, mutexy, IPC). Bezpieczeństwo systemów operacyjnych (kontrola dostępu, ochrona zasobów, mechanizmy bezpieczeństwa)	
Kierunkowe efekty uczenia się	**Przestępczość w cyberprzestrzeni** *Cybercrime*	**ECTS: 3**
CYB_WG02 CYB_WG08 CYB_UW02 CYB_UK04 CYB_UO06 CYB_KO03 CYB_KR05	Przedmiot poświęcony jest systematyce i charakterystyce przestępczości komputerowej oraz internetowej w ujęciu prawnokarnym i kryminologicznym. Omawiane są najważniejsze kategorie cyberprzestępstw: włamania do systemów informatycznych, kradzież danych, oszustwa internetowe, ataki DDoS, ransomware, przestępstwa przeciwko prywatności oraz materiały dotyczące wykorzystywania seksualnego dzieci. Studenci poznają przepisy Kodeksu karnego dotyczące przestępczości komputerowej, a także Konwencję Rady Europy o cyberprzestępczości (Konwencję Budapeszteńską) i dyrektywy unijne w tym zakresie. Kurs uwzględnia analizę działalności grup cyberprzestępczych, modelu Crime-as-a-Service oraz metod dochodzeniowych stosowanych przez organy ścigania. Absolwent rozumie specyfikę ścigania przestępstw popełnianych w środowisku cyfrowym, w tym problematykę jurysdykcji i współpracy międzynarodowej.	
Kierunkowe efekty uczenia się	**System bezpieczeństwa państwa** *The state's security system*	**ECTS: 3**
CYB_WG02 CYB_UK03 CYB_UK04 CYB_UO06 CYB_UW01 CYB_KK01	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. 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	**Operacje informacyjne i oddziaływanie kognitywne** *Information operations and cognitive influence*	**ECTS: 3**
CYB_WG02 CYB_UK03 CYB_UK04 CYB_UO06 CYB_UW01 CYB_KK01	Zagrożenia asymetryczne, informacyjne i hybrydowe w teorii stosunków międzynarodowych oraz w nauce o bezpieczeństwie. Podmioty stosunków międzynarodowych stanowiące zagrożenie w bezpieczeństwie informacji. Procesy globalizacyjne i postęp technologiczny a konflikty zbrojne. 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.	
Kierunkowe efekty uczenia się	**Wstęp do programowania** *Introduction to Programming*	**ECTS: 4**
CYB_WG06 CYB_WG08 CYB_UW01 CYB_UK04 CYB_UO06	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.	

CYB_UU07 CYB_KK02	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	**Bezpieczeństwo aplikacji** *Application security*	**ECTS: 4**
CYB_WG06 CYB_WG08 CYB_UW01 CYB_UK04 CYB_UO06 CYB_KO03	Kurs wprowadza studentów w zagadnienia bezpiecznego projektowania, implementacji i testowania oprogramowania. Omawiane są najczęściej występujące podatności aplikacyjne sklasyfikowane według standardów OWASP Top 10, takie jak wstrzykiwanie kodu SQL, cross-site scripting (XSS), nieprawidłowa autoryzacja czy błędna konfiguracja zabezpieczeń. Studenci poznają metodyki Secure Software Development Lifecycle (SSDLC) oraz narzędzia do automatycznej analizy bezpieczeństwa kodu źródłowego (SAST/DAST). Przedmiot uwzględnia aspekty prawne związane z odpowiedzialnością producentów oprogramowania, wymogami certyfikacyjnymi oraz regulacjami sektorowymi (np. PCI DSS). Ćwiczenia praktyczne obejmują identyfikację i eksploitację wybranych podatności w kontrolowanym środowisku laboratoryjnym.	
Kierunkowe efekty uczenia się	**Bezpieczeństwo sieci komputerowych** *Computer network security*	**ECTS: 4**
CYB_WG06 CYB_WG08 CYB_UW01 CYB_UK03 CYB_UK04 CYB_UO06 CYB_KO03	Przedmiot obejmuje fundamentalne zagadnienia z zakresu ochrony infrastruktury sieciowej przed nieautoryzowanym dostępem, podsłuchem i atakami sieciowymi. Studenci zapoznają się z architekturą sieci TCP/IP, protokołami sieciowymi oraz mechanizmami ich podatności na ataki (sniffing, spoofing, man-in-the-middle, ataki na DNS). Kurs obejmuje zagadnienia konfiguracji i zarządzania zaporami ogniowymi (firewall), systemami wykrywania i zapobiegania włamaniom (IDS/IPS), sieciami VPN oraz segmentacją sieci. Omawiana jest ochrona sieci bezprzewodowych (WiFi, WPA3) oraz zagadnienia bezpieczeństwa w protokołach warstwy aplikacji (HTTP/S, SMTP, FTP). Przedmiot uwzględnia obowiązujące standardy i normy dotyczące bezpieczeństwa sieci (ISO 27033, NIST) oraz wymogi regulacyjne nakładane na operatorów infrastruktury krytycznej.	
Kierunkowe efekty uczenia się	**Podstawy pentestingu** *The basics of penetration testing*	**ECTS: 28**
CYB_WG06 CYB_WG08 CYB_UW01 CYB_UK04 CYB_UO06 CYB_KK02	Kurs wprowadza w metodologię etycznego hakowania i testów penetracyjnych jako narzędzia weryfikacji bezpieczeństwa systemów informatycznych. Omawiane są etapy procesu pentestingu: rekonesans, skanowanie, enumeracja, eksploitacja podatności oraz raportowanie wyników. Studenci zapoznają się z popularnymi narzędziami używanymi przez testerów bezpieczeństwa (Kali Linux, Metasploit, Nmap, Burp Suite) oraz metodykami branżowymi PTES, OWASP Testing Guide i OSSTMM. Przedmiot kładzie szczególny nacisk na aspekty prawne działalności pentesterów, w tym kwestię umów, zakresu autoryzacji oraz odpowiedzialności karnej za nieuprawniony dostęp do systemów. Ćwiczenia laboratoryjne przeprowadzane są wyłącznie na dedykowanych środowiskach testowych, z zachowaniem zasad etyki zawodowej.	
Kierunkowe efekty uczenia się	**Programowanie** *Programming*	**ECTS: 3**
CYB_WG06	Przedmiot zapewnia studentom kierunku cyberbezpieczeństwo praktyczną znajomość programowania niezbędną do zrozumienia i analizy oprogramowania złośliwego, automatyzacji zadań bezpieczeństwa oraz tworzenia narzędzi diagnostycznych. Kurs obejmuje podstawy wybranego	

CYB_WG08 CYB_UW01 CYB_UK04 CYB_UO06 CYB_UU07 CYB_KK02	języka programowania (Python lub podobny), ze szczególnym uwzględnieniem zagadnień istotnych z perspektywy bezpieczeństwa: operacji na plikach i procesach, komunikacji sieciowej, przetwarzania danych oraz pisania skryptów. Studenci uczą się czytać i analizować kod źródłowy w celu identyfikacji podatności oraz rozumieć działanie prostych exploitów i malware. Omawiane są dobre praktyki pisania bezpiecznego kodu oraz typowe błędy programistyczne prowadzące do powstania luk bezpieczeństwa. Przedmiot stanowi fundament dla dalszych kursów z zakresu analizy złośliwego oprogramowania i informatyki śledczej.	
Kierunkowe efekty uczenia się	**Dostęp do informacji publicznej i ochrona informacji niejawnych** *Access to public information and the protection of undisclosed information*	**ECTS: 3**
CYB_WG03 CYB_WG05 CYB_WG08 CYB_UW01 CYB_UK04 CYB_UO06 CYB_KO03	Pojęcie informacji, sposoby klasyfikowania informacji, ocena wiarygodności informacji. Konkretyzacja prawa dostępu do informacji publicznej: charakterystyka ustawy o dostępie do informacji publicznej, pojęcie sprawy publicznej, pojęcie informacji publicznej i informacji przetworzonej. Procedury udostępniania informacji publicznej. Biuletyn Informacji Publicznej. Wnioskowy tryb udzielania informacji publicznej. Ograniczenie dostępu do informacji publicznej: ochrona tajemnic ustawowo chronionych, prywatność osoby fizycznej, tajemnica przedsiębiorcy. Ponowne wykorzystanie informacji publicznej. Ochrona informacji niejawnych: pojęcie informacji niejawnych, klasyfikowanie informacji niejawnych. Organizacja ochrony informacji niejawnych: podmiotowy zakres obowiązku ochrony informacji niejawnych, służby ochrony państwa, pion ochrony informacji niejawnych, kancelarie tajne. Dostęp do informacji niejawnych: zasady udostępniania informacji niejawnych, postępowanie sprawdzające.	
Kierunkowe efekty uczenia się	**Zarządzanie bezpieczeństwem informacji w przedsiębiorstwie** *Information Security Management in a Business*	**ECTS: 3**
CYB_WG03 CYB_WG07 CYB_WG08 CYB_UK03 CYB_UK04 CYB_UO06 CYB_KO04	Kurs poświęcony jest budowie, wdrożeniu i utrzymaniu systemu zarządzania bezpieczeństwem informacji (ISMS) w organizacji komercyjnej. Studenci zapoznają się z normą ISO/IEC 27001 jako podstawowym standardem zarządzania bezpieczeństwem informacji oraz powiązanymi normami serii ISO 27000. Omawiane są procesy analizy ryzyka, doboru i wdrażania zabezpieczeń, zarządzania incydentami bezpieczeństwa oraz ciągłością działania (BCM/BCP). Przedmiot uwzględnia aspekty prawne i regulacyjne, w tym wymagania RODO dotyczące bezpieczeństwa przetwarzania danych osobowych, sektorowe regulacje finansowe (DORA) oraz obowiązki wynikające z dyrektywy NIS2. Studenci nabywają kompetencje niezbędne do pełnienia roli inspektora ochrony danych (IOD) lub menadżera ds. bezpieczeństwa informacji (CISO) w środowisku korporacyjnym.	
Kierunkowe efekty uczenia się	**Systemy i technologie w cyberbezpieczeństwie** *Cybersecurity Systems and Technologies*	**ECTS: 4**
CYB_WG03 CYB_WG06 CYB_UW01 CYB_UK04 CYB_UO06 CYB_UU07 CYB_KR05	Technologie bezpieczeństwa stosowane w systemach informatycznych instytucji publicznych i prywatnych.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	**Technologie sieciowe**	**ECTS: 4**

	Network Technologies	
CYB_WK03 CYB_WG06 CYB_WG08 CYB_UW01 CYB_UK04 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	**Elementy kryptologii** *Elements of Cryptology*	**ECTS: 4**
CYB_WG06 CYB_WG08 CYB_UW01 CYB_UK04 CYB_UO06 CYB_KK02 CYB_KO03	Przedmiot wprowadza studentów w matematyczne i praktyczne podstawy kryptologii i kryptografii jako narzędzia ochrony poufności, integralności i autentyczności danych. Omawiane są symetryczne i asymetryczne algorytmy szyfrowania (AES, RSA, ECC), funkcje skrótu (SHA-2/3), podpisy cyfrowe oraz protokoły uzgadniania kluczy (Diffie-Hellman). Studenci poznają infrastrukturę klucza publicznego (PKI), certyfikaty cyfrowe i protokoły bezpiecznej komunikacji (TLS/SSL). Kurs obejmuje również zagadnienia kryptoanalizy, historii kryptografii oraz współczesnych zagrożeń dla algorytmów kryptograficznych, w tym wpływu obliczeń kwantowych. Przedmiot uwzględnia regulacje prawne dotyczące stosowania kryptografii w Polsce i UE, w tym przepisy o podpisie elektronicznym (eIDAS) oraz ograniczenia eksportowe.	
Kierunkowe efekty uczenia się	**Podstawy technologii chmurowych** *The basics of cloud technology*	**ECTS: 3**
CYB_WG03 CYB_WG06 CYB_UW01 CYB_UK03 CYB_UK04 CYB_UO06 CYB_KO03	Kurs omawia architekturę, modele usługowe (IaaS, PaaS, SaaS) i modele wdrożeniowe (chmura publiczna, prywatna, hybrydowa) platform chmurowych oraz wynikające z nich implikacje dla bezpieczeństwa informacji. Studenci zapoznają się z głównymi dostawcami usług chmurowych (AWS, Azure, Google Cloud) i mechanizmami zabezpieczeń oferowanymi przez te platformy, w tym zarządzaniem tożsamością i dostępem (IAM), szyfrowaniem danych w spoczynku i tranzycie oraz narzędziami monitorowania bezpieczeństwa. Omawiane są zagrożenia specyficzne dla środowisk chmurowych: błędna konfiguracja zasobów, niewłaściwe zarządzanie dostępem oraz podatności wirtualizacji i konteneryzacji. Przedmiot uwzględnia regulacyjny wymiar przetwarzania danych w chmurze, w tym wymagania RODO dotyczące transferu danych do państw trzecich oraz sektorowe regulacje ostrożnościowe. Studenci oceniają ryzyko prawne i operacyjne związane z przyjęciem strategii cloud-first w organizacji.	
Kierunkowe efekty uczenia się	**Podstawy technologii mobilnych i internetu rzeczy (IoT)** *The basics of mobile technology and the Internet of Things (IoT)*	**ECTS: 2**
CYB_WG06 CYB_UW01 CYB_UK03 CYB_UK04 CYB_UO06 CYB_KO03	Przedmiot omawia architekturę i specyfikę bezpieczeństwa systemów mobilnych (Android, iOS) oraz urządzeń i ekosystemów Internetu Rzeczy. Studenci zapoznają się z zagrożeniami charakterystycznymi dla platform mobilnych: złośliwymi aplikacjami, atakami na komunikację bezprzewodową (Bluetooth, NFC, WiFi), phishingiem mobilnym oraz lukami w systemach operacyjnych urządzeń. W zakresie IoT omawiane są podatności wynikające z ograniczonych zasobów obliczeniowych urządzeń, niezabezpieczonych interfejsów sieciowych, słabych mechanizmów uwierzytelniania oraz problemów z aktualizacją oprogramowania układowego (firmware). Kurs uwzględnia regulacje prawne dotyczące certyfikacji bezpieczeństwa urządzeń IoT (Cyber Resilience Act, ETSI EN 303 645) oraz ochrony prywatności użytkowników urządzeń mobilnych. Studenci analizują realne przypadki naruszeń bezpieczeństwa systemów mobilnych i IoT oraz metody ich zapobiegania.	

CYB_KR05		
Kierunkowe efekty uczenia się	**Ethical hacker**	**ECTS: 3**
CYB_WG06 CYB_WG08 CYB_UW01 CYB_UK04 CYB_UO06 CYB_KK02	Wykorzystanie gotowych scenariuszy we współpracy z Cisco Academy, do przeprowadzenia praktycznych warsztatów z zakresu testów penetracyjnych i etycznego hackingu (rola, zakres uprawnień, standardy działania). Metodyka ataku. Identyfikacja podatności w systemach, sieciach i aplikacjach. Techniki obronne i hardening (konfiguracja zabezpieczeń, zarządzanie podatnościami, aktualizacje). Analiza incydentów i reagowanie (zbieranie dowodów, podstawy informatyki śledczej). Dokumentowanie testów i raportowanie (raport pentesterski, rekomendacje naprawcze, zgodność/compliance).	
Kierunkowe efekty uczenia się	**Audyt bezpieczeństwa sieci teleinformatycznych** *IT Network Security Audit*	**ECTS: 4**
CYB_WG06 CYB_WG07 CYB_UK03 CYB_UW02 CYB_UW01 CYB_UK04 CYB_UO06 CYB_KO03 CYB_KR05	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	**Prawo ochrony danych osobowych** *Personal data protection law*	**ECTS: 3**
CYB_WG03 CYB_WG08 CYB_UK03 CYB_UK04 CYB_UO06 CYB_KO03	Przedmiot prawa ochrony danych osobowych. Źródła prawa ochrony danych osobowych. Cele i zakres ochrony danych osobowych. Prawa osób, których dane dotyczą. Ochrona danych osobowych w Polsce w perspektywie standardów Unii Europejskiej. Rozporządzenie ogólne o ochronie danych osobowych (RODO) – zasady przetwarzania danych osobowych według RODO. Obowiązki administratorów i podmiotów przetwarzających dane. Przetwarzanie danych w celu zwalczania i zapobiegania przestępczości. Mechanizmy nadzoru.	
Kierunkowe efekty uczenia się	**Zarządzanie bezpieczeństwem informacji w administracji publicznej** *Information security management in public administration*	**ECTS: 3**
CYB_WG06 CYB_WG07 CYB_UW01 CYB_UK03 CYB_UK04 CYB_UO06 CYB_KO03 CYB_KR05	Kurs koncentruje się na specyfice zarządzania bezpieczeństwem informacji w podmiotach sektora publicznego, uwzględniając odmienne uwarunkowania prawne, organizacyjne i techniczne w stosunku do sektora prywatnego. Studenci zapoznają się z krajowymi i unijnymi regulacjami dotyczącymi cyberbezpieczeństwa administracji publicznej: ustawą o krajowym systemie cyberbezpieczeństwa (KSC), wymaganiami dyrektywy NIS2 dla podmiotów publicznych oraz standardami Krajowych Ram Interoperacyjności (KRI). Omawiane są struktury odpowiedzialne za cyberbezpieczeństwo państwa: CSIRT GOV, CSIRT NASK, CSIRT MON oraz sektorowe zespoły reagowania na incydenty. Przedmiot obejmuje zagadnienia zarządzania informacjami niejawnymi, ochrony danych osobowych w administracji publicznej oraz reagowania na incydenty	

	bezpieczeństwa w podmiotach publicznych. Studenci nabywają kompetencje niezbędne do pracy na stanowiskach ds. bezpieczeństwa informacji w urzędach administracji rządowej i samorządowej.	
Kierunkowe efekty uczenia się	**Metodyka przygotowania projektu** *Project Management Methodology*	**ECTS: 3**
CYB_WG06 CYB_WG07 CYB_WK02 CYB_WK05 CYB_UW04 CYB_UW06 CYB_UO01 CYB_UO02 CYB_UK04 CYB_UO06 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	**Formy prowadzenia działalności gospodarczej** *Types of business activity*	**ECTS: 3**
CYB_WG01 CYB_WG07 CYB_UK04 CYB_UO06 CYB_UU07 CYB_KO04	Prawne pojęcie przedsiębiorstwa, przedsiębiorcy i działalności gospodarczej. Prawne formy prowadzenia działalności gospodarczej. Podjęcie działalności gospodarczej – obowiązki rejestracyjne. Zawieranie umów przez przedsiębiorców. Reprezentacja przedsiębiorcy: organy osób prawnych, pełnomocnictwo i prokura. Obowiązki przedsiębiorcy wobec innych uczestników obrotu.	
Kierunkowe efekty uczenia się	**Podstawy finansów prywatnych i publicznych** *Fundamentals of private and public finance*	**ECTS: 3**
CYB_WG01 CYB_WG07 CYB_UK04 CYB_UO06 CYB_KK01 CYB_KO04	Pojęcie finansów, zakres, systematyka, istota pieniądza – formy, rodzaje, obieg, funkcje finansów. Rodzaje kredytów. Różnica między kredytem a pożyczką. Pojęcie, instrumenty, segmenty rynku finansowego. pojęcia sektora finansów publicznych i jego segmenty, źródła finansowania wydatków publicznych (w tym struktura finansowa sektora), pojęcie, klasyfikacja i rodzaje podatków, dotacje i subwencje, finanse jednostek samorządu terytorialnego. Planowanie finansowe w sektorze finansów publicznych, istota budżetu państwa i charakterystyka procedury budżetowej, analiza budżetu państwa danego roku, istota deficytu budżetowego i sposoby jego finansowania, problematyka długu publicznego (w tym zarządzanie długiem publicznym), polityka finansowa: pojęcie, rodzaje i narzędzia. „Inteligencja finansowa", czynniki odpowiedzialne za tworzenie bogactwa, budżet domowy, zasady wydawania i oszczędzania pieniędzy, dochód aktywny i pasywny. Finanse behawioralne a klasyczna teoria finansów (racjonalność ekonomiczna i zasady efektywnego rynku), anomalie - przykłady. Konstrukcja budżetu UE, wpływy, struktura wydatków, strefa euro. Polska a strefa euro.	

Kierunkowe efekty uczenia się	**Informatyka śledcza** *Digital forensics*	**ECTS: 4**
CYB_WG03 CYB_WG04 CYB_WG06 CYB_UK04 CYB_UO06 CYB_UW02 CYB_KK01	Przedmiot wprowadza w metodologię i techniki cyfrowej analizy śledczej (digital forensics) stosowanej w postępowaniach karnych i cywilnych oraz wewnętrznych dochodzeniach korporacyjnych. Studenci poznają zasady zabezpieczania cyfrowego materiału dowodowego z zachowaniem łańcucha pieczy (chain of custody) oraz jego analizy na nośnikach danych, w systemach operacyjnych, pamięci RAM i sieci. Kurs obejmuje pracę z dedykowanymi narzędziami forensycznymi (Autopsy, Wireshark, Volatility, FTK) oraz standardami dokumentowania wyników analizy na potrzeby postępowania sądowego. Omawiane są regulacje procesowe dotyczące dopuszczalności dowodów cyfrowych w polskim i europejskim porządku prawnym, a także aspekty etyczne pracy biegłego w sprawach informatycznych. Studenci ćwiczą przeprowadzanie kompleksowej analizy śledczej na spreparowanych obrazach dysków i scenariuszach incydentów bezpieczeństwa.	
Kierunkowe efekty uczenia się	**Cyberkultura w XXI w.** *Cyberculture in the 21st Century*	**ECTS: 2**
CYB_WG04 CYB_WG08 CYB_UK04 CYB_UO06 CYB_KO03	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	**Współczesny terroryzm polityczny** *Contemporary Political Terrorism*	**ECTS: 3**
CYB_WG02 CYB_WG05 CYB_UK04 CYB_UO06 CYB_KK02	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 etniczno-narodowy; Terroryzm społeczno – rewolucyjny; Terroryzm islamski; Terroryzm państwowy; Koncepcje przyszłości terroryzmu.	
Kierunkowe efekty uczenia się	**OPSEC w internecie – podstawy anonimizacji w sieci** *OPSEC on the Internet – basics of online anonymization*	**ECTS: 3**
CYB_WG03 CYB_WG05 CYB_WG08 CYB_UW01 CYB_UW02 CYB_UK04 CYB_UO06 CYB_KO03	Kurs omawia zasady bezpieczeństwa operacyjnego (OPSEC) w środowisku cyfrowym, ze szczególnym uwzględnieniem technik i narzędzi służących ochronie prywatności oraz anonimizacji aktywności w sieci. Studenci zapoznają się z mechanizmami śledzenia użytkowników w internecie (ciasteczka, fingerprinting, metadane), technikami anonimizacji (sieci Tor, VPN, I2P) oraz higieną cyfrową jako elementem bezpieczeństwa osobistego i operacyjnego. Kurs obejmuje zastosowania OPSEC w kontekście zawodowym: ochronę dziennikarzy, sygnalistów (whistleblowers), prawników i funkcjonariuszy służb specjalnych. Omawiane są granice prawne korzystania z narzędzi anonimizujących w Polsce i UE, w tym regulacje dotyczące usług VPN, kwestia legalności dostępu do darknetu oraz odpowiedzialność za działania podejmowane anonimowo w sieci. Studenci wypracowują indywidualny model zagrożeń (threat model) i uczą się dostosowywać środki ochrony do konkretnego profilu ryzyka.	
Kierunkowe efekty uczenia się	**Wojna hybrydowa**	**ECTS: 3**

	Hybrid Warfare	
CYB_WG02 CYB_WG05 CYB_UK03 CYB_UK04 CYB_UO06 CYB_KK01	Geneza wojny hybrydowej. Procesy dotyczące problematyki wojny informacyjnej i hybrydowej, definicja i istota wojny hybrydowej, rodzaje wojny hybrydowej, przykłady wojny hybrydowej. Zagrożenia asymetryczne i hybrydowe w teorii stosunków międzynarodowych oraz w nauce o bezpieczeństwie. Podmioty stosunków międzynarodowych stanowiące zagrożenie asymetryczne i hybrydowe. Procesy globalizacyjne i postęp technologiczny a konflikty asymetryczne. Procesy globalizacyjne i postęp technologiczny a konflikty asymetryczne. Wojny hybrydowe – historia i współczesność. Terroryzm międzynarodowy i cyberterroryzm jako przykład zagrożenia asymetrycznego. Główne obszary transnarodowej przestępczości zorganizowanej – handel narkotykami, handel ludźmi, przemyt ludzi, broni i towarów. Wpływ korupcji na bezpieczeństwo państw.	
Kierunkowe efekty uczenia się	**Projekt społeczny** *Social Project*	**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	**Praktyka zawodowa** *Internship*	**ECTS: 28**
CYB_WG03 CYB_WG04 CYB_WG06 CYB_UW01 CYB_UW02 CYB_UK03 CYB_UO06 CYB_KK01 CYB_KK02 CYB_KO03 CYB_KO04 CYB_KR05	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.	

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. wychowanie fizyczne, 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%

Na studiach I stopnia studenci są zobowiązani do zrealizowania w ramach programu studiów projektu społecznego. Wymóg ten wynika z przyjętych przez UAFM naczelnych wartości oraz celów strategicznych, które zakładają upraktycznienie procesu studiowania oraz kształcenie studentów w duchu wartości, jaką jest odpowiedzialność społeczna. Tematy projektów powinny odzwierciedlać wiedzę i umiejętności nabyte przez studenta w toku studiów oraz wykazywać umiejętność praktycznego zastosowania przez studenta wiedzy do rozwiązywania zdiagnozowanego przez siebie problemu praktycznego lub określonej potrzeby społecznej. Realizując projekt społeczny, student jest zobowiązany do tworzenia dokumentacji projektu na wszystkich jego etapach, zgodnie ze wzorami tej dokumentacji opracowanymi przez uczelnię. Student w ramach trwających przez rok zajęć Metodyka przygotowania projektu i Projekt społeczny, pod opieką promotora przygotowuje koncepcję swojego indywidualnego projektu społecznego, plan jego realizacji, przeprowadza działania projektowe oraz dokonuje ewaluacji jego skutków. Po każdym z semestrów tych zajęć student przedstawia promotorowi opisywaną w sylabusach dokumentację poszczególnych etapów pracy projektowej. Dopuszczalny zakres tematyczny projektu jest określany w drodze porozumienia z wykładowcą będącym opiekunem projektu i powinien stanowić praktyczną aplikację wiedzy i umiejętności określonych dyscyplinami, do których przyporządkowany jest kierunek. Przedmiotem projektu społecznego powinno być działanie wykorzystujące w praktyce wiedzę i umiejętności studenta z zakresu cyberbezpieczeństwa, zdobytych w trakcie studiów. Dopuszcza się także realizacje projektów społecznych o charakterze interdyscyplinarnym. Nadzór nad właściwym doborem tematu, zakresu i metod projektu sprawuje wykładowca – opiekun projektu. Projekt społeczny realizowany przez studenta powinien zachowywać ogólną metodologię realizacji projektu. Zastosowane w projekcie metody powinny być adekwatne do zdiagnozowanego problemu oraz zaproponowanego sposobu jego rozwiązania. Na każdym etapie przygotowania i realizacji projektu student dokumentuje podejmowane przez siebie czynności w formie odpowiadającej specyfice projektu i uzgodnionej z promotorem. Podczas zajęć Projekt społeczny na szóstym semestrze, wykorzystując środki multimedialne, student przygotowuje także prezentację, którą będzie przedstawiał w trakcie egzaminu dyplomowego. Projekt społeczny jest oceniany w aspektach formalnych i merytorycznych. Ocena projektu jest dokonywana według uprzednio opracowanych wystandaryzowanych kryteriów. Zaliczenie zajęć Projekt społeczny na semestrze szóstym następuje po zaakceptowaniu przez promotora całości dokumentacji zrealizowanego projektu. Promotor dokonuje oceny projektu danego studenta w oparciu o wyskalowane kryteria, które są

przedstawiane do wiadomości studentów przy rozpoczynaniu zajęć Metodyka przygotowania projektu i Projekt społeczny. Kompleksowa weryfikacja osiągniętych w toku całych studiów efektów uczenia się następuje w drodze procesu dyplomowania i egzaminu dyplomowego, którego celem jest weryfikacja wiedzy i umiejętności oraz kompetencji społecznych studenta zdobytych w toku studiów.

Do egzaminu dyplomowego może zostać dopuszczony student, który spełnia następujące warunki:

• osiągnął wszystkie efekty uczenia się przewidziane w programie studiów;

• uzyskał pozytywne wyniki zaliczeń i egzaminów ze wszystkich przedmiotów i rodzajów zajęć przewidzianych w programie studiów oraz wymaganej łącznej liczby punktów ECTS;

• uregulował wszystkie należne zobowiązania – w tym finansowe – wobec Uczelni;

• złożył wszystkie wymagane dokumenty.

Egzamin dyplomowy jest egzaminem zamkniętym i ma formę ustną. Egzamin przeprowadza komisja egzaminacyjna powoływana przez Dziekana, w skład której wchodzą co najmniej trzy osoby: przewodniczący, promotor oraz członek komisji wyznaczany przez Dziekana spośród nauczycieli akademickich pracujących na kierunku cyberbezpieczeństwo. W składzie komisji powinna znajdować się co najmniej jedna osoba ze stopniem doktora. W wyjątkowych sytuacjach, gdy obecność promotora podczas egzaminu dyplomowego jest niemożliwa, dziekan lub prorektor ds. kształcenia wyznacza do składu komisji nauczyciela akademickiego zatrudnionego w Uczelni jako osobę zastępującą promotora.

Na egzaminie dyplomowym kończącym studia pierwszego stopnia, student dokonuje prezentacji zrealizowanego przez siebie projektu, wykorzystując przygotowaną wcześniej przez siebie prezentację

multimedialną. Każdy z członków komisji ocenia prezentację studenta oraz jego odpowiedzi w zakresie kryteriów obejmujących aspekty treściowe i formalne prezentacji. Egzamin dyplomowy obejmuje trzy pytania, w tym co najmniej dwa z zakresu kierunku (z wykazu pytań ogłoszonego studentom najpóźniej na początku ostatniego semestru studiów) oraz jedno zadawane przez komisję z tematyki zaprezentowanego projektu. Z egzaminu dyplomowego sporządza się protokół, w którym są zapisywane m.in. pytania zadane studentowi, oceny za odpowiedzi na nie, ocena ostateczna egzaminu dyplomowego oraz końcowy wynik studiów. Protokół jest podpisywany przez wszystkich członków komisji i archiwizowany w teczce osobowej studenta.

Zasady i forma odbywania praktyk zawodowych

Ogólne zasady organizacji praktyk zawodowych, wzory niezbędnych dokumentów, zadania opiekunów praktyk oraz tryb zaliczania praktyk określa Regulamin Praktyk Zawodowych w Uniwersytecie Andrzeja Frycza Modrzewskiego w Krakowie. Regulaminie stanowi m.in., iż Uczelnia zapewnia miejsca praktyk dla studentów i zawiera w tej sprawie porozumienie z jednostkami przyjmującymi 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, stażu lub wolontariatu (o ile umożliwia to osiągnięcie efektów uczenia się przewidzianych dla praktyk) oraz w ramach programu ERASMUS+. Obowiązkowym sposobem dokumentacji przebiegu praktyki i realizowanych w jej trakcie zadań jest prowadzony przez studenta „Dzienniczek praktyk". Szczegółowe zasady realizacji praktyk, 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 jednostki, w których odbywają się praktyki, reguły zatwierdzania miejsca praktyki samodzielnie wybranego przez studenta oraz warunki kwalifikowania studenta na praktyki określa Program Praktyk Zawodowych. Celem studenckich praktyk zawodowych jest zaznajomienie studentów z praktycznymi zagadnieniami związanymi z wybranym kierunkiem kształcenia oraz realiami wykonywania zawodu, poprzez umożliwienie zdobycia wiedzy, doświadczeń, umiejętności oraz ukształtowania postaw w rzeczywistych warunkach funkcjonowania podmiotu (przedsiębiorstwa, instytucji lub organizacji).

Nadrzędnymi celami praktyki są:

• Zapoznanie się z organizacją i funkcjonowaniem podmiotu (przedsiębiorstwa, organizacji, instytucji).

• Wykonywanie w warunkach rzeczywistych wybranych prac, zadań lub aktywności typowych dla kierunku kształcenia.

• Analiza i ocena wybranego obszaru działalności podmiotu (przedsiębiorstwa, organizacji, instytucji) oraz ewentualnie zaproponowanie planu naprawczego.

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

- na trzecim semestrze (2 rok studiów) – w wymiarze 180 godz., 7 ECTS
- na czwartym semestrze (2 rok studiów) – w wymiarze 180 godz., 7 ECTS
- na piątym semestrze (3 rok studiów) – w wymiarze 180 godz., 7 ECTS
- na szóstym semestrze (3 rok studiów) – w wymiarze 180 godz. 7 ECTS

Łączny wymiar praktyk wynosi 720 godzin realizowanych. Student uzyskuje łącznie 28 punktów ECTS za zrealizowane praktyki zawodowe.

Student może odbywać praktyki w następujących formach:

- na podstawie skierowania na praktykę do jednostki wskazanej przez uczelnię lub studenta,
- na podstawie wykonywanej pracy zawodowej, odbywanego stażu lub wolontariatu,
- na podstawie prowadzonej działalności gospodarczej.

Treści programowe realizowane podczas praktyki zawodowej powinny odzwierciedlać specyfikę zadań powierzanych w danej organizacji. Podczas praktyki zawodowej student zaznajamia się z zasadami oraz przepisami bezpieczeństwa i higieny pracy obowiązującymi w danej organizacji. Niezależnie od rodzaju organizacji, student podczas praktyki poznaje ogólne cele i zadania realizowane przez organizację oraz – bardziej szczegółowo – obowiązki i zadania pracowników zatrudnionych w danej organizacji. Zapoznaje się z zakresem działań jednostki przyjmującej, z dokumentacją przedsiębiorstwa, statutem, strukturą organizacyjną, przebiegiem procesów pracy oraz – w miarę dostępności – ze strategią i planami rozwoju, programami komputerowymi i wynikami ekonomicznymi itp. W sposób szczególny student poznaje specyficzne dla pracy, metody i narzędzia stosowane w danej organizacji i uczy się praktycznie stosować przynajmniej niektóre z nich pod nadzorem opiekuna zakładowego praktyk. Metody te i narzędzia mogą różnić się w zależności od specyfiki danej organizacji. Student może także zapoznać się z innymi lub interdyscyplinarnymi metodami i narzędziami stosowanymi w organizacji. Student powinien zostać zaznajomiony z zasadami obowiązującymi go podczas wykonywania czynności i zadań zawodowych w relacjach do przełożonych i współpracowników, w tym do innych specjalistów pracujących w danej organizacji. Ponadto student zostanie zaznajomiony z obowiązującymi zasadami, normami i formami pracy potrzebnymi dla prawidłowego funkcjonowania danej organizacji, poznaje ludzi, atmosferę pracy, relacje interpersonalne w tym środowisku, kulturę organizacyjną.

Dzięki praktykom student rozwija umiejętności obserwowania i rozumienia środowiska pracy oraz zasady i zwyczaje, jakie w nim są przyjęte, prawa nieformalne i formalne, jakie nim rządzą. Podczas praktyki zawodowej student powinien zostać zaznajomiony z zasadami etycznymi i przepisami prawnymi regulującymi pracę w danej organizacji i w odniesieniu do konkretnych czynności i zadań powierzanych mu do wykonania, dzięki obserwacji, a następnie stopniowym uczestniczeniu w bieżącej działalności operacyjnej wybranej jednostki organizacyjnej (bądź wybranych jednostek). W trakcie odbywania praktyki zawodowej studentowi należy zapewnić sposobność i możliwość zastosowania wiedzy do rozwiązania konkretnych problemów lub zadań praktycznych. W treściach przekazywanych studentowi należy szczególnie podkreślać związek między wiedzą naukową i jej praktycznym wykorzystaniem. Jednocześnie należy u studenta kształtować postawę pokory i świadomość granic własnych kompetencji zawodowych.

Efekty uczenia się przypisane do praktyk zawodowych na kierunku studiów cyberbezpieczeństwo

Symbol efektu uczenia się	Efekt uczenia się
CYB_WG03	Ma wiedzę na temat regulacji prawnych związanych z cyberbezpieczeństwem i zapewnieniem ochrony danych osobowych, informacji, zna zasady funkcjonowania krajowego systemu cyberbezpieczeństwa oraz rozwiązań międzynarodowych w tym zakresie, a także zna ich zastosowania praktyczne.
CYB_WG04	Zna i rozumie kierunki rozwoju i kompetencje członków społeczeństwa informacyjnego, orientuje się w jego kodach kulturowych i komunikacyjnych. Zna i rozumie zagrożenia, wyzwania wynikające z funkcjonowania w świecie cyfrowym i ich wpływ na współczesne państwa, społeczeństwo, jednostki oraz organizacje publiczne i prywatne.
CYB_WG06	Ma wiedzę na temat programowania, zapewniania bezpieczeństwa sieci i systemów komputerowych, operacyjnych oraz aplikacji. Zna i rozumie zasady zarządzania bezpieczeństwem informacji i danych osobowych, w różnych systemach bezpieczeństwa, a także rozumie ich zastosowania w praktyce zawodowej.
CYB_UW01	Potrafi wykorzystywać posiadaną wiedzę, identyfikując i rozwiązując problemy w działalności zawodowej, w obszarach związanych z naukami o polityce i administracji, naukami o bezpieczeństwie i informatyce.
CYB_UW02	Potrafi, korzystając z właściwych metod i narzędzi, w tym zaawansowanych technik informacyjno- komunikacyjnych, pozyskiwać informacje z właściwych źródeł, dokonywać ich oceny, krytycznej analizy i syntezy, w celu rozwiązania złożonych problemów związanych z działalnością zawodową w obszarze cyberbezpieczeństwa.
CYB_UK03	Potrafi komunikować się z otoczeniem, w tym posługiwać się w praktyce specjalistyczną terminologią z zakresu bezpieczeństwa i cyberbezpieczeństwa w działalności zawodowej.
CYB_UO06	Potrafi planować i organizować pracę indywidualną oraz w ramach zespołu, w tym gotów jest współdziałać z innymi w zespołach, także o charakterze interdyscyplinarnym.
CYB_KK01	Jest gotowy do krytycznej oceny wiarygodności różnych źródeł informacji, a także potrafi odpowiedzialnie ocenić granice swoich kompetencji zawodowych i rozumie potrzebę zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązywaniem problemów zawodowych.
CYB_KK02	Jest świadomy granic swoich kompetencji oraz konieczności ciągłego rozwijania się poprzez poszerzanie swojej wiedzy, nawiązywanie nowych relacji oraz ustawiczne udoskonalanie umiejętności w zakresie bezpieczeństwa cyfrowego
CYB_KO03	Jest świadomy społecznej roli absolwenta tego kierunku studiów, w szczególności odpowiedzialności za konsekwencje swojej działalności zawodowej. Rozumie potrzebę przekazywania społeczeństwu informacji na temat cyberbezpieczeństwa, a także jest gotowy do działania na rzecz interesu publicznego w zakresie bezpieczeństwa cyfrowego.
CYB_KO04	Potrafi myśleć i działać w sposób przedsiębiorczy w obszarze cyberbezpieczeństwa.
CYB_KR05	Ma świadomość znaczenia pracy własnej i konieczności przestrzegania zasad etyki zawodowej, wymaga tego również od innych. Jest gotowy do podejmowania działań w celu zachowania dorobku i tradycji zawodu.