

**Opis poszczególnych przedmiotów lub grup przedmiotów dla studiów podyplomowych
pn. Cyberbezpieczeństwo w ochronie zdrowia prowadzonych na Wydziale Elektrycznym**

1.	Nazwa przedmiotu lub grupy przedmiotu	Cyberbezpieczeństwo
2.	Tryb prowadzenia zajęć (zdalny/stacjonarny)	Stacjonarny (14) / zdalny (14)
3.	Liczba punktów ECTS przypisana do przedmiotu lub grupy przedmiotów	4 (2/2) ECTS
34	Formy prowadzenia zajęć dla przedmiotu lub grupy przedmiotu z przypisaną liczbą godzin	Wykład (28)
5.	Treści programowe dla przedmiotu lub grupy przedmiotów	
<p>Pojęcie cyberbezpieczeństwa Cyberprzestrzeń; sieci, systemy i użytkownicy; systemy cyberfizyczne; współczesne sieci i systemy; wprowadzenie do dziedziny cyberbezpieczeństwa; Pojęcia podstawowe – CIA (Confidentiality, Integrity, Availability); Podatność, zagrożenie, skutek, ryzyko; budowa wielowarstwowego cyberbezpieczeństwa i programy; model dojrzałości i adekwatności środków cyberbezpieczeństwa; analiza ryzyka cyberzagrożeń i powiązanie z różnymi działaniami na rzecz podnoszenia cyberbezpieczeństwa; Zagrożenia dla cyberbezpieczeństwa, bezpieczeństwa informacji i ochrony danych osobowych w ochronie zdrowia. Podstawy prawne zapewnienia cyberbezpieczeństwa, bezpieczeństwa informacji i ochrony danych osobowych w ochronie zdrowia oraz planowane kierunki zmian przepisów; Zagrożenia płynące z cyberprzestrzeni; Problemy etyczne, prawne i ekonomiczne w cyberbezpieczeństwie; Zagrożenia wynikające z łańcuchów dostaw, sieci elektroenergetycznej i fizycznej ochrony obiektów; Ataki i cyberataki na infrastrukturę krytyczną dla jednostki ochrony zdrowia; Modelowanie zagrożeń i ocena ryzyka; Analiza przypadków.</p>		
6.	Formy weryfikacji i oceny osiągniętych efektów kształcenia (warunki i sposób zaliczenia)	
Efekty uczenia się będą weryfikowane przez: rozmowę oceniającą, test wiedzy, dyskusję moderowaną, ocenę zadań problemowych wykonywanych w trakcie zajęć oraz obserwację nauczyciela w warunkach symulowanych.		
7.	Efekty uczenia się przypisane do tych przedmiotów lub grup przedmiotów i ich odniesienie do efektów uczenia się dla programu studiów podyplomowych	
	Symbol efektu uczenia się dla przedmiotu lub grupy przedmiotów	Opis efektu uczenia się dla przedmiotu lub grupy przedmiotów
		Symbol efektu uczenia się dla programu studiów podyplomowych

Wiedza		
COZ_101_W01	ma wiedzę dotyczącą podstawowych pojęć z zakresu cyberbezpieczeństwa.	COZ_W01
COZ_101_W02	ma wiedzę dotyczącą podstawowych pojęć z zakresu infrastruktury krytycznej jednostki ochrony zdrowia	COZ_W02
COZ_101_W03	Zna podstawowe terminy i pojęcia z zakresu usług w służbie zdrowia	COZ_W03
COZ_101_W04	Zna pojęcia i uwarunkowania pozatechniczne działalności inżynierskiej z zakresu cyberbezpieczeństwa	COZ_W04 COZ_W08
COZ_101_W05	ma wiedzę dotyczącą podstawowych pojęć środowiska krytycznej infrastruktury w jednostce ochrony zdrowia	COZ_W03 COZ_W09
Umiejętności		
COZ_101_U01	potrafi krytycznie analizować dostępną literaturę w zakresie podstaw cyberbezpieczeństwa	COZ_U01
COZ_101_U02	potrafi sformułować problemy dotyczące cyberbezpieczeństwa w ochronie zdrowia przy użyciu właściwej terminologii	COZ_U01 COZ_U04
COZ_101_U03	potrafi opisać współczesne problemy cyberbezpieczeństwa w ochronie zdrowia posługując się wybranymi metodami i modelami	COZ_U01 COZ_U05
COZ_101_U04	potrafi opisać współczesne zagrożenia cyberbezpieczeństwa w ochronie zdrowia posługując się wybranymi metodami i modelami w odniesieniu do pojęć z zakresu cyberbezpieczeństwa w ochronie zdrowia	COZ_U08
COZ_101_U05	Potrafi dobrać odpowiedni model cyberbezpieczeństwa w ochronie zdrowia adekwatny do uwarunkowań i zdefiniowanej sytuacji projektowej	COZ_U06
COZ_101_U06	Potrafi wykorzystać wybrane model i narzędzia cyberbezpieczeństwa w ochronie zdrowia do pracy i organizacji zespołu w celu rozwiązania problemów stawianych na zajęciach	COZ_U07 COZ_U08
COZ_101_U07	potrafi aktywnie uczestniczyć w dyskusji na tematy związane z cyberbezpieczeństwem w ochronie zdrowia używając poprawnej terminologii i formułując trafne argumenty	COZ_U01 COZ_U04
Kompetencje społeczne		
COZ_101_K01	ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy	COZ_K03
COZ_101_K02	ma świadomość konieczności stosowania właściwego języka dziedzinowego w komunikacji w zespole i osobami spoza niego	COZ_K04
COZ_101_K03	ma świadomość konieczności stałego aktualizowania i wzbogacania posiadanej wiedzy oraz zdobywania nowych	COZ_K02

	umiejętności w zakresie cyberbezpieczeństwa w ochronie zdrowia	
COZ_101_K04	ma świadomość istotności przekazywania wiedzy na temat metod i narzędzi oraz dobrych praktyk zapewnienia cyberbezpieczeństwa w ochronie zdrowia	COZ_K03
COZ_101_K05	Rozumie potrzebę stosowania dobrych praktyk i sprawdzonych rozwiązań w zapewnieniu cyberbezpieczeństwa w ochronie zdrowia	COZ_K01 COZ_K03

1.	Nazwa przedmiotu lub grupy przedmiotu	Bezpieczeństwo informacji i ochrona danych osobowych
2.	Tryb prowadzenia zajęć (zdalny/stacjonarny)	zdalny
3.	Liczba punktów ECTS przypisana do przedmiotu lub grupy przedmiotów	4 ECTS
4.	Formy prowadzenia zajęć dla przedmiotu lub grupy przedmiotu z przypisaną liczbą godzin	Wykład (16) / Projekt (12)
5.	Treści programowe dla przedmiotu lub grupy przedmiotów	
<p>Ochrona danych osobowych zgodnie RODO i związanym przepisami szczegółowymi dla ochrony zdrowia Znane i często spotykane podatności związane z cyberbezpieczeństwem, bezpieczeństwem informacji i ochroną danych osobowych w ochronie zdrowia Podstawowe zabezpieczenia z zakresu cyberbezpieczeństwa, bezpieczeństwa informacji i ochrony danych osobowych Identyfikacja ryzyka, szacowanie ryzyka, postępowanie z ryzykiem jak podstawowe składowe zarządzania ryzykiem w ochronie zdrowia Kryptografia asymetryczna i symetryczna; kryptografia klucza publicznego; funkcje skrótu; certyfikaty; podpis cyfrowy; mechanizmy kontroli integralności danych; uwierzytelnienie i autoryzacja; ochrona dostępności danych: backupy, redundancja; strategie ochrony danych: klasyfikacja, dane wrażliwe; przegląd mechanizmów wbudowanych w systemy sieciowe, komputerowe, operacyjne oraz aplikacje i bazy danych pod kątem bezpieczeństwa danych; Bezpieczeństwo w systemach operacyjnych; wirtualizacja i maszyny wirtualne; serwery i komunikacja zdalna – SSH Analiza case study Projekt: zapewnienie ochrony danych osobowych w jednostce ochrony zdrowia</p>		
6.	Formy weryfikacji i oceny osiągniętych efektów kształcenia (warunki i sposób zaliczenia)	
<p>Efekty uczenia się będą weryfikowane przez: rozmowę oceniającą, test wiedzy, dyskusję moderowaną, ocenę zadań problemowych wykonywanych w trakcie zajęć oraz obserwację nauczyciela w warunkach symulowanych.</p>		
7.	Efekty uczenia się przypisane do tych przedmiotów lub grup przedmiotów i ich odniesienie do efektów uczenia się dla programu studiów podyplomowych	
	Symbol efektu uczenia się dla przedmiotu lub grupy przedmiotów	Symbol efektu uczenia się dla programu studiów podyplomowych
Wiedza		
	COZ_102_W01	ma wiedzę dotyczącą podstawowych pojęć bezpieczeństwa i ochrony danych osobowych.
	COZ_102_W02	ma wiedzę dotyczącą podstawowych pojęć bezpieczeństwa i ochrony danych medycznych
	COZ_103_W03	Zna podstawowe pojęcia zarządzania bezpieczeństwem i ochroną danych osobowych
	COZ_103_W04	Zna pojęcia i uwarunkowania pozatechniczne działalności inżynierskiej w zakresie bezpieczeństwa i ochrony danych osobowych
	COZ_103_W05	ma wiedzę dotyczącą podstawowych pojęć i narzędzi ochrony informatycznej danych

Umiejętności		
COZ_102_U01	potrafi krytycznie analizować dostępną literaturę w zakresie bezpieczeństwa i ochrony danych osobowych	COZ_U01 COZ_U08
COZ_102_U02	potrafi sformułować problemy dotyczące bezpieczeństwa i ochrony danych osobowych przy użyciu właściwej terminologii	COZ_U01 COZ_U08
COZ_102_U03	potrafi opisać współczesne problemy bezpieczeństwa i ochrony danych osobowych posługując się wybranymi metodami i modelami	COZ_U01 COZ_U07
COZ_102_U04	potrafi opisać współczesne zagrożenia bezpieczeństwa i ochrony danych osobowych posługując się wybranymi metodami i modelami	COZ_U05 COZ_U07
COZ_102_U05	potrafi dobrać odpowiedni model bezpieczeństwa i ochrony danych osobowych adekwatny do uwarunkowań i zdefiniowanej sytuacji projektowej	COZ_U06 COZ_U04
COZ_102_U06	potrafi wykorzystać wybrane model i narzędzia informatyczne do pracy i organizacji zespołu w celu rozwiązania problemów stawianych na zajęciach	COZ_U07
COZ_102_U07	potrafi aktywnie uczestniczyć w dyskusji na tematy związane z bezpieczeństwa i ochrony danych osobowych, używając poprawnej terminologii i formułując trafne argumenty	COZ_U01 COZ_U08
COZ_102_U08	potrafi skutecznie stosować wybrane elementy bezpieczeństwa i ochrony danych osobowych do rozwiązywania problemów praktycznych samodzielnie i w zespole	COZ_U06 COZ_U07
Kompetencje społeczne		
COZ_102_K01	ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy	COZ_K03
COZ_102_K02	Ma świadomość konieczności stosowania właściwego języka dziedzinowego w komunikacji w zespole i osobami spoza niego	COZ_K04
COZ_102_K03	ma świadomość konieczności stałego aktualizowania i wzbogacania posiadanej wiedzy oraz zdobywania nowych umiejętności w zakresie bezpieczeństwa i ochrony danych osobowych	COZ_K02

COZ_102_K04	ma świadomość istotności przekazywania wiedzy na temat metod i narzędzi oraz dobrych praktyk bezpieczeństwa i ochrony danych osobowych	COZ_K03
COZ_102_K05	Rozumie potrzebę stosowania dobrych praktyk i sprawdzonych rozwiązań w bezpieczeństwie i ochronie danych osobowych	COZ_K01 COZ_K03

1.	Nazwa przedmiotu lub grupy przedmiotu	Zagrożenia i ochrona infrastruktury fizycznej
2.	Tryb prowadzenia zajęć (zdalny/stacjonarny)	zdalny
3.	Liczba punktów ECTS przypisana do przedmiotu lub grupy przedmiotów	4 ECTS
4.	Formy prowadzenia zajęć dla przedmiotu lub grupy przedmiotu z przypisaną liczbą godzin	Wykład (16) / Projekt (12)
5.	Treści programowe dla przedmiotu lub grupy przedmiotów	
<p>Zagrożenia osobowe celowe i przypadkowe oraz ochrona fizyczna Zagrożenia naturalne, przypadkowe, awarie. Aspekty organizacyjne i zarządcze w ochronie fizycznej w jednostkach ochrony zdrowia Zagadnienia techniczne ocena sieci energetycznych i teleinformatycznych Problemy zasilania energetycznego, bezpieczeństwo instalacji elektrycznych, ciągłość dostaw energii, alternatywne źródła zasilania Zagadnienia dotyczące oceny ochrony fizycznej i bezpieczeństwa przeciwpożarowego. Ocena zagrożeń łańcuchów logistycznych i dostępności personelu Przygotowanie audytu ochrony infrastruktury fizycznej, jego przeprowadzenie i ocena wyników Narzędzia informatyczne ochrony i diagnostyki ataków, zastosowania w pracy w ochronie zdrowia</p>		
6.	Formy weryfikacji i oceny osiągniętych efektów kształcenia (warunki i sposób zaliczenia)	
<p>Efekty uczenia się będą weryfikowane przez: rozmowę oceniającą, test wiedzy, dyskusję moderowaną, ocenę zadań problemowych wykonywanych w trakcie zajęć oraz obserwację nauczyciela w warunkach symulowanych.</p>		
7.	Efekty uczenia się przypisane do tych przedmiotów lub grup przedmiotów i ich odniesienie do efektów uczenia się dla programu studiów podyplomowych	
	Symbol efektu uczenia się dla przedmiotu lub grupy przedmiotów	Symbol efektu uczenia się dla programu studiów podyplomowych
Wiedza		
	COZ_103_W01	ma wiedzę dotyczącą podstawowych pojęć i podatności w aspektach infrastruktury fizycznej
	COZ_103_W02	ma wiedzę dotyczącą podstawowych pojęć ochrony p poż, energetycznej i logistycznej
	COZ_103_W03	Zna podstawowe metody ochrony infrastruktury fizycznej w jednostkach ochrony zdrowia
	COZ_103_W04	Zna pojęcia i uwarunkowania pozatechniczne działalności inżynierskiej w zakresie infrastruktury fizycznej w jednostkach ochrony zdrowia
	COZ_103_W05	ma wiedzę dotyczącą podstawowych narzędzi ochrony infrastruktury fizycznej w jednostkach ochrony zdrowia
Umiejętności		
	COZ_103_U01	potrafi krytycznie analizować dostępną literaturę w zakresie ochrony infrastruktury fizycznej w jednostkach ochrony zdrowia

COZ_103_U02	potrafi sformułować problemy dotyczące ochrony infrastruktury fizycznej w jednostkach ochrony zdrowia przy użyciu właściwej terminologii	COZ_U02 COZ_U04
COZ_103_U03	potrafi opisać współczesne problemy ochrony infrastruktury fizycznej w jednostkach ochrony zdrowia	COZ_U01 COZ_U04
COZ_103_U04	potrafi opisać współczesne zagrożenia ochrony infrastruktury fizycznej w jednostkach ochrony zdrowia posługując się wybranymi metodami i modelami	COZ_U03 COZ_U07
COZ_103_U05	Potrafi dobrać odpowiednie narzędzia ochrony infrastruktury fizycznej w jednostkach ochrony zdrowia adekwatne do uwarunkowań i zdefiniowanej sytuacji projektowej	COZ_U04
COZ_103_U06	Potrafi wykorzystać wybrane model i narzędzia ochrony infrastruktury fizycznej w jednostkach ochrony zdrowia do pracy i organizacji zespołu w celu rozwiązania problemów stawianych na zajęciach	COZ_U07
COZ_103_U07	potrafi aktywnie uczestniczyć w dyskusji na tematy związane z ochroną infrastruktury fizycznej w jednostkach ochrony zdrowia, używając poprawnej terminologii i formułując trafne argumenty	COZ_U08 COZ_U04
COZ_103_U08	potrafi skutecznie stosować wybrane elementy ochrony infrastruktury fizycznej w jednostkach ochrony zdrowia do rozwiązywania problemów praktycznych samodzielnie i w zespole	COZ_U06 COZ_U07
Kompetencje społeczne		
COZ_103_K01	ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy	COZ_K03
COZ_103_K02	ma świadomość konieczności stosowania właściwego języka dziedzinowego w komunikacji w zespole i osobami spoza niego	COZ_K04
COZ_103_K03	ma świadomość konieczności stałego aktualizowania i wzbogacania posiadanej wiedzy oraz zdobywania nowych umiejętności w zakresie ochrony infrastruktury fizycznej w jednostkach ochrony zdrowia	COZ_K02
COZ_103_K04	ma świadomość istotności przekazywania wiedzy na temat metod i narzędzi oraz dobrych praktyk ochrony	COZ_K03

	infrastruktury fizycznej w jednostkach ochrony zdrowia	
COZ_103_K05	Rozumie potrzebę stosowania dobrych praktyk i sprawdzonych rozwiązań w ochronie infrastruktury fizycznej w jednostkach ochrony zdrowia	COZ_K01 COZ_K03

1.	Nazwa przedmiotu lub grupy przedmiotu	Zarządzanie ciągłością działania
2.	Tryb prowadzenia zajęć (zdalny/stacjonarny)	zdalny
3.	Liczba punktów ECTS przypisana do przedmiotu lub grupy przedmiotów	4 ECTS
4.	Formy prowadzenia zajęć dla przedmiotu lub grupy przedmiotu z przypisaną liczbą godzin	Wykład (16) / Projekt (12)
5.	Treści programowe dla przedmiotu lub grupy przedmiotów	
<p>Wprowadzenie, historia i rodzaje zagrożeń i rozwoju zabezpieczeń dla ciągłości działania Podstawowe pojęcia w ciągłości działania Zarządzanie ciągłością działania wg ISO/IEC 22301 Ocena krytyczności procesów i analiza BIA Podstawowe zasady audytu systemu zarządzania wg ISO 19011 Audytowanie systemu zarządzania ciągłością działania, PN ISO/IEC 22301:2019 Dyrektywa UE NIS, PN ISO/IEC 19011 Ustawa o zarządzaniu kryzysowym Metody opracowania i oceniania podstawowych dokumentów systemu zarządzania ciągłością działania Zasady udziału w audycie ciągłości działania Metody i narzędzia oceny stan audytowanej organizacji Metody i narzędzia oceny zagrożeń łańcuchów logistycznych i dostępności personelu Analiza case study</p>		
6.	Formy weryfikacji i oceny osiągniętych efektów kształcenia (warunki i sposób zaliczenia)	
<p>Efekty uczenia się będą weryfikowane przez: rozmowę ocenającą, test wiedzy, dyskusję moderowaną, ocenę zadań problemowych wykonywanych w trakcie zajęć oraz obserwację nauczyciela w warunkach symulowanych.</p>		
7.	Efekty uczenia się przypisane do tych przedmiotów lub grup przedmiotów i ich odniesienie do efektów uczenia się dla programu studiów podyplomowych	
	Symbol efektu uczenia się dla przedmiotu lub grupy przedmiotów	Symbol efektu uczenia się dla programu studiów podyplomowych
Wiedza		
	COZ_104_W01	ma wiedzę dotyczącą podstawowych pojęć i terminologii ciągłości działania
	COZ_104_W02	ma wiedzę dotyczącą podstawowych standardów ciągłości działania
	COZ_104_W03	zna podstawowe metody pracy przy zarządzaniu ciągłością działania
	COZ_104_W04	zna pojęcia i uwarunkowania pozatechniczne działalności inżynierskiej w zakresie ciągłości działania
	COZ_104_W05	ma wiedzę dotyczącą podstawowych narzędzi zarządzania ciągłością działania
		COZ_W03
		COZ_W01
		COZ_W03
		COZ_W08
		COZ_W09
Umiejętności		
	COZ_104_U01	potrafi krytycznie analizować dostępną literaturę w zakresie zarządzania ciągłością działania
	COZ_104_U02	potrafi sformułować problemy dotyczące zarządzania ciągłością działania przy użyciu właściwej terminologii
		COZ_U01
		COZ_U03
		COZ_U01
		COZ_U04

COZ_104_U03	potrafi opisać współczesne problemy zarządzania ciągłością działania posługując się wybranymi metodami i modelami	COZ_U01 COZ_U04 COZ_U02
COZ_104_U04	potrafi opisać współczesne zagrożenia zarządzania ciągłością działania posługując się wybranymi metodami i modelami	COZ_U05 COZ_U07 COZ_U02
COZ_104_U05	potrafi dobrać odpowiednie narzędzia zarządzania ciągłością działania adekwatne do uwarunkowań i zdefiniowanej sytuacji projektowej	COZ_U05 COZ_U07 COZ_U02
COZ_104_U06	potrafi wykorzystać wybrane modele i narzędzia informatyczne do zarządzania ciągłością działania w celu rozwiązania problemów stawianych na zajęciach	COZ_U02 COZ_U04
COZ_104_U07	potrafi aktywnie uczestniczyć w dyskusji na tematy związane z zarządzaniem ciągłością działania, używając poprawnej terminologii i formułując trafne argumenty	COZ_U03 COZ_U04 COZ_U07
COZ_104_U08	potrafi skutecznie stosować wybrane elementy zarządzania ciągłością działania do rozwiązywania problemów praktycznych samodzielnie i w zespole	COZ_U03 COZ_U06 COZ_U02
Kompetencje społeczne		
COZ_104_K01	ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy	COZ_K03
COZ_104_K02	ma świadomość konieczności stosowania właściwego języka dziedzinowego w komunikacji w zespole i osobami spoza niego	COZ_K04
COZ_104_K03	ma świadomość konieczności stałego aktualizowania i wzbogacania posiadanej wiedzy oraz zdobywania nowych umiejętności w zakresie zarządzania ciągłością działania	COZ_K02
COZ_104_K04	ma świadomość istotności przekazywania wiedzy na temat metod i narzędzi oraz dobrych praktyk zarządzania ciągłością działania	COZ_K03
COZ_104_K05	rozumie potrzebę stosowania dobrych praktyk i sprawdzonych rozwiązań w zarządzaniu ciągłością działania	COZ_K01 COZ_K03

1.	Nazwa przedmiotu lub grupy przedmiotu	Wymogi prawne i normy zarządzania bezpieczeństwem w ochronie zdrowia
2.	Tryb prowadzenia zajęć (zdalny/stacjonarny)	Zdalny
3.	Liczba punktów ECTS przypisana do przedmiotu lub grupy przedmiotów	4 ECTS
4.	Formy prowadzenia zajęć dla przedmiotu lub grupy przedmiotu z przypisaną liczbą godzin	Wykład (16) / Projekt (12)
5.	Treści programowe dla przedmiotu lub grupy przedmiotów	
<p>Normy i standardy międzynarodowe dotyczące bezpieczeństwa informacji i ochrony danych osobowych ze szczególnym uwzględnieniem ochrony zdrowia Odpowiedzialność prawna, osobowa i kary finansowe w przypadku dopuszczenia do naruszenia cyberbezpieczeństwa, bezpieczeństwa informacji i ochrony danych osobowych w ochronie zdrowia Normy ISO/IEC 27001 i 27002 jako podstawowe wymagania i zalecenia dla zarządzania bezpieczeństwem informacji Norma ISO/IEC 27799 jako szczegółowe zalecenia dla zarządzania bezpieczeństwem informacji w ochronie zdrowia Normy ISO/IEC 27701 jako wymagania zalecenia dotyczące ochrony danych osobowych Norma ISO 22301 wymagania zapewnienia ciągłości działania</p>		
6.	Formy weryfikacji i oceny osiągniętych efektów kształcenia (warunki i sposób zaliczenia)	
<p>Efekty uczenia się będą weryfikowane przez: rozmowę oceniającą, test wiedzy, dyskusję moderowaną, ocenę zadań problemowych wykonywanych w trakcie zajęć oraz obserwację nauczyciela w warunkach symulowanych.</p>		
7.	Efekty uczenia się przypisane do tych przedmiotów lub grup przedmiotów i ich odniesienie do efektów uczenia się dla programu studiów podyplomowych	
	Symbol efektu uczenia się dla przedmiotu lub grupy przedmiotów	Symbol efektu uczenia się dla programu studiów podyplomowych
Wiedza		
	COZ_105_W01	ma wiedzę dotyczącą norm prawnych stosowanych w aspektach cyberbezpieczeństwa w ochronie zdrowia
	COZ_105_W02	ma wiedzę dotyczącą audytów bezpieczeństwa
	COZ_105_W03	Zna podstawowe metody pracy z normami prawnymi stosowanymi w aspektach cyberbezpieczeństwa w ochronie zdrowia
	COZ_105_W04	Zna pojęcia i uwarunkowania pozatechniczne działalności inżynierskiej w zakresie norm prawnych stosowanych w aspektach cyberbezpieczeństwa w ochronie zdrowia
	COZ_105_W05	ma wiedzę dotyczącą podstawowych narzędzi audytorskich kontekście audytów bezpieczeństwa w ochronie zdrowia

Umiejętności		
COZ_105_U01	potrafi krytycznie analizować dostępną literaturę w zakresie norm krajowych i międzynarodowych i regulacji prawnych związanych z cyberbezpieczeństwem w ochronie zdrowia	COZ_U01 COZ_U03
COZ_105_U02	potrafi sformułować problemy dotyczące planowania i realizacji audytu	COZ_U01 COZ_U04
COZ_105_U03	potrafi dobrać odpowiednie normy prawne i standardy adekwatne do uwarunkowań i zdefiniowanej sytuacji projektowej	COZ_U05
COZ_105_U04	potrafi wykorzystać normy prawne i standardy do pracy i organizacji zespołu w celu rozwiązania problemów stawianych na zajęciach	COZ_U06
COZ_105_U05	potrafi aktywnie uczestniczyć w dyskusji na tematy związane z regulacjami prawnymi w zakresie cyberbezpieczeństwa w ochronie zdrowia używając poprawnej terminologii i formułując trafne argumenty	COZ_U01 COZ_U08
COZ_105_U06	potrafi skutecznie stosować wybrane normy i standardy do rozwiązywania problemów praktycznych samodzielnie i w zespole	COZ_U05 COZ_U07
Kompetencje społeczne		
COZ_105_K01	ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy	COZ_K03
COZ_105_K02	ma świadomość konieczności stosowania właściwego języka dziedzinowego w komunikacji w zespole i osobami spoza niego	COZ_K04
COZ_105_K03	ma świadomość konieczności stałego aktualizowania i wzbogacania posiadanej wiedzy oraz zdobywania nowych umiejętności w zakresie norm prawnych stosowanych w aspektach cyberbezpieczeństwa w ochronie zdrowia	COZ_K02
COZ_105_K04	ma świadomość istotności przekazywania wiedzy na temat norm prawnych stosowanych w aspektach cyberbezpieczeństwa w ochronie zdrowia	COZ_K03
COZ_105_K05	Rozumie potrzebę stosowania norm prawnych stosowanych w aspektach	COZ_K01 COZ_K03

	cyberbezpieczeństwa w ochronie zdrowia	
--	---	--

1.	Nazwa przedmiotu lub grupy przedmiotu	Audyt wewnętrzny systemów ochrony zdrowia
2.	Tryb prowadzenia zajęć (zdalny/stacjonarny)	zdalny
3.	Liczba punktów ECTS przypisana do przedmiotu lub grupy przedmiotów	4 ECTS
4.	Formy prowadzenia zajęć dla przedmiotu lub grupy przedmiotu z przypisaną liczbą godzin	Wykład (16) / Projekt (12)
5.	Treści programowe dla przedmiotu lub grupy przedmiotów	
<p>Pojęcie audytu i audytora wewnętrznego Regulacje prawne w zakresie audytu wewnętrznego Przegląd zasadniczych treści z zakresu audytu, w tym elementy związane z certyfikacją: - audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji wg ISO/IEC 27001 - audytor wewnętrzny systemu zarządzania ochroną identyfikacji osób wg ISO/IEC 27701 - audytor wewnętrzny systemy zarządzania ciągłością działania wg ISO 22301 - audytor wewnętrzny systemu zarządzania usługami wg ISO/IEC 20000-1 Zagadnienia praktyczne i sposoby oceny przedmiotu audytu Zagadnienia praktyczne przykłady incydentów, zagrożeń, podatności w jednostkach ochrony zdrowia Przygotowanie audytu, jego przeprowadzenie i ocena wyników Możliwe certyfikacje audytorskie</p>		
6.	Formy weryfikacji i oceny osiągniętych efektów kształcenia (warunki i sposób zaliczenia)	
Efekty uczenia się będą weryfikowane przez: rozmowę oceniającą, test wiedzy, dyskusję moderowaną, ocenę zadań problemowych wykonywanych w trakcie zajęć oraz obserwację nauczyciela w warunkach symulowanych. W ramach zajęć słuchacz powinien zdać dwa spośród czterech oferowanych do wyboru kursów audytorskich.		
7.	Efekty uczenia się przypisane do tych przedmiotów lub grup przedmiotów i ich odniesienie do efektów uczenia się dla programu studiów podyplomowych	
	Symbol efektu uczenia się dla przedmiotu lub grupy przedmiotów	Symbol efektu uczenia się dla programu studiów podyplomowych
Wiedza		
	COZ_106_W01	ma wiedzę dotyczącą podstawowych pojęć audytu i audytu wewnętrznego
	COZ_106_W02	ma wiedzę dotyczącą podstawowych narzędzi oraz norm audytu i audytu wewnętrznego
	COZ_106_W03	Zna podstawowe metody przeprowadzania audytu i audytu wewnętrznego
	COZ_106_W04	Zna pojęcia i uwarunkowania pozatechniczne działalności inżynierskiej w zakresie audytu i audytu wewnętrznego
Umiejętności		
	COZ_106_U01	potrafi krytycznie analizować dostępną literaturę w zakresie audytu i audytu wewnętrznego
	COZ_106_U02	potrafi sformułować problemy dotyczące zakresu audytu i audytu wewnętrznego przy użyciu właściwej terminologii

COZ_106_U03	potrafi zaplanować i zrealizować czynności audytu wewnętrznego z zakresu prezentowanych norm	COZ_U05 COZ_U07
COZ_106_U04	potrafi przygotować dokumentację zgodną ze standardem audytu wewnętrznego i zaprezentowanej normy	COZ_U07 COZ_U08
Kompetencje społeczne		
COZ_106_K01	ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy	COZ_K03
COZ_106_K02	Ma świadomość konieczności stosowania właściwego języka dziedzinowego w komunikacji w zespole i z osobami spoza niego	COZ_K04
COZ_106_K03	ma świadomość konieczności stałego aktualizowania i wzbogacania posiadanej wiedzy oraz zdobywania nowych umiejętności w zakresie modelowania danych	COZ_K02
COZ_106_K04	ma świadomość istotności przekazywania wiedzy na temat metod i narzędzi oraz dobrych praktyk modelowania danych	COZ_K03
COZ_106_K05	Rozumie potrzebę stosowania dobrych praktyk i sprawdzonych rozwiązań baz danych	COZ_K01 COZ_K03

1.	Nazwa przedmiotu lub grupy przedmiotu	Seminarium problemowe /Projekt końcowy
2.	Tryb prowadzenia zajęć (zdalny/stacjonarny)	stacjonarny / zdalny
3.	Liczba punktów ECTS przypisana do przedmiotu lub grupy przedmiotów	6 (3/3) ECTS
4.	Formy prowadzenia zajęć dla przedmiotu lub grupy przedmiotu z przypisaną liczbą godzin	Seminarium (8) Projekt (28)
5.	Treści programowe dla przedmiotu lub grupy przedmiotów	
<p>Praca samodzielna nad analizą literaturową i problemową z wybranych elementów związanych z tematyką studiów Samodzielne pogłębienie tematyki związanej z tematyką studiów Identyfikacja rzeczywistych problemów związanych z tematyką studiów Propozycje rozwiązania zidentyfikowanych problemów związanych z tematyką studiów Samodzielne przygotowanie projektu na wybrany temat związany z tematyką studiów Projekt Zapewnienie cyberbezpieczeństwa, bezpieczeństwa informacji i ochrony danych osobowych we jednostce ochrony zdrowia w której pracują wykonawcy</p>		
6.	Formy weryfikacji i oceny osiągniętych efektów kształcenia (warunki i sposób zaliczenia)	
<p>Efekty uczenia się będą weryfikowane przez: rozmowę oceniającą, ocenę wystąpienia, ocenę opracowania rozwiązania zadań problemowych, ocenę pracy i prezentacji końcowej. Słuchacz wykonuje projekt zapewnienia cyberbezpieczeństwa, bezpieczeństwa informacji i ochrony danych osobowych w jednostce ochrony zdrowia.</p>		
7.	Efekty uczenia się przypisane do tych przedmiotów lub grup przedmiotów i ich odniesienie do efektów uczenia się dla programu studiów podyplomowych	
	Symbol efektu uczenia się dla przedmiotu lub grupy przedmiotów	Symbol efektu uczenia się dla programu studiów podyplomowych
Umiejętności		
	COZ_107_U01	Umie identyfikować rzeczywiste problemy związane z tematyką studiów
		COZ_U01 COZ_U02 COZ_U03 COZ_U04 COZ_U05 COZ_U06 COZ_U07
	COZ_107_U02	Umie wykorzystać wiedzę zakresu studiów do sformułowania propozycji rozwiązania rzeczywistych problemów związanych z tematyką studiów
		COZ_U01 COZ_U02 COZ_U03 COZ_U04 COZ_U05 COZ_U06 COZ_U07
	COZ_107_U03	Potrafi udokumentować i przedstawić rozwiązania rzeczywistych problemów związanych z tematyką studiów
		COZ_U01 COZ_U02 COZ_U03 COZ_U04 COZ_U05 COZ_U06 COZ_U07 COZ_U08
Kompetencje społeczne		

COZ_107_K01	Jest gotów do oceny przekazywanych informacji na temat modeli	COZ_K01, COZ_K02
COZ_107_K02	Dbą o język komunikacji z klientem i komunikacji wewnątrz zespołu	COZ_K04
COZ_107_K03	Uczciwie i z szacunkiem współpracuje w zespole nad budową modeli i wzajemnie podnosi kwalifikacje swoje i zespołu	COZ_K03