Zamierzone dla programu studiów podyplomowych pn. *Cyberbezpieczeństwo w ochronie zdrowia* efekty uczenia się z uwzględnieniem najważniejszych sposobów weryfikacji osiągnięcia tych efektów przez uczestnika studiów podyplomowych

Lp.	Symbol efektu uczenia się	Efekt uczenia się	Najważniejsze sposoby weryfikacji osiągnięcia efektu uczenia się przez uczestnika studiów podyplomowych
1	*2*	*3*	*4*
Wiedza			
1	COZ_W01	zna i rozumie podstawowe pojęcia z zakresu cyberbezpieczeństwa (bezpieczeństwa systemów elektroenergetycznych i logistycznych), systemów elektroenergetycznych i logistycznych i relacje między nimi	rozmowa oceniająca, test wiedzy, dyskusja moderowana
2	COZ_W02	ma wiedzę dotyczącą podatności i zagrożeń występujących w systemach informacyjnych, teleinformatycznych, energetycznych i fizycznych w odniesieniu do systemów służby zdrowia, w tym wiedzę dotyczącą modelowania podatności i zagrożeń w służbie zdrowia	rozmowa oceniająca, test wiedzy, dyskusja moderowana
3	COZ_W03	ma wiedzę dotyczącą problemów ciągłości działania usług występujących jednostkach służby zdrowia w tym zasad ochrony i zapewnienia ciągłości zasilania elektroenergetycznego, i usług logistycznych	rozmowa oceniająca, test wiedzy, dyskusja moderowana
4	COZ_W04	ma wiedzę dotyczącą regulacji prawnych oraz norm krajowych i międzynarodowych w zakresie zarządzania bezpieczeństwem informacji w ochronie zdrowia, ciągłości działania, zarządzania zmianą i ochroną danych osobowych z uwzględnieniem specyfiki w służbie zdrowia w tym zasad prowadzenia audytów	rozmowa oceniająca, test wiedzy, dyskusja moderowana
5	COZ_W05	zna metody i narzędzia analizy bezpieczeństwa systemów informacyjnych, sieci teleinformatycznych, systemów energetycznych i fizycznych oraz oceny ryzyka związanego z ich funkcjonowaniem	rozmowa oceniająca, test wiedzy, dyskusja moderowana
6	COZ_W06	zna odpowiedzialność prawną i finansową w przypadku dopuszczenia do naruszenia cyberbezpieczeństwa, bezpieczeństwa informacji i ochrony danych osobowych w ochronie zdrowia	rozmowa oceniająca, test wiedzy, dyskusja moderowana
7	COZ_W07	ma wiedzę dotyczącą zarządzania incydentami związanymi z funkcjonowaniem systemów informacyjnych i sieci teleinformatycznych, w tym metod i narzędzi służących do analizy i obsługi incydentów	rozmowa oceniająca, test wiedzy, dyskusja moderowana
8	COZ_W08	rozumie pozatechniczne (prawne, etyczne, ekonomiczne, społeczne, socjotechniczne i inne) uwarunkowania działalności inżynierskiej w zakresie cyberbezpieczeństwa	rozmowa oceniająca, test wiedzy, dyskusja moderowana
9	COZ_W09	ma podstawową wiedzę dotyczącą zarządzania cyberbezpieczeństwem w jednostkach służby zdrowia z uwzględnieniem jej specyfiki oraz audytu i audytu wewnętrznego na potrzeby analizy cyberbezpieczeństwa	rozmowa oceniająca, test wiedzy, dyskusja moderowana

Lp.	Symbol efektu uczenia się	Efekt uczenia się	Najważniejsze sposoby weryfikacji osiągnięcia efektu uczenia się przez uczestnika studiów podyplomowych
1	*2*	*3*	*4*
		w jednostkach ochrony zdrowia	
Umiejętności			
10	COZ_U01	potrafi – przy formułowaniu i rozwiązywaniu zadań związanych z analizą stosowania cyberbezpieczeństwa w ochronie zdrowia – pozyskiwać informacje z właściwie dobranych źródeł (literatury, baz danych i innych źródeł), dokonywać krytycznej analizy i syntezy tych informacji oraz posługiwać się normami krajowymi i międzynarodowymi z tego zakresu	obserwacja w warunkach symulowanych, ocena zadań problemowych
11	COZ_U02	potrafi dokonać analizy i oceny podatności i zagrożeń występujących w systemach informacyjnych, sieciach teleinformatycznych, sieciach energetycznych oraz przewidzieć ich skutki, wykorzystując właściwe modele, metody i narzędzia	obserwacja w warunkach symulowanych, ocena zadań problemowych, ocena pracy i prezentacji końcowej
12	COZ_U03	potrafi przeprowadzić analizę incydentów występujących w systemach informacyjnych, sieciach teleinformatycznych, systemach energetycznych wykorzystując właściwe metody i narzędzia	obserwacja w warunkach symulowanych, ocena zadań problemowych
13	COZ_U04	potrafi zaprojektować odpowiednie do postawionych wymagań mechanizmy zapewniania cyberbezpieczeństwa w ochronie zdrowia a w szczególności: - sformułować wymagania i skontrolować mechanizmy bezpieczeństwa w systemach informatycznych, - sformułować wymagania i skontrolować bezpieczną usługę sieciową związaną z przechowywaniem i przesyłaniem danych oraz kontrolą dostępu, - sformułować wymagania i skontrolować mechanizmy zapewniające ciągłość działania w tym ciągłość zasilania energetycznego, - zintegrować mechanizmy dotyczące różnych aspektów cyberbezpieczeństwa, wykorzystując odpowiednio dobrane metody i narzędzia, - zaplanować i zrealizować czynności audytorskie	obserwacja w warunkach symulowanych, ocena zadań problemowych, ocena pracy i prezentacji końcowej
14	COZ_U05	potrafi zaplanować i przeprowadzić badanie dotyczące wybranego aspektu bezpieczeństwa w ochronie zdrowia , sformułować wymagania, skontrolować oraz sporządzić dokumentację przeprowadzonego badania zgodną z wymaganymi norm i standardów	obserwacja w warunkach symulowanych, ocena zadań problemowych, ocena pracy i prezentacji końcowej
15	COZ_U06	potrafi wykonać analizę możliwych zagrożeń cyberbezpieczeństwa w ochronie zdrowia i ocenić ich wpływ na środowisko w służbie zdrowia	obserwacja w warunkach symulowanych, ocena zadań problemowych

Lp.	Symbol efektu uczenia się	Efekt uczenia się	Najważniejsze sposoby weryfikacji osiągnięcia efektu uczenia się przez uczestnika studiów podyplomowych
1	*2*	*3*	*4*
		oraz stworzyć plan zapewnienia bezpieczeństwa i przygotować jego wdrożenie, z wykorzystaniem środków technicznych adekwatnych do określonego otoczenia organizacyjnego	
16	COZ_U07	potrafi skonstruować i ocenić projekt zapewnienia cyberbezpieczeństwa, bezpieczeństwa informacji i ochrony danych w jednostce ochrony zdrowia z uwzględnieniem obowiązujących norm krajowych i międzynarodowych, w tym potrafi współpracować z audytorem w w/w zakresie	obserwacja w warunkach symulowanych, ocena zadań problemowych, ocena projektu i prezentacji końcowej
17	COZ_U08	potrafi przygotować i przedstawić prezentację oraz współdziałać i uczestniczyć w dyskusji na tematy związane z cyberbezpieczeństwem, używając poprawnej terminologii i właściwych argumentów	obserwacja w warunkach symulowanych, ocena projektu i prezentacji końcowej
Kompetencje społeczne			
18	COZ_K01	rozumie konieczność działania w sposób profesjonalny, przestrzegania i propagowania zasad etyki zawodowej związanej z działalnością inżyniera-specjalisty w zakresie cyberbezpieczeństwa w ochronie zdrowia, docenia wartość pracy w zespole	rozmowa oceniająca, obserwacja w warunkach symulowanych, ocena pracy iprezentacji końcowej
19	COZ_K02	odczuwa potrzebę stałego aktualizowania i wzbogacania posiadanej wiedzy oraz zdobywania nowych umiejętności, m.in. w związku z postępami nauki i techniki w zakresie cyberbezpieczeństwa w ochronie zdrowia	rozmowa oceniająca, obserwacja w warunkach symulowanych, ocena pracy i prezentacji końcowej
20	COZ_K03	ma świadomość potrzeby formułowania i przekazywania społeczeństwu – m.in. poprzez środki masowego przekazu – informacji i opinii dotyczących osiągnięć nauki i techniki oraz innych aspektów związanych z cyberbezpieczeństwem w ochronie zdrowia; podejmuje starania, aby przekazać takie informacje i opinie w sposób powszechnie zrozumiały	rozmowa oceniająca, obserwacja w warunkach symulowanych
21	COZ_K04	dba o właściwy język komunikacji oraz skuteczną i uczciwą formułę komunikacji wewnętrznej i zewnętrznej	rozmowa oceniająca, obserwacja w warunkach symulowanych