# Efekty uczenia się dla studiów podyplomowych pn. *Cyberbezpieczeństwo w ochronie zdrowia* prowadzonych na Wydziale Elektrycznym gdzie:

**Obowiązkowe jest:**

[1] „Odniesienie – symbol I/III" oznacza odniesienie do charakterystyk drugiego stopnia efektów uczenia się Polskiej Ramy Kwalifikacji dla profilu ogólnoakademickiego (symbol I) lub odniesienie dla kwalifikacji obejmujących kompetencje inżynierskie (symbol III), określonych **Rozporządzeniem 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* (Dz.U. z 2018 r. poz. 2218) i uwzględnia odpowiednio Kod składnika charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji, określony w uchwale Senatu PW *w sprawie przyjęcia przez Politechnikę Warszawską kodu składnika charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego*,

[2] „Odniesienie-symbol" oznacza odniesienie do uniwersalnych charakterystyk pierwszego stopnia Polskiej Ramy Kwalifikacji, określonych w załączniku do **Ustawy z dnia 22 grudnia 2015 r.** *o Zintegrowanym Systemie Kwalifikacji* (tj. Dz.U. z 2020 r. poz. 226, z późn. zm.)

**Nieobowiązkowe (do zastosowania, jeśli jest to celowe) jest:**

[3] „Odniesienie-zawodowe" oznacza odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji dla poziomów 6, 7 i 8 określonych w **Rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego** z dnia 13 kwietnia 2016 r. *w sprawie charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji typowych dla kwalifikacji o charakterze zawodowym – poziomy 1-8* (Dz.U. z 2016 r. poz.537, z późn. zm.)

[4] „Odniesienie-sektorowe" oznacza odniesienie do charakterystyk efektów uczenia się dla kwalifikacji na poziomach 6, 7 i 8 Sektorowej Ramy Kwalifikacji, właściwej dla danych studiów podyplomowych

| Lp. | Symbol efektu uczenia się | Efekt uczenia się | [1]Odniesienie – symbol I/III | [2]Odniesienie – symbol | [3]Odniesienie – zawodowe [nieobowiązkowe] | [4]Odniesienie – sektorowe [nieobowiązkowe] |
|---|---|---|---|---|---|---|
| *1* | *2* | *3* | *4* | *5* | *6* | *7* |
| **Wiedza** | | | | | | |
| 1 | COZ_W01 | zna i rozumie podstawowe pojęcia z zakresu cyberbezpieczeństwa (bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych), systemów elektroenergetycznych i logistycznych i relacje między nimi | I.P6S_WG.o | P6U_W | | |
| 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 | I.P6S_WG.o | P6U_W | | |
| 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 | I.P6S_WG.o | P6U_W | | |
| 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 | I.P6S_WG.o | P6U_W | | |

| Lp. | Symbol efektu uczenia się | Efekt uczenia się | [1]Odniesienie – symbol I/III | [2]Odniesienie – symbol | [3]Odniesienie – zawodowe [nieobowiązkowe] | [4]Odniesienie – sektorowe [nieobowiązkowe] |
|---|---|---|---|---|---|---|
| *1* | *2* | *3* | *4* | *5* | *6* | *7* |
| 5 | COZ_W05 | zna metody i narzędzia analizy bezpieczeństwa systemów informacyjnych, sieci teleinformatycznych, systemów energetycznych i fizycznych oraz oceny ryzyka związanego z ich funkcjonowaniem | I.P6S_WG.o | P6U_W | | |
| 6 | COZ_W06 | zna odpowiedzialność prawną i finansową w przypadku dopuszczenia do naruszenia cyberbezpieczeństwa, bezpieczeństwa informacji i ochrony danych osobowych w ochronie zdrowia | I.P6S_WG.o | P6U_W | | |
| 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 | I.P6S_WG.o | P6U_W | | |
| 8 | COZ_W08 | rozumie pozatechniczne (prawne, etyczne, ekonomiczne, społeczne, socjotechniczne i inne) uwarunkowania działalności inżynierskiej w zakresie cyberbezpieczeństwa | I.P6S_WK | P6U_W | | |
| 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 w jednostkach ochrony zdrowia | I.P6S_WG.o | P6U_W | | |
| **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 | I.PS6_UW | P6U_U | | |
| 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 | I.P6S_UW.o<br>III.P6S_UW.o | P6U_U | | |
| 12 | COZ_U03 | potrafi przeprowadzić analizę incydentów występujących w systemach informacyjnych, sieciach teleinformatycznych, systemach energetycznych wykorzystując właściwe metody i narzędzia | I.P6_UW.o<br>III.P6S_UW.o | P6U_U | | |

| Lp. | Symbol efektu uczenia się | Efekt uczenia się | [1]Odniesienie – symbol I/III | [2]Odniesienie – symbol | [3]Odniesienie – zawodowe [nieobowiązkowe] | [4]Odniesienie – sektorowe [nieobowiązkowe] |
|---|---|---|---|---|---|---|
| *1* | *2* | *3* | *4* | *5* | *6* | *7* |
| 13 | COZ_U04 | potrafi zaprojektować odpowiednie do postawionych wymagań mechanizmy zapewniania cyberbezpieczeństwa w ochronie zdrowia a w szczególności:<br>- sformułować wymagania i skontrolować mechanizmy bezpieczeństwa w systemach informatycznych,<br>- sformułować wymagania i skontrolować bezpieczną usługę sieciową związaną z przechowywaniem i przesyłaniem danych oraz kontrolą dostępu,<br>- sformułować wymagania i skontrolować mechanizmy zapewniające ciągłość działania w tym ciągłość zasilania energetycznego,<br>- zintegrować mechanizmy dotyczące różnych aspektów cyberbezpieczeństwa, wykorzystując odpowiednio dobrane metody i narzędzia,<br>- zaplanować i zrealizować czynności audytorskie | I.P6_UW.o<br>III.P6S_UW.o | P6U_U | | |
| 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 | I.P6S_UW.o<br>I.P6S_UK<br>III.P6S_UW.o | P6U_U | | |
| 15 | COZ_U06 | potrafi wykonać analizę możliwych zagrożeń cyberbezpieczeństwa w ochronie zdrowia i ocenić ich wpływ na środowisko w służbie zdrowia oraz stworzyć plan zapewnienia bezpieczeństwa i przygotować jego wdrożenie, z wykorzystaniem środków technicznych adekwatnych do określonego otoczenia organizacyjnego | I.P6S_UW.o<br>III.P6S_UW.o | P6U_U | | |
| 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 | I.P6S_UW.o<br>III.P6S_UW.o | P6U_U | | |
| 17 | COZ_U08 | potrafi przygotować i przedstawić prezentację oraz współdziałać i uczestniczyć w dyskusji na tematy związane z cyberbezpieczeństwem, używając poprawnej terminologii | I.P6S_UK<br>I.P6S_UO<br>I.P6S_UU | P6U_U | | |

| Lp. | Symbol efektu uczenia się | Efekt uczenia się | [1]Odniesienie – symbol I/III | [2]Odniesienie – symbol | [3]Odniesienie – zawodowe [nieobowiązkowe] | [4]Odniesienie – sektorowe [nieobowiązkowe] |
|---|---|---|---|---|---|---|
| *1* | *2* | *3* | *4* | *5* | *6* | *7* |
| | | i właściwych argumentów | | | | |
| **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 | I.P6S_KR | P6U_K | | |
| 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 | I.P6S_KK | P6U_K | | |
| 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 | I.P6S_KO | P6U_K | | |
| 21 | COZ_K04 | dba o właściwy język komunikacji oraz skuteczną i uczciwą formułę komunikacji wewnętrznej i zewnętrznej | I.P6S_KK | P6U_K | | |