Efekty uczenia się dla studiów podyplomowych pn. Inżynieria Cyberbezpieczeństwa, prowadzonych na Wydziale Elektroniki i Technik Informacyjnych, 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* (Dz.U. z 2020 r. poz. 226)

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 Edukacji Narodowej** 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)

[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	ICYB_W01	Zna i rozumie podstawowe pojęcia z zakresu cyberbezpieczeństwa (bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych) i relacje między nimi.	I.P6S_WG.o	P6U_W		
2	ICYB_W02	Ma wiedzę dotyczącą podatności i zagrożeń występujących w systemach informacyjnych i sieciach teleinformatycznych, w tym wiedzę dotyczącą modelowania podatności i zagrożeń.	I.P6S_WG.o	P6U_W		
3	ICYB_W03	Zna metody i narzędzia analizy bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych, w tym ich oprogramowania, oraz oceny ryzyka związanego z ich funkcjonowaniem.	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*
4	ICYB_W04	Ma wiedzę dotyczącą: – bezpieczeństwa danych, – bezpieczeństwa komunikacji w sieci teleinformatycznej, – bezpieczeństwa systemów operacyjnych i oprogramowania, tworzącą podstawy do projektowania rozwiązań mających na celu zapewnienie bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych.	I.P6S_WG.o	P6U_W		
5	ICYB_W05	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		
6	ICYB_W06	Rozumie pozatechniczne (prawne, etyczne, ekonomiczne, społeczne, socjotechniczne i inne) uwarunkowania działalności inżynierskiej w zakresie cyberbezpieczeństwa.	I.P6S_WK	P6U_W		
7	ICYB_W07	Ma podstawową wiedzę dotyczącą zarządzania cyberbezpieczeństwem na poziomie instytucji/organizacji.	I.P6S_WG.o	P6U_W		
Umiejętności						
8	ICYB_U01	Potrafi – przy formułowaniu i rozwiązywaniu zadań związanych z analizą podatności i zagrożeń oraz zapewnieniem bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych – pozyskiwać informacje z właściwie dobranych źródeł (literatury, baz danych i innych źródeł) oraz dokonywać krytycznej analizy i syntezy tych informacji.	I.P6S_UW	P6U_U		
9	ICYB_U02	Potrafi dokonać analizy i oceny podatności i zagrożeń występujących w systemach informacyjnych i sieciach teleinformatycznych oraz przewidzieć ich skutki, wykorzystując właściwe modele, metody i narzędzia.	I.P6S_UW.o III.P6S_UW.o	P6U_U		
10	ICYB_U03	Potrafi przeprowadzić analizę incydentów występujących w systemach informacyjnych i sieciach teleinformatycznych, wykorzystując właściwe metody i narzędzia.	I.P6S_UW.o 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*
11	ICYB_U04	Potrafi zaprojektować odpowiednie do postawionych wymagań mechanizmy zapewniania bezpieczeństwa w systemach informacyjnych i sieciach teleinformatycznych, a w szczególności: – odpowiednio skonfigurować mechanizmy bezpieczeństwa w systemach operacyjnych Windows i Linux, – zaprojektować bezpieczną usługę sieciową związaną z przechowywaniem i przesyłaniem danych oraz kontrolą dostępu, – zintegrować mechanizmy dotyczące różnych aspektów cyberbezpieczeństwa, wykorzystując odpowiednio dobrane metody i narzędzia.	I.P6S_UW.o III.P6S_UW.o	P6U_U		
12	ICYB_U05	Potrafi zaplanować i przeprowadzić badanie dotyczące wybranego aspektu bezpieczeństwa systemu informacyjnego lub sieci teleinformatycznej oraz sporządzić dokumentację przeprowadzonego badania.	I.P6S_UW.o I.P6S_UK III.P6S_UW.o	P6U_U		
13	ICYB_U06	Potrafi wykonać analizę możliwych zagrożeń i oraz ocenić ich wpływ na zadane środowisko teleinformatyczne oraz stworzyć plan zapewnienia bezpieczeństwa i przygotować jego wdrożenie, z wykorzystaniem środków technicznych adekwatnych do określonego otoczenia organizacyjnego.	I.P6S_UW.o III.P6S_UW.o	P6U_U		
14	ICYB_U07	Potrafi przygotować i przedstawić prezentację oraz uczestniczyć w dyskusji na tematy związane z cyberbezpieczeństwem, używając poprawnej terminologii i właściwych argumentów.	I.P6S_UK	P6U_U		
15	ICYB_U08	Potrafi planować i organizować pracę własną oraz współdziałać z innymi osobami w ramach prac w zespole.	I.P6S_UO	P6U_U		
16	ICYB_U09	Ma umiejętność samokształcenia się w celu podnoszenia kompetencji w zakresie cyberbezpieczeństwa.	I.P6S_UU	P6U_U		

Kompetencje społeczne						
17	ICYB_K01	Rozumie konieczność działania w sposób profesjonalny, przestrzegania i propagowania zasad etyki zawodowej związanej z działalnością inżyniera-specjalisty w zakresie cyberbezpieczeństwa, docenia wartość pracy w zespole.	I.P6S_KR	P6U_K		
18	ICYB_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.	I.P6S_KK	P6U_K		
19	ICYB_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 bezpieczeństwem systemów informacyjnych i sieci teleinformatycznych; podejmuje starania, aby przekazać takie informacje i opinie w sposób powszechnie zrozumiały.	I.P6S_KO	P6U_K		