

Nazwa kierunku: *IT Cyber Security*

Profil – ogólnoakademicki

Poziom studiów : studia II. stopnia

Dziedzina: nauki społeczne, dyscyplina naukowa: nauki o polityce i administracji – 55%, oraz nauki ścisłe i przyrodnicze, dyscyplina: informatyka 45%

Poziom Polskiej Ramy Kwalifikacji – poziom 7

Symbole efektów	Efekty uczenia się	Odniesienie do uniwersalnych charakterystyk PRK ¹	Odniesienie do charakterystyki drugiego stopnia PRK dla właściwego poziomu ²
1	2	3	4
	WIEDZA: ABSOLWENT ZNA I ROZUMIE	Kod składnik opisu	Kod składnik opisu
K_W01	w stopniu pogłębionym miejsce cyberbezpieczeństwa w strukturze współczesnego bezpieczeństwa i sposoby jego teoretycznego ujmowania	P7U_W	P7S_WG
K_W02	w stopniu zaawansowanym społeczne i technologiczne uwarunkowania różnorodności zagrożeń bezpieczeństwa w cyberprzestrzeni	P7U_W	P7S_WK
K_W03	w stopniu zaawansowanym dylematy współczesnej cywilizacji warunkowane rolą czynnika technologicznego i funkcjonowaniem cyberprzestrzeni oraz przyspieszeniem historycznym	P7U_W	P7S_WK
K_W04	w pogłębionym stopniu różnorodne działania społeczne i polityczne na rzecz zapewniania bezpieczeństwa w cyberprzestrzeni, istniejące tu tendencje	P7U_W	P7S_WG
K_W05	w pogłębionym stopniu ekonomiczna, prawne i etyczne uwarunkowania działalności zawodowej oraz zasady ochrony własności przemysłowej i prawa autorskiego	P7U_W	P7S_WK
K_W06	fakty, obiekty i zjawiska oraz dotyczące ich metody i teorie wyjaśniające zależności między nimi, stanowiące wiedzę z zakresu podstaw informatyki	P7U_W	P7S_WG
K_W07	wybrane zagadnienia z zakresu systemów operacyjnych ze szczególnym uwzględnieniem tych dotyczących	P7U_W	P7S_WG

¹ Należy odnieść się do właściwego poziomu PRK 6-8 zgodnie z załącznikiem do ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji

² Odniesienie do charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 Polskiej Ramy Kwalifikacji typowych dla kwalifikacji uzyskiwanych w ramach systemu szkolnictwa wyższego i nauki po uzyskaniu kwalifikacji pełnej na poziomie 4 – zgodnie z 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. W przypadku studiów inżynierskich powinny uwzględniać również możliwość uzyskania wszystkich kompetencji inżynierskich, o których mowa w cz. III rozporządzenia. Efekty uczenia się dla kierunków z dziedziny sztuki powinny zawierać odniesienia również do cz. II rozporządzenia.

	bezpieczeństwa informatycznego		
K_W08	zagadnienia związane z wybranymi językami programowania	P7U_W	P7S_WG
K_W09	zagadnienia z zakresu bezpieczeństwa systemów informatycznych w tym wybrane protokoły kryptograficzne	P7U_W	P7S_WG
K_W10	zagadnienia związane z technologiami sieciowymi, w tym współczesne protokoły komunikacyjne oraz zagadnienia związane z budową aplikacji sieciowych i różne formy przedsiębiorczości	P7U_W	P7S_WG
	UMIEJĘTNOŚCI: ABSOLWENT POTRAFI	Kod składnika opisu	Kod składnik opisu
K_U01	z wykorzystaniem posiadanej wiedzy w sposób innowacyjny, z zastosowaniem dobrze dobranych informacji oraz metod i instrumentów reagować na zagrożenia bezpieczeństwa w cyberprzestrzeni w różnych obszarach życia społecznego i na różnych poziomach jego organizacji	P7U_U	P7S_UW
K_U02	komunikować różnym odbiorcom z zastosowaniem dobranej, specjalistycznej siatki pojęciowej o zagrożeniach w cyberprzestrzeni i sposobach przeciwdziałania im, prowadzić debaty na te tematy, także w języku obcym na poziomie minimum B2+	P7U_U	P7S_UK
K_U03	współdziałać w zespołach zajmujących się identyfikacją zagrożeń bezpieczeństwa w cyberprzestrzeni lub przeciwdziałaniem im oraz kierować pracami tych zespołów	P7U_U	P7S_UO
K_U04	samodzielnie planować i realizować własne uczenie się przez całe życie w zakresie różnorodności i zmiany zagrożeń bezpieczeństwa w cyberprzestrzeni i sposobów przeciwdziałania im także z uwzględnieniem technologii informatycznych	P7U_U	P7S_UU
K_U05	wykorzystywać posiadaną wiedzę do formułowania i rozwiązywania złożonych i nietypowych problemów dotyczących bezpieczeństwa systemów informatycznych	P7U_U	P7S_UW
K_U06	właściwie dobrać oraz zastosować metody i narzędzia z zakresu informatyki, ze szczególnym uwzględnieniem tych dotyczących analizy bezpieczeństwa systemów informatycznych	P7U_U	P7S_UW
K_U07	tworzyć algorytmy i programy komputerowe oraz wykorzystywać istniejące pakiety oprogramowania w celu zaprojektowania i wykonania analizy bezpieczeństwa systemów oraz formułować hipotezy badawcze związane z rozwiązywaniem prostych problemów badawczych	P7U_U	P7S_UW
	KOMPETENCJE SPOŁECZNE: ABSOLWENT JEST GOTÓW DO	Kod składnika opisu	Kod składnik opisu
K_K01	krytycznej oceny informacji na temat bezpieczeństwa systemów informatycznych, różnorodnych zagrożeń bezpieczeństwa w cyberprzestrzeni i sposobów przeciwdziałania im z wykorzystaniem specjalistycznej wiedzy	P7U_U	P7S_KK
K_K02	zgodnego z interesem publicznym, wykazując się przedsiębiorczością wypełniania w różnych obszarach życia społeczno-politycznego zobowiązań w zakresie identyfikacji zagrożeń bezpieczeństwa w cyberprzestrzeni i przeciwdziałania im	P7U_U	P7S_KO
K_K03	odpowiedzialnego pełnienia ról zawodowych na różnych poziomach organizacji życia społecznego, adaptowania się do zmieniających się potrzeb społecznych poprzez podnoszenie kwalifikacji w zakresie cyberbezpieczeństwa, dbania o etos zawodowy włącznie z przestrzeganiem zasad etyki zawodowej	P7U_U	P7S_KR

K_K04	krytycznej oceny posiadanej wiedzy i odbieranych treści z zakresu bezpieczeństwa systemów informatycznych	P7U_K	P7S_KK
K_K05	wypełniania zobowiązań społecznych, współorganizowania działalności na rzecz środowiska społecznego z wykorzystaniem technologii informatycznych	P7U_K	P7S_KO
K_K06	inicjowania działań na rzecz interesu publicznego z uwzględnieniem korzyści wynikłych z praktycznego wykorzystywania technik informacyjno-komunikacyjnych	P7U_K	P7S_KO