Tabela kierunkowych efektów uczenia się dla kierunku Cyberbezpieczeństwo

Kategoria PRK	Symbol	Kierunkowe efekty uczenia się	Kod składnika opisu
Wiedza: absolwent zna i rozumie	K1_W01	Ma rozszerzoną i pogłębioną wiedzę z zakresu algebry liniowej, analizy matematycznej, matematyki dyskretnej, probabilistyki i statystki niezbędną do opisu i analizy działania elementów i układów właściwych dla kierunku studiów	P6S_WG
	K1_W02	Ma zaawansowaną wiedzę z fizyki niezbędną do zrozumienia podstawowych zjawisk fizycznych występujących w elementach i układach elektronicznych oraz systemach komunikacyjnych	P6S_WG
	K1_W03	Posiada słownictwo ogólne języka obcego na poziomie B2 według ESOKJ oraz specjalistyczne słownictwo dotyczące wybranych obszarów informatyki i sztucznej inteligencji.	P6S_WG
	K1_W04	Zna kluczowe struktury gramatyczne potrzebne do opisywania i tłumaczenia zjawisk i procesów związanych ze studiowanym kierunkiem.	P6S_WG
	K1_W05	Ma zaawansowaną wiedzę w zakresie złożonych struktur danych; zna zasady administrowania danymi i związanymi z nimi standardami; zna zasady cyberbezpieczeństwa i prywatności wykorzystywane do zarządzania ryzykiem związanym z wykorzystywaniem, przetwarzaniem, przechowywaniem i przesyłaniem informacji lub danych	P6S_WG
	K1_W06	Ma zaawansowaną wiedzę w zakresie zasad tworzenia programów komputerowych, struktur języków programowania, ich poziomów oraz używanych algorytmów; ma zaawansowaną wiedzę z zakresu inżynierii oprogramowania;	P6S_WG
	K1_W07	Ma pogłębioną i wiedzę na temat typów i architektur sieci komputerowych oraz zasad ich projektowania, konfigurowania i utrzymania; zna i rozumie wykorzystywane w nich protokoły, algorytmy oraz mechanizmy.	P6S_WG
	K1_W08	Ma szczegółową wiedzę na temat budowy elektronicznych układów cyfrowych, w tym układów programowalnych; ma pogłębioną znajomość budowy komputerów oraz ich komponentów; zna i rozumie zachodzące w nich zjawiska oraz wykorzystywane mechanizmy	P6S_WG
	K1_W09	Ma pogłębioną wiedzę na temat cyklu życia, projektowania oraz eksploatacji odpornych na ataki programowych systemów informatycznych; zna i rozumie zasady ich działania; zna narzędzia wykorzystywanych do identyfikacji luk w oprogramowaniu komunikacyjnym; zna wpływ konfiguracji oprogramowania na bezpieczeństwo;	P6S_WG
	K1_W10	Rozumie pojęcie ataku sieciowego oraz jego powiązanie zarówno z zagrożeniami, jak i lukami w zabezpieczeniach; zna techniki wykrywania włamań do elementów infrastruktury sieciowej; Ma pogłębioną wiedzę na temat wektorów ataku na infrastrukturę sieciową oraz metod analizy ruchu sieciowego w celu wykrycia naruszeń bezpieczeństwa sieci; dysponuje zaawansowaną wiedzę w zakresie zabezpieczeń sieciowych	P6S_WG
	K1_W11	Ma pogłębioną wiedzę na temat projektowania, konfigurowania oraz utrzymania systemów komputerowych, w tym systemów rozproszonych; zna i rozumie wykorzystywane w nich mechanizmy	P6S_WG
	K1_W12	Ma pogłębioną wiedzę w zakresie uwierzytelniania, autoryzacji i zasad sterowania dostępem do systemów komputerowych; jest świadom konieczności stosowania polityk sterowania dostępem oraz ich adaptacji do poziomu ryzyka; zna zasady uwierzytelniania biometrycznego;	P6S_WG

	K1_W13	Zna zasady ukrywania danych, tj. kryptografię i steganografię; ma zaawansowaną wiedzę z zakresu kryptografii, algorytmów kryptograficznych i ich ograniczeń oraz ich znaczenia dla cyberbezpieczeństwa; ma poszerzoną wiedzę w zakresie kompresji danych	P6S_WG
	K1_W14	Ma ogólną wiedzę na temat kluczowych zagadnień przetwarzania rozproszonego oraz zaawansowaną wiedzę szczegółową dotyczącą zagadnień przetwarzania chmurowego dostępnego na rynku; zna modele usług chmurowych oraz koncepcje związane z ich bezpieczeństwem, zarządzaniem, zamówieniami i administracją; zna ekonomiczne, prawne i inne uwarunkowania działalności firm świadczących usługi chmurowe.	P6S_WG
	K1_W15	Ma wiedzę na temat zasad, wymagań i procedur związanych z bezpieczeństwem łańcucha dostaw technologii informatycznych oraz zarządzania ryzykiem w łańcuchu dostaw; jest świadomy konieczności stosowania przepisów, polityk, procedur kluczowych dla cyberbezpieczeństwa infrastruktury krytycznej; zna procesy zarządzania ryzykiem, w tym metody jego oceny i ograniczania;.	P6S_WG
	K1_W16	Ma podstawową wiedzę na temat systemów maszynowego uczenia się i sztucznych sieci neuronowych; uporządkowaną wiedzę dotyczącą zasad oraz metod rozwiązywania problemów decyzyjnych i optymalizacyjnych, w tym algorytmów heurystycznych i nieheurystycznych do przeszukiwania przestrzeni stanów, również z uwzględnieniem ograniczeń zasobowych; zna metody sztucznej inteligencji stosowane w zagadnieniach związanych z cyberbezpieczeństwem.	P6S_WG
	K1_W17	Ma pogłębioną wiedzę na temat do przepisów prawa, regulacji, zasad i norm etycznych w zakresie cyberbezpieczeństwa i prywatności; jest świadom skutków operacyjnych naruszeń cyberbezpieczeństwa; ma również dogłębną znajomość zasad ochrony prywatności oraz wymagań organizacyjnych (obejmujących poufność, integralność, dostępność, uwierzytelnianie i niezaprzeczalność);	P6S_WG
	K1_W18	Zna i rozumie zagrożenia, na które narażona jest współczesna cywilizacji masowo wykorzystująca usługi cyfrowe; orientuje się w najnowszych trendach rozwojowych związanych ze studiowanym kierunkiem	P6S_WK
	K1_W19	Ma podstawową wiedzę dotyczącą zarządzania projektami informatycznymi i teleinformatycznymi	P6S_WK
	K1_W20	Ma podstawową wiedzę dotyczącą tworzenia, zarządzania i prowadzenia oraz rozwoju działalności gospodarczej związanej z nadaną kwalifikacją;	P6S_WK
	K1_W21	Ma podstawową wiedzę niezbędną do zrozumienia społecznych, etycznych, ekonomicznych, ekologicznych, prawnych i innych pozatechnicznych uwarunkowań działalności inżynierskiej	P6S_WK
	K1_W22	Ma podstawową wiedzę w zakresie patentów oraz stosowania prawa autorskiego, ustawy o ochronie danych osobowych oraz własności przemysłowej i intelektualnej	P6S_WK
Umiejętności: absolwent potrafi	K1_U01	Potrafi korzystać ze źródeł literaturowych, integrować pozyskane informacje, oceniać je oraz dokonywać ich interpretacji i wyciągać wnioski, w celu rozwiązania złożonych i nietypowych problemów w obszarze cyberbezpieczeństwa	P6S_UW
	K1_U02	Potrafi korzystać z odpowiednio dobranych metod i narzędzi, w tym zaawansowanych technik informacyjno-komunikacyjnych; umie również opracować proste aplikacje lub skonfigurować podstawowy system w celu przeprowadzenia symulacji, analizy oraz projektowania systemów lub aplikacji zgodnych z profilem	P6S_UW

		kierunku studiów	
	K1_U03	Potrafi zaplanować i przeprowadzić testy oprogramowania oraz systemów i sieci komputerowych w celu wykrycia w nich podatności na ataki; potrafi zaproponować rozwiązania poprawiające bezpieczeństwo działania	P6S_UW
	K1_U04	Potrafi zaplanować i przeprowadzić symulacje komputerowe i pomiary, w tym symulacje i pomiary dotyczące działania systemów teleinformatycznych, potrafi przedstawić otrzymane wyniki w formie liczbowej i graficznej, dokonać ich interpretacji i wyciągnąć właściwe wnioski	P6S_UW
	K1_U05	Przy formułowaniu i rozwiązaniu zadań inżynierskich z zakresu cyberbezpieczeństwa potrafi wykorzystać znane modele matematyczne i algorytmy oraz metody symulacyjne, eksperymentalne i analityczne	P6S_UW
	K1_U06	Przy formułowaniu zadań inżynierskich potrafi dokonać wstępnej oceny ekonomicznej zaprojektowania, implementacji, konfiguracji i utrzymania oprogramowania i systemów spełniających wymogi cyberbezpieczeństwa i zachowania prywatności	P6S_UW
	K1_U07	Potrafi, przy formułowaniu i rozwiązywaniu zadań dotyczących cyberbezpieczeństwa, dostrzegać ich aspekty systemowe i pozatechniczne, w tym etyczne, ekonomiczne i prawne	P6S_UW
	K1_U08	Potrafi dokonać porównania różnych rozwiązań technicznych, ocenić je ze względu na wybrane kryteria użytkowe, ekonomiczne, ekologiczne, prawne oraz etyczne	P6S_UW
	K1_U09	Potrafi, z wykorzystaniem odpowiednio dobranych metod oraz narzędzi, dokonać krytycznej analizy i oceny funkcjonowania istniejących rozwiązań stosowanych w oprogramowaniu, przetwarzaniu danych oraz systemach i sieciach komputerowych	P6S_UW
	K1_U10	Na podstawie dostępnej dokumentacji i specyfikacji oraz standardów potrafi zaprojektować i zaimplementować w językach wysokiego poziomu bezpieczną aplikację internetową lub mobilną	
	K1_U11	Na podstawie dokumentacji technicznej, obowiązujących standardów, przy użyciu właściwych metod, narzędzi i elementów, potrafi zbudować, skonfigurować i uruchomić typowy system lub sieć komputerową spełniające wymogi cyberbezpieczeństwa	P6S_UW
	K1_U12	Potrafi przygotować i przedstawić prezentację w języku polskim i obcym na temat zadania związanego z kierunkiem studiów, komunikuje się z użyciem specjalistycznej terminologii, przedstawia i uzasadnia różne opinie i stanowiska	P6S_UK
	K1_U13	Potrafi przygotować i ustnie przedstawić w języku polskim i obcym zwarte opracowanie o aktualnych problemach cyberbezpieczeństwa; umie prowadzić dyskusję popularyzującą zagadnienia związane z kierunkiem studiów, a swoje poglądy popierać wiedzą inżynierską	P6S_UK
	K1_U14	Ma umiejętności w zakresie języka obcego na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego, a także umie czytać ze zrozumieniem karty katalogowe, normy, dokumentacje techniczne oraz instrukcje obsługi układów i urządzeń właściwych dla kierunku studiów	P6S_UK
	K1_U15	Potrafi planować oraz organizować pracę indywidualną i w zespole (w tym opracować i zrealizować harmonogram prac zapewniający dotrzymanie terminu), stosuje zasady bezpieczeństwa i higieny pracy, a także umie pracować w zespołach o charakterze interdyscyplinarnym i wielokulturowym	P6S_UO
	K1_U16	Potrafi samodzielnie planować i realizować własne uczenie się przez całe życie (np. studia drugiego i trzeciego stopnia, studia	P6S_UU

		podyplomowe, kursy prowadzane przez firmy i organizacje zawodowe) w celu podnoszenia kompetencji zawodowych i społecznych	
Kompetencje: absolwent jest gotów do	K1_K01	Rozumie znaczenie podnoszenia kompetencji zawodowych, osobistych i społecznych; ma świadomość, że wiedza i umiejętności w obszarze cyberbezpieczeństwa szybko ewoluują	P6U-KK
	K1_K02	Rozumie znaczenie wiedzy w rozwiązywaniu problemów z zakresu cyberbezpieczeństwa; jest świadomy konieczności wykorzystania wiedzy ekspertów podczas rozwiązywania zadań inżynierskich w zakresie wykraczającym poza własne kompetencje	P6U-KK
	K1_K03	Jest świadomy społecznej roli absolwenta uczelni technicznej, w szczególności rozumie potrzebę formułowania i przekazywania społeczeństwu informacji na temat cyberbezpieczeństwa, w tym jego pozytywnych i negatywnych aspektów, informacji oraz opinii dotyczących działalności inżynierskiej, osiągnięć techniki, a także dorobku i tradycji zawodu informatyka, a także jest gotowy do działania na rzecz interesu publicznego	P6U-KO
	K1_K04	Potrafi myśleć i działać w sposób przedsiębiorczy w obszarze cyberbezpieczeństwa	P6U-KO
	K1_K05	Ma świadomość znaczenia pracy własnej i konieczności przestrzegania zasad etyki zawodowej, jest gotowy do podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania, a także dbałości o dorobek i tradycje zawodu	P6U-KR