

ZAKŁADANE EFEKTY UCZENIA SIĘ

Wydział: Informatyki i Telekomunikacji

Kierunek studiów: Cyberbezpieczeństwo

Poziom studiów: studia pierwszego stopnia / ~~drugiego stopnia~~ / ~~jednolite studia magisterskie~~*

Profil: ogólnoakademicki / ~~praktyczny~~*

Umiejscowienie kierunku

Dziedzina nauki: nauki techniczne

Dyscyplina/dyscypliny w przypadku kilku dyscyplin proszę wskazać dyscyplinę wiodącą)

...informatyka i telekomunikacja

Objaśnienie oznaczeń:

P6U – charakterystyki uniwersalne odpowiadające kształceniu na studiach pierwszego stopnia - 6 poziom PRK*

P7U – charakterystyki uniwersalne odpowiadające kształceniu na studiach drugiego stopnia - 7 poziom PRK*

P6S – charakterystyki drugiego stopnia odpowiadające kształceniu na studiach pierwszego stopnia studiów - 6 poziom PRK *

P7S – charakterystyki drugiego stopnia odpowiadające kształceniu na studiach drugiego stopnia/ jednolitych magisterskich – 7 poziom PRK*

W – kategoria „wiedza”

U – kategoria „umiejętności”

K – kategoria „kompetencje społeczne”

K(symbol kierunku)_W1, K(symbol kierunku)_W2, K(symbol kierunku)_W3, ...- efekty kierunkowe dot. kategorii „wiedza”

K(symbol kierunku)_U1, K(symbol kierunku)_U2, K(symbol kierunku)_U3, ...- efekty kierunkowe dot. kategorii „umiejętności”

K(symbol kierunku)_K1, K(symbol kierunku)_K2, K(symbol kierunku)_K3, ...- efekty kierunkowe dot. kategorii „kompetencje społeczne”

S(symbol specjalności)_W..., S(symbol specjalności)_W..., S(symbol specjalności)_W..., ...- efekty specjalnościowe dot. kategorii „wiedza”

S(symbol specjalności)_U..., S(symbol specjalności)_U..., S(symbol specjalności)_U..., ...- efekty specjalnościowe dot. kategorii „umiejętności”

S(symbol specjalności)_K..., S(symbol specjalności)_K..., S(symbol specjalności)_K..., ...- efekty specjalnościowe dot. kategorii „kompetencje społeczne”

...._inż – efekty uczenia się umożliwiające uzyskanie kompetencji inżynierskich

*niepotrzebne usunąć

Kierunkowe efekty uczenia się

Symbol kierunkowych efektów uczenia się	Opis efektów uczenia się dla kierunku studiów Po ukończeniu kierunku studiów absolwent:	Odniesienie do charakterystyk PRK		
		Uniwersalne charakterystyki pierwszego stopnia (U)	Charakterystyki drugiego stopnia typowe dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego (S)	
			Charakterystyki dla kwalifikacji na poziomach 6/7* PRK	Charakterystyki dla kwalifikacji na poziomach 6 i 7 PRK, umożliwiających uzyskanie kompetencji inżynierskich
WIEDZA (W)				
K1CBE_W01	Zna podstawy metrologii, teorii i techniki pomiarów wielkości elektrycznych. Zna sprzęt pomiarowy stosowany w pomiarach wielkości elektrycznych. Jest w stanie scharakteryzować potrzeby pomiarowe, wskazać wielkości mierzone, dobrać metodykę pomiaru i oszacować niepewność. Zna rolę pomiarów i wpływ miarodajności i dokładności pomiarów w zapewnieniu niezawodności i bezpieczeństwa systemów teleinformatycznych i bieżącej ocenie jakości ich pracy.	P6U_W	P6S_WG	P6S_WG
K1CBE_W02	Zna pojęcie algorytmu oraz metody jego reprezentacji, podstawowe konstrukcję języków algorytmicznych, pojęcie rekurencji, zasady programowania strukturalnego, podstawowe algorytmy sortowania i przeszukiwania danych, a także dynamiczne i złożone struktury danych.	P6U_W	P6S_WG	P6S_WG
K1CBE_W03	Zna podstawy technik informatycznych, usług sieciowych oraz technologii zapewnienia bezpieczeństwa związanych z pozyskiwaniem, przetwarzaniem i prezentowaniem informacji.	P6U_W	P6S_WG	
K1CBE_W04	Ma podstawową i podbudowaną teoretycznie wiedzę niezbędną do rozumienia społecznych, etycznych i filozoficznych uwarunkowań działalności inżynierskiej, zna i rozumie pojęcia z zakresu ochrony własności przemysłowej, prawa autorskiego, przedsiębiorczości i zarządzania jakością	P6U_W	P6S_WG	
K1CBE_W05	Ma podstawową wiedzę w zakresie wybranych działów matematyki i fizyki niezbędną do rozumienia zagadnień w zakresie cyberbezpieczeństwa	P6U_W	P6S_WG	
K1CBE_W06	Posiada ogólną, przekrojową wiedzę o zasadniczych obszarach telekomunikacji, w tym: procesach przetwarzania sygnału, mediach	P6U_W	P6S_WG	

	transmisyjnych i sieciach oraz systemach. Aspekty te zna od strony funkcjonalnej, ale osadzonej także w kontekście cyberbezpieczeństwa, tzn. istniejących zagrożeń i ogólnych rekomendacji związanych z ich redukcją, stosowanych w różnej klasy systemach telekomunikacyjnych.			
K1CBE_W07	Zna podstawy teorii i techniki systemów z uwzględnieniem specyfiki cybernetycznych systemów krytycznych, w tym zagadnienia klasyfikacji i modelowania systemów oraz zarządzania systemami o różnych strukturach.	P6U_W	P6S_WG	
K1CBE_W08	Ma podstawową wiedzę o celach i strukturze układów sterowania. Zna podstawowe struktury układów regulacji oraz regulatorów liniowych. Ma wiedzę dotyczącą sterowników PLC, DCS, systemów SCADA ze szczególnym uwzględnieniem aspektów cyberbezpieczeństwa. Ma ogólną wiedzę na temat konstrukcji robotów, ich budowy, i zastosowania, ma elementarną wiedzę z zakresu sterowania i języków programowania robotów. Ma podstawową wiedzę z zakresu doboru regulatorów i nastaw regulatorów, czujników, sterowników przemysłowych, oraz urządzeń wykonawczych. Zna podstawowe cele i cechy budynków inteligentnych oraz związane z nimi problemy cyberbezpieczeństwa.	P6U_W	P6S_WG	
K1CBE_W09	Zna podstawy inżynierii i metodologii programowania obiektowego.	P6U_W	P6S_WG	P6S_WG
K1CBE_W10	Posiada wiedzę na temat cyfrowego kanału telekomunikacyjnego, jego poszczególnych elementów i związanych z nim funkcji i stosowanych kodów liniowych.	P6U_W	P6S_WG	P6S_WG
K1CBE_W11	Zna strukturę wewnętrzną i metody programowania mikroprocesorów i mikrokontrolerów.	P6U_W	P6S_WG	P6S_WG
K1CBE_W12	Ma ogólną wiedzę dotyczącą systemów zarządzania bezpieczeństwem informacji (SZBI) zgodnych z normami/regulacjami europejskimi (NIS) i krajowymi (ustawa KSC), budowy systemów ochrony: informacji niejawnych, danych osobowych i informacji objętych tajemnicą zawodową. Potrafi określić wymagania oraz obszary związane z projektowaniem i wdrażaniem Polityki Bezpieczeństwa Informacji w zależności od charakteru przedsiębiorstwa. Potrafi określić hierarchię i metody dostępu do informacji niejawnej. Potrafi określić ogólne ramy obowiązków osób odpowiedzialnych za ochronę informacji i systemów informatycznych w organizacji.	P6U_W	P6S_WG	P6S_WG
K1CBE_W13	Posiada podstawową wiedzę z zakresu budowy systemów operacyjnych, roli i zasad działania ich podsystemów, a także zna podstawowe algorytmy szeregowania zadań.	P6U_W	P6S_WG	P6S_WG

K1CBE_W14	Zna podstawowe zagadnienia z zakresu teorii cyfrowego przetwarzania sygnałów deterministycznych i losowych będących nośnikami informacji, w szczególności zagadnienia: próbkowania, kwantyzacji, detekcji i filtracji.	P6U_W	P6S_WG	P6S_WG
K1CBE_W15	Posiada wiedzę na temat systemów kryptograficznych w telekomunikacji oraz wiedzę umożliwiającą rozróżnianie metod szyfrowania informacji.	P6U_W	P6S_WG	P6S_WG
K1CBE_W16	Zna podstawowe pojęcia i twierdzenia z teorii pola elektromagnetycznego.	P6U_W	P6S_WG	P6S_WG
K1CBE_W17	Ma wiedzę dotyczącą funkcjonowania sieci komputerowych, modelem odniesienia, topologią, elementami sieci, protokołami komunikacyjnymi, w szczególności: potrafi wytłumaczyć działanie urządzeń sieciowych z protokołem TCP/IP, obejmującą planowanie adresacji IP, klasowe i bezklasowe mechanizmy wyboru trasy, rutowanie statyczne i dynamiczne oraz techniki przełączania w sieciach Ethernet.	P6U_W	P6S_WG	P6S_WG
K1CBE_W18	Zna podstawowe pojęcia związane z bezpieczeństwem i metodami jego zwiększania w systemach operacyjnych, Zna podstawowe pojęcia audytu technicznego i testów penetracyjnych. Zna podstawowe narzędzia monitorowania bezpieczeństwa systemów i ich cechy Zna zastosowanie narzędzi: monitorowania bezpieczeństwa systemów, audytu technicznego i testów penetracyjnych.	P6U_W	P6S_WG	P6S_WG
K1CBE_W19	Posiada ogólną, przekrojową wiedzę z zakresu kompatybilności elektromagnetycznej (KEM) oraz powiązanymi aspektami bezpieczeństwa elektromagnetycznego i cyberbezpieczeństwa różnych urządzeń i systemów, obejmującą architekturę bezpieczeństwa i potencjalne źródła zagrożeń EM występujące w różnych środowiskach EM (w tym także terroryzm elektromagnetyczny), zjawiska fizyczne i drogi wnikania zaburzeń EM do wnętrza urządzeń oraz ich ulotu na zewnątrz, stosowane techniki oraz środki techniczne i organizacyjne zwiększające poziom bezpieczeństwa EM oraz niezawodność działania urządzeń i systemów, stosowane metody testowania i oceny bezpieczeństwa EM oraz klasyfikacji zabezpieczeń a także Identyfikacji krytycznych infrastruktur, elementów infrastruktury, urządzeń i ich części oraz oprogramowania istotnych dla życia i zdrowia ludzkiego oraz funkcjonowania państwa i gospodarki.	P6U_W	P6S_WG	P6S_WG
K1CBE_W20	Ma wiedzę z zakresu działania sieci w topologii nadmiarowej z przełącznikami z użyciem VLAN. Zna metody działania i sposób zastosowania protokołów dynamicznego wyboru trasy. Zna typowe protokoły stosowane w sieciach rozległych WAN oraz metody dołączania LAN do ISP.	P6U_W	P6S_WG	P6S_WG

K1CBE_W21	Ma ogólną wiedzę z zarządzania infrastrukturą teleinformatyczną, obejmującą funkcje i obszary zarządzania, w szczególności: dotyczącą teorii niezawodności i zarządzania oraz niezawodnościowych modeli sieci telekomunikacyjnych. Jest w stanie opisać proces eksploatacji oraz cechy zarządzania jakością. Ma wiedzę na temat podstawowych norm i metod zarządzania TMN i ITSM (w szczególności ITIL) oraz organizacji centrum zarządzania (NOC). Ma ogólną wiedzę związaną z miejscem w organizacji i zadaniami grupy /zespołu klasy SOC (Security Operation Center) i powiązania z NOC.	P6U_W	P6S_WG	P6S_WG
K1CBE_W22	Ma ogólną wiedzę na temat organizacji i usług bezpieczeństwa realizowanych w ramach Security Operation Center (SOC) oraz sposobów i metod monitorowania oraz detekcji zagrożeń w systemach informatycznych. Ma ogólną wiedzę na temat struktury organizacji i architektury systemów wykrywania zagrożeń. Zna systemy wykrywające zagrożenia oraz systemy prewencyjne, rozumie analizę korelacji zdarzeń w systemach komputerowych, wie jak dobrać oraz skonfigurować narzędzia monitorujące zagrożenia, w szczególności jak przygotować sondy monitorujące.	P6U_W	P6S_WG	P6S_WG
K1CBE_W23	Zna metody i mechanizmy zapewniające bezpieczeństwo w sieciach komputerowych, w tym: warunkowego dostępu, filtrowania ruchu oraz utajniania treści. Ma wiedzę o metodach uwierzytelniania i szyfrowania, wykrywania i przeciwdziałania atakom.	P6U_W	P6S_WG	P6S_WG
K1CBE_W24	Ma wiedzę na temat stosowanych metod audytu formalnego oraz technicznego a w szczególności podstawowe założenia norm ISO rodziny 27000. Ma ogólną wiedzę na temat struktury organizacji i architektury systemów wykrywania zagrożeń. Ma wiedzę na temat narzędzi i metod audytu technicznego oraz zna wybrane metody audytu technicznego oraz zastosowanie wybranych narzędzi do audytu technicznego i testów penetracyjnych. Ma wiedzę ogólną w zakresie metodyk zarządzania ryzykiem.	P6U_W	P6S_WG	P6S_WG
K1CBE_W25	Ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie wybranych działów cyberbezpieczeństwa; zna i rozumie wybrane zagadnienia stanowiące wiedzę szczegółową, właściwe dla programu kształcenia w ramach określonej specjalności.	P6U_W	P6S_WG	P6S_WG
UMIĘTNOŚCI (U)				
K1CBE_U01	Potrafi rozwiązywać zadania obliczeniowe z użyciem narzędzi komputerowych.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U02	Potrafi przygotować i skonfigurować środowisko uruchomieniowe oraz uruchamiać skrypty dla różnych języków programowania. Potrafi napisać skrypty przetwarzające dane z plików; pobierać i przetwarzać dane z internetu za pomocą interfejsów API. Potrafi automatyzować za pomocą skryptów zadania systemowe.	P6U_U	P6S_UW	P6S_UW_INŻ

K1CBE_U03	Umie zapisać algorytm w postaci schematu blokowego, podać rozwiązanie prostych zadań w postaci algorytmów oraz podać sposób ich testowania. Umie korzystać ze środowiska informatycznego oraz programować z użyciem typów prostych, łańcuchów znakowych, pętli, procedur i funkcji.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U04	Umie posługiwać się edytorami tekstów, arkuszami kalkulacyjnymi, wykonać prezentację multimedialną, publikować informacje w sieci, przesyłać dane w sieci, kontrolować i konfigurować politykę bezpieczeństwa aplikacji.	P6U_U	P6S_UW	
K1CBE_U05	Potrafi posługiwać się metodami matematyki i fizyki do rozwiązywania szczegółowych problemów w obszarze cyberbezpieczeństwa	P6U_U	P6S_UW	
K1CBE_U06	Posiada umiejętność modelowania systemów oraz stosowania prostych algorytmów do rozwiązywania zadań z zakresu identyfikacji i rozpoznawania systemów oraz sterowania systemami.	P6U_U	P6S_UW	
K1CBE_U07	Umie samodzielnie tworzyć programy zorientowane obiektowo.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U08	Potrafi tworzyć aplikacje dla systemu Android wraz z obsługą komunikacji z peryferiami urządzenia mobilnego oraz projektować i implementować własne interfejsy użytkownika.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U09	Potrafi analizować właściwości kodu oraz ma umiejętność jego zaprojektowania.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U10	Potrafi przygotować i uruchomić oprogramowanie wykorzystujące strukturę wewnętrzną mikrokontrolerów.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U11	Umie dokonać wstępnego przeglądu standardów ochrony informacji, potrafi przedstawić założenia poszczególnych dokumentów normatywnych i prawnych. Umie omówić niezbędne mechanizmy prawne oraz zasady, metody i instrumenty ochrony informacji oraz problem odpowiedzialności za naruszenie prawa chroniącego informację. Potrafi określić założenia i zakres Polityki Bezpieczeństwa Informacji organizacji	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U12	Potrafi korzystać z systemu operacyjnego Linux w zakresie średnio zaawansowanego użytkownika, w tym pisać proste skrypty powłoki, stosując podstawowe konstrukcje pętli, instrukcje warunkowe oraz metody przekazywania parametrów.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U13	Umie dokonać analizy własności sygnałów w dziedzinie czasowej i częstotliwościowej i syntezy filtrów cyfrowych z użyciem dedykowanego oprogramowania.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U14	Potrafi rozwiązywać podstawowe zagadnienia teorii pola elektromagnetycznego	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U15	Potrafi konfigurować hosty i routery do pracy w sieci lokalnej, stosować narzędzia diagnostyczne, obserwować i analizować	P6U_U	P6S_UW	P6S_UW_INŻ

	zdarzenia sieciowe. Potrafi zaplanować adresację IP, podłączyć i skonfigurować routery i przełączniki, użyć protokoły dynamicznego routowania.			
K1CBE_U16	Potrafi przeanalizować sposoby ochrony systemu operacyjnego (w tym konfiguruje komponenty bezpieczeństwa systemu) oraz rozpoznać podstawowe zagrożenia oraz ataki. Potrafi wdrożyć zalecenia norm i rekomendacji do systemu operacyjnego oraz mierzyć ich skuteczność - wykonać audyt bezpieczeństwa.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U17	Ma umiejętności i kompetencje zgodne z wymaganiami określonymi dla poziomu; pozyskuje, rozumie i interpretuje teksty specjalistyczne; śledzi ze zrozumieniem i formułuje wypowiedzi na tematy związane ze studiowaną dyscypliną oraz pracą zawodową, stosując środki adekwatne do sytuacji; czyta, interpretuje, ocenia i tworzy teksty o tematyce specjalistycznej; wykorzystuje sprawności językowe w kontaktach interpersonalnych i w komunikacji w międzynarodowym środowisku akademickim i zawodowym.	P6U_U	P6S_UK	
K1CBE_U18	Potrafi wytypować właściwe metody testowania EMC i oceny bezpieczeństwa, skonfigurować stanowiska i urządzenia, wykonać podstawowe testy oraz opracowywać i zinterpretować otrzymane wyniki badań. Potrafi zastosować dostępne techniki i materiały do rozwiązywania podstawowych problemów związanych z KEM i bezpieczeństwem elektromagnetycznym, wyznaczać ich parametry techniczne stosowanych zabezpieczeń, dokonywać ich klasyfikacji oraz ocenić skuteczność zastosowania.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U19	Umie selektywnie poszukiwać wiedzę w zakresie zagadnień cyberbezpieczeństwa powiązane go z aspektami EMC oraz komunikatywnie ją zaprezentować z merytoryczną argumentacją rozwiązań technicznych i organizacyjnych oraz własnego stanowiska i poglądu, popartego gruntowną wiedzą zdobytą w trakcie gromadzenia materiałów do przygotowania wystąpienia.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U20	Potrafi konfigurować i diagnozować sieci w topologii nadmiarowej z przełącznikami z użyciem VLAN oraz zastosować protokoły dynamicznego wyboru trasy. Potrafi konfigurować i diagnozować sieci z typowymi protokoły stosowane w sieciach rozległych WAN oraz podłączać LAN do ISP.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U21	Potrafi sformułować i zaprezentować główne cele oraz zadania zarządzania, utrzymania i ochrony infrastruktury teleinformatycznej przetwarzania informacji organizacji. Potrafi zinterpretować podstawowe elementy modelu zarządzania infrastruktura i usługami. Potrafi definiować parametry niezawodnościowych modeli sieci teleinformatycznej oraz określać wymagania związane z eksploatacją urządzeń i systemów. Potrafi wskazać mechanizmy zapewniania	P6U_U	P6S_UW	P6S_UW_INŻ

	ciągłości świadczenia usług dla systemów wspierających infrastrukturę teleinformatyczną.			
K1CBE_U22	Umie zaimplementować narzędzia monitorujące zdarzenia oraz bezpieczeństwo w systemie komputerowym. Potrafi przygotować system składający się z wielu komponentów do monitorowania zagrożeń. Potrafi dobrać sondy dla różnych kategorii zdarzeń w monitorowanym systemie. Umie korelować zdarzenia pochodzące z wielu źródeł danych i używać wskaźników jakościowych i ilościowych, np. ocenić skuteczność wdrożonego systemu monitorowania.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U23	Umie projektować rozwiązania mające na celu monitorowanie oraz wykrywanie zagrożeń w systemach informatycznych. Umie dobrać i zaprojektować sondy danych do pojawiających się zagrożeń, tak by móc korelować pochodzące z nich informacje. Umie przeanalizować i dobrać do charakterystyki informacji przedsiębiorstwa narzędzia kolekcji zdarzeń i wykrywania zagrożeń klasy SIEM.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U24	Potrafi skonfigurować i uruchomić mechanizmy bezpieczeństwa na ruterach i urządzeniach firewall, tunele szyfrowane i mechanizmy IDS.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U25	Potrafi używać narzędzi audytu technicznego do przetestowania bezpieczeństwa aplikacji sieciowej. Potrafi zaplanować poszczególne etapy testu penetracyjnego i określić ich kryteria. Potrafi wykonać poszczególne etapy testu penetracyjnego i przygotować raport. Potrafi dokonać mapowania potrzeb (formalnych i związanych z cechami organizacji) oraz niezbędnego poziomu organizacji usług bezpieczeństwa.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U26	Ma przygotowanie niezbędne do pracy w środowisku przemysłowym oraz znajomość zasad bezpieczeństwa związanych ze stanowiskiem pracy.	P6U_U	P6S_UO, P6S_UU	P6S_UO_INŻ, P6S_UU_INŻ,
K1CBE_U27	Umie zaproponować i zestawić układ pomiarowy adekwatny do potrzeb oraz wykonać pomiary przyrządami wielkości elektrycznych, oszacować ich wiarygodność i ocenić niepewność.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U28	Potrafi wykorzystywać posiadaną wiedzę specjalistyczną do formułowania i rozwiązywania złożonych i nietypowych problemów z wybranych zagadnień cyberbezpieczeństwa, pozyskiwać specjalistyczne informacje ze źródeł, dokonywać ich analizy, syntezy i oceny przydatności do realizowanych zadań.	P6U_U	P6S_UW	P6S_UW_INŻ
KOMPETENCJE SPOŁECZNE (K)				
K1CBE_K01	Prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu inżyniera; Ma świadomość roli społecznej absolwenta uczelni technicznej. Rozumie potrzebę formułowania i przekazywania społeczeństwu informacji i opinii dotyczących osiągnięć techniki i innych aspektów działalności inżyniera; Potrafi	P6U_K	P6S_KR	

	przekazać taką informację i opinie w sposób zrozumiały, z uzasadnieniem różnych punktów widzenia.			
K1CBE_K02	Rozumie prawne aspekty i skutki działalności inżynierskiej.	P6U_K	P6S_KR	
K1CBE_K03	Ma świadomość ważności i zrozumienie humanistycznych aspektów i skutków działalności inżynierskiej. Poznaje skutki wpływu działalności technicznej na środowisko, i związaną z tym odpowiedzialność społeczną nauki i techniki.	P6U_K	P6S_KK	
K1CBE_K04	Ma świadomość niezbędności aktywności indywidualnych i zespołowych wykraczających poza działalność inżynierską.	P6U_K		
K1CBE_K05	Rozumie ideę normalizacji, certyfikacji i integracji systemów zarządzania jakością, ochroną środowiska, bezpieczeństwem pracy i bezpieczeństwem informacji. Rozumie koncepcję zarządzania przez jakość. Identyfikuje podstawowe problemy zarządzania jakością, w tym kosztów jakości oraz zasady ich rozwiązywania. Zna ogólne zasady tworzenia i rozwoju form indywidualnej przedsiębiorczości.	P6U_K	P6S_KO	
K1CBE_K06	Potrafi współpracować z zespołem przy realizacji złożonego zadania inżynierskiego. Potrafi przedstawić efekty swojej pracy w zrozumiałej formie. Rozumie konieczność samokształcenia oraz rozwijania zdolności do samodzielnego stosowania posiadanej wiedzy i umiejętności	P6U_K	P6S_KK	

*niepotrzebne usunąć