

KIERUNKOWE EFEKTY KSZTAŁCENIA

Wydział: Elektroniki
Kierunek studiów: Cyberbezpieczeństwo (CB)
Studia w j. polskim

Stopień studiów: Pierwszy (1)
Profil: Ogólnoakademicki (A)

Umiejscowienie kierunku w obszarze kształcenia:

Kierunek studiów Cyberbezpieczeństwo o profilu ogólnoakademickim należy do obszaru i dziedziny kształcenia w zakresie nauk technicznych, w dyscyplinach informatyka i telekomunikacja.

Na kierunku prowadzone są dwie specjalności:

- Bezpieczeństwo sieci teleinformatycznych (BST)
- Bezpieczeństwo danych (BD)

Warunkiem uzyskania dyplomu z daną specjalnością jest zrealizowanie w trakcie studiów co najmniej grupy kursów wybieralnych przypisanych do tej specjalności oraz przygotowanie pracy dyplomowej (inżynierskiej) o tematyce bezpośrednio związanej z tą specjalnością.

Kwalifikacje absolwenta:

Po ukończeniu studiów pierwszego stopnia na kierunku Cyberbezpieczeństwo absolwent uzyskuje kompetencje pierwszego stopnia i otrzymuje tytuł zawodowy inżyniera, potwierdzony dyplomem ukończenia studiów wyższych pierwszego stopnia wydanym przez Politechnikę Wrocławską.

Liczba punktów ECTS konieczna do uzyskania kwalifikacji: 210

Do dyplomu wpisuje się jedną z dwóch specjalności:

- Bezpieczeństwo sieci teleinformatycznych
- Bezpieczeństwo danych

Objaśnienia oznaczeń:

- K1CB - symbol dla kierunku na pierwszym stopniu studiów - kierunkowe efekty kształcenia
 - _W01 - symbole dla efektów kształcenia w zakresie WIEDZY
 - _U01 - symbole dla efektów kształcenia w zakresie UMIEJĘTNOŚCI
 - _K01 - symbole dla efektów kształcenia w zakresie KOMPETENCJI SPOŁECZNYCH
 - _BST - symbole dla kierunku na pierwszym stopniu studiów – specjalnościowe efekty kształcenia dla specjalności: Bezpieczeństwo sieci teleinformatycznych
 - _BD - symbole dla kierunku na pierwszym stopniu studiów – specjalnościowe efekty kształcenia dla specjalności: Bezpieczeństwo danych

Dla precyzyjnego określenia odniesienia do definicji zapisanych w charakterystyce drugiego stopnia Polskiej Ramy Kwalifikacji wprowadzono rozszerzenia oraz ponumerowano poszczególne składniki:

- _NT – obszar kształcenia w zakresie nauk technicznych
- _INŻ – kwalifikacje obejmujące kompetencje inżynierskie

Efekty kształcenia na I stopniu studiów dla kierunku CBE	OPIS KIERUNKOWYCH EFEKTÓW KSZTAŁCENIA Po zakończeniu studiów I stopnia na kierunku CYBERBEZPIECZEŃSTWO absolwent:	Odniesienie efektów kształcenia dla obszaru nauk technicznych (T)
WIEDZA		
K1CB_W01	Zna podstawy metrologii, teorii i techniki pomiarów wielkości elektrycznych.	P6U_W, P6S_WG
K1CB_W02	Umie formułować i definiować zadania dotyczące użycia komputerowych narzędzi obliczeniowych w zagadnieniach typowych dla elektroniki i telekomunikacji.	P6U_W, P6S_WG
K1CB_W03	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
K1CB_W04	Zna podstawy technik informatycznych (w tym usług sieciowych) związanych z pozyskiwaniem, przetwarzaniem i prezentowaniem informacji.	P6U_W, P6S_WG
K1CB_W05	Ma podstawową wiedzę niezbędną do rozumienia etyczno-społecznych aspektów działalności inżynierskiej.	P6U_W, P6S_WG
K1CB_W06	Zna i rozumie podstawowe pojęcia i zasady z zakresu ochrony własności przemysłowej i prawa autorskiego - umie korzystać z zasobów informacji patentowej.	P6S_WK
K1CB_W07	Ma podstawową wiedzę w zakresie własności funkcji (trygonometrycznych, potęgowych, wykładniczych, logarytmicznych, cyklometrycznych i do nich odwrotnych), rachunku różniczkowego i całkowego funkcji jednej oraz wielu zmiennych. Ma podstawową wiedzę z zakresu grup, pierścieni, ciał i operacji na zbiorach skończonych, przestrzeni liniowych i afinicznych.	P6U_W, P6S_WG
K1CB_W08	Ma podstawową wiedzę w zakresie liczb zespolonych, wielomianów, rachunku macierzowego z zastosowaniem do rozwiązywania układów równań liniowych, geometrii analitycznej na płaszczyźnie i w przestrzeni.	P6U_W, P6S_WG
K1CB_W09	Zna podstawowe metody wnioskowania (indukcja, dedukcja, abdukcja). Ma podstawową wiedzę w zakresie społecznych i filozoficznych uwarunkowań działalności inżynierskiej	P6S_WK
K1CB_W11	Zna podstawy telekomunikacji i definiuje podstawowe pojęcia z zakresu telekomunikacji.	P6U_W, P6S_WG
K1CB_W12	Zna podstawy teorii systemów, własności	P6U_W,

	podstawowych struktur systemów oraz sposoby rozwiązywania prostych zadań identyfikacji, rozpoznawania i sterowania.	P6S_WG
K1CB_W13	Zna podstawy inżynierii i metodologii programowania obiektowego.	P6U_W, P6S_WG
K1CB_W14	Ma ogólną wiedzę w zakresie fizyki niezbędna do rozumienia zjawisk fizycznych wykorzystywanych w studiowanej dyscyplinie	P6U_W, P6S_WG
K1CB_W15	Ma podstawową wiedzę w zakresie matematycznych modeli probabilistycznych.	P6U_W, P6S_WG
K1CB_W16	Ma podstawową wiedzę z zakresu kombinatoryki oraz matematyki dyskretnej. Potrafi modelować i rozwiązywać praktyczne problemy dotyczące struktur definiowanych na zbiorach skończonych.	P6U_W, P6S_WG
K1CB_W17	Ma podstawową wiedzę w zakresie funkcji zmiennej zespolonej oraz równań różniczkowych zwyczajnych oraz szeregów potęgowych, szeregu Fouriera, transformat Fouriera i Laplace'a.	P6U_W, P6S_WG
K1CB_W18	Posiada wiedzę na temat cyfrowego kanału telekomunikacyjnego, jego poszczególnych elementów i związanych z nim funkcji i stosowanych kodów liniowych.	P6U_W, P6S_WG
K1CB_W19	Posiada wiedzę na temat testów i metod testowania hipotez statystycznych, wymagań nakładanych na estymatory parametrów rozkładów i metod ich konstruowania na potrzeby systemów przetwarzania i przesyłania informacji.	P6U_W, P6S_WG
K1CB_W20	Zna strukturę wewnętrzną i metody programowania mikroprocesorów i mikrokontrolerów.	P6U_W, P6S_WG, P6S_WG_NT, P6S_WG_INŻ
K1CB_W21	Ma ogólną wiedzę dotyczącą systemów zarządzania bezpieczeństwem informacji zgodnych z odpowiednimi normami, 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.	P6U_W, P6S_WG
K1CB_W22	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_NT, P6S_WG_INŻ
K1CB_W23	Zna podstawowe zagadnienia z zakresu teorii cyfrowego przetwarzania sygnałów deterministycznych i losowych będących nośnikiem informacji, w szczególności zagadnienia: próbkowania, kwantyzacji, detekcji i filtracji.	P6U_W, P6S_WG
K1CB_W24	Posiada wiedzę na temat systemów kryptograficznych	P6U_W,

	w telekomunikacji oraz wiedzę umożliwiającą rozróżnianie metod szyfrowania informacji.	P6S_WG
K1CB_W25	Zna podstawowe pojęcia i twierdzenia z teorii pola elektromagnetycznego.	P6U_W, P6S_WG
K1CB_W26	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_NT, P6S_WG_INŻ
K1CB_W27	Zna podstawowe pojęcia związane z bezpieczeństwem i metodami jego zwiększania w systemach operacyjnych, zna zastosowanie narzędzi: monitorowania bezpieczeństwa systemów, audytu technicznego i testów penetracyjnych.	P6U_W, P6S_WG, P6S_WG_NT, P6S_WG_INŻ
K1CB_W28	Ma ogólną wiedzę z zakresu kompatybilności elektromagnetycznej i elektromagnetycznego bezpieczeństwa systemów i sieci. Potrafi scharakteryzować źródła zaburzeń elektromagnetycznych, wskazać mechanizmy i drogi rozchodzenia się zaburzeń elektromagnetycznych oraz wskazać zagrożenia wynikające z elektromagnetycznego ulotu informacji jak i oddziaływania zaburzeń elektromagnetycznych na urządzenia, systemy i sieci. Potrafi wskazać testy i pomiary niezbędne do oceny bezpieczeństwa elektromagnetycznego oraz wskazać metody ochrony urządzeń, systemów i sieci zwiększające ich bezpieczeństwo elektromagnetyczne i niezawodność działania.	P6U_W, P6S_WG, P6S_WG_NT, P6S_WG_INŻ
K1CB_W29	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_NT, P6S_WG_INŻ
K1CB_W30	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.	P6U_W, P6S_WG, P6S_WG_NT, P6S_WG_INŻ
K1CB_W31	Ma ogólną wiedzę na temat sposobów monitorowania oraz detekcji zagrożeń w systemach informatycznych. Zna systemy wykrywające zagrożenia oraz systemy prewencyjne, rozumie analizę korelacji zdarzeń w	P6U_W, P6S_WG, P6S_WG_NT, P6S_WG_INŻ

	systemach komputerowych, wie jak dobrać oraz skonfigurować narzędzia monitorujące zagrożenia, w szczególności jak przygotować sondy monitorujące.	
K1CB_W32	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_NT, P6S_WG_INŻ
K1CB_W33	Ma wiedzę na temat stosowanych metod audytu formalnego oraz technicznego oraz podstawowe założenia norm ISO rodziny 27000. Zna wybrane metody audytu technicznego oraz zastosowanie wybranych narzędzi do audytu technicznego i testów penetracyjnych.	P6U_W, P6S_WG, P6S_WG_NT, P6S_WG_INŻ
K1CB_W34	Posiada podstawową wiedzę o procesach zarządzania. Zna funkcje, zasady i instrumenty zarządzania oraz identyfikuje podstawowe problemy zarządzania. Zna podstawowe pojęcia z zakresu zarządzania jakością, rozumie istotę, cele i uwarunkowania procesu doskonalenia jakości. Rozpoznaje i objaśnia podstawowe metody i narzędzia doskonalenia jakości. Zna podstawowe zagadnienia związane z przedsiębiorczością.	P6S_WK, P6S_WK_NT, P6S_WK_INŻ
	Osiąga efekty kształcenia w kategorii WIEDZA dla jednej z następujących specjalności: - Bezpieczeństwo sieci teleinformatycznych (BST) – załącznik nr 1 - Bezpieczeństwo danych (BD) – załącznik nr 2	
UMIEJĘTNOŚCI		
K1CB_U01	Potrafi rozwiązywać zadania obliczeniowe z użyciem narzędzi komputerowych.	P6S_UW
K1CB_U02	Umie zapisać algorytm w postaci schematu blokowego, podać rozwiązanie prostych zadań w postaci algorytmów oraz podać sposób ich testowania.	P6S_UW
K1CB_U03	Umie korzystać ze środowiska informatycznego oraz programować z użyciem typów prostych, łańcuchów znakowych, pętli, procedur i funkcji.	P6U_U, P6S_UW
K1CB_U04	Umie posługiwać się edytorami tekstów, arkuszami kalkulacyjnymi, wykonać prezentację multimedialną, publikować informacje w sieci.	P6S_UW
K1CB_U05	Potrafi poprawnie i efektywnie zastosować wiedzę z algebry liniowej i geometrii analitycznej do jakościowej i ilościowej analizy zagadnień matematycznych w obszarze cyberbezpieczeństwa.	P6S_UW
K1CB_U06	Potrafi poprawnie i efektywnie zastosować wiedzę z rachunku różniczkowego i całkowego funkcji jednej i wielu zmiennych do jakościowej i ilościowej analizy zagadnień matematycznych w obszarze cyberbezpieczeństwa.	P6S_UW

K1CB_U07	Posiada umiejętność reprezentacji wiedzy eksperckiej i eksperymentalnej w formie schematów blokowych, grafów, zestawów wyrażeń logicznych, w szczególności kreowania systemów wejściowo-wyjściowych i tworzenie ich modeli matematycznych.	P6U_U, P6S_UW
K1CB_U08	Umie samodzielnie tworzyć programy zorientowane obiektowo.	P6U_U, P6S_UW
K1CB_U09	Potrafi poprawnie i efektywnie zastosować poznane zasady i prawa fizyki do jakościowej i ilościowej analizy zagadnień fizycznych o charakterze inżynierskim.	P6S_UW
K1CB_U10	Ma podstawową wiedzę z zakresu kombinatoryki oraz matematyki dyskretnej. Potrafi modelować i rozwiązywać praktyczne problemy dotyczące struktur definiowanych na zbiorach skończonych	P6U_U, P6S_UW
K1CB_U11	Potrafi poprawnie i efektywnie zastosować wiedzę z równań różniczkowych zwyczajnych oraz transformat Fouriera i Laplace'a do jakościowej i ilościowej analizy zagadnień matematycznych w obszarze cyberbezpieczeństwa.	P6S_UW
K1CB_U12	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_UW04_NT, P6S_UW04_INŻ
K1CB_U13	Potrafi analizować właściwości kodu oraz ma umiejętność jego zaprojektowania.	P6U_U, P6S_UW, P6S_UW04_NT, P6S_UW04_INŻ
K1CB_U14	Potrafi dobrać i zastosować podstawowe testy statystyczne oraz stosować i dobrać metody estymacji dla prostych modeli statystycznych.	P6S_UW
K1CB_U15	Potrafi przygotować i uruchomić oprogramowanie wykorzystujące strukturę wewnętrzną mikrokontrolerów.	P6U_U, P6S_UW, P6S_UW01_NT, P6S_UW01_INŻ
K1CB_U16	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.	P6U_U, P6S_UW
K1CB_U17	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
K1CB_U18	Umie dokonać analizy własności sygnałów w dziedzinie czasowej i częstotliwościowej i syntezy	P6U_U, P6S_UW,

	filtrów cyfrowych z użyciem dedykowanego oprogramowania.	P6S_UW01_NT, P6S_UW01_INŻ
K1CB_U19	Potrafi rozwiązywać podstawowe zagadnienia teorii pola elektromagnetycznego	P6S_UW
K1CB_U20	Potrafi konfigurować hosty i routery do pracy w sieci lokalnej, stosować narzędzia diagnostyczne, obserwować i analizować zdarzenia sieciowe. Potrafi zaplanować adresację IP, podłączyć i skonfigurować routery i przełączniki, użyć protokoły dynamicznego rutowania.	P6U_U, P6S_UW, P6S_UW01_NT, P6S_UW01_INŻ
K1CB_U21	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_UW01_NT, P6S_UW01_INŻ
K1CB_U22	Potrafi samodzielnie korzystać z różnorodnych obcojęzycznych źródeł informacji, w szczególności literatury fachowej, integrować uzyskane informacje i stosować w celu pogłębienia wiedzy specjalistycznej i poszerzania własnych kompetencji językowych.	P6S_UK
K1CB_U23	Rozumie obcojęzyczne teksty słuchane i czytane o tematyce ogólnej i naukowo-technicznej związanej z dziedziną nauki i dyscyplinami naukowymi właściwymi dla studiowanego kierunku studiów.	P6S_UK
K1CB_U24	Dysponuje wystarczającym zakresem środków językowych, aby stosunkowo bezbłędnie wypowiadać się (ustnie i pisemnie), formułować i uzasadniać opinie, wyjaśniać swoje stanowisko, przedstawiać wady i zalety różnych rozwiązań, uczestniczyć w dyskusji i prezentować tematykę ogólną i naukowo-techniczną.	P6S_UK
K1CB_U25	Umiejętnie posługuje się językiem obcym w międzynarodowym środowisku zawodowym z uwzględnieniem wiedzy inter-kulturowej oraz formalnego i nieformalnego rejestru wypowiedzi, zgodnie z wymaganiami określonymi dla poziomu B2.	P6S_UK
K1CB_U26	Potrafi konfigurować stanowiska i urządzenia do badań EMC, wyznaczać parametry techniczne stosowanych zabezpieczeń i dokonywać ich klasyfikacji. Potrafi wykonywać podstawowe badania emisyjności i podatności urządzeń, systemów i sieci na zaburzenia elektromagnetyczne oraz opracowywać i interpretować otrzymane wyniki badań.	P6U_U, P6S_UW, P6S_UW01_NT, P6S_UW01_INŻ
K1CB_U27	Umie selektywnie poszukiwać wiedzę w zadanej tematyce oraz komunikatywnie ją prezentować z merytoryczną argumentacją rozwiązań technicznych oraz własnego stanowiska i poglądu.	P6S_UK, P6S_UW03_NT, P6S_UW03_INŻ
K1CB_U28	Potrafi konfigurować i diagnozować sieci w topologii	P6U_U,

	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.	P6S_UW, P6S_UW01_NT, P6S_UW01_INŻ
K1CB_U29	Potrafi sformułować i zaprezentować główne cele oraz zadania zarządzania i utrzymania infrastruktury teleinformatycznej. Potrafi zinterpretować podstawowe elementy modelu zarządzania. Potrafi definiować parametry niezawodnościowych modeli sieci teleinformatycznej oraz określać wymagania związane z eksploatacją urządzeń i systemów.	P6U_U, P6S_UW
K1CB_U30	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_UW01_NT, P6S_UW01_INŻ
K1CB_U31	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.	P6U_U, P6S_UW, P6S_UW04_NT, P6S_UW04_INŻ
K1CB_U32	Potrafi skonfigurować i uruchomić mechanizmy bezpieczeństwa na ruterach i urządzeniach firewall, tunele szyfrowane i mechanizmy IDS.	P6U_U, P6S_UW, P6S_UW01_NT, P6S_UW01_INŻ
K1CB_U33	Potrafi używać narzędzi audytu technicznego do przetestowania bezpieczeństwa aplikacji sieciowej. Potrafi wykonać poszczególne etapy testu penetracyjnego i przygotować raport.	P6S_UW, P6S_UW01_NT, P6S_UW01_INŻ
K1CB_U34	Ma przygotowanie niezbędne do pracy w środowisku przemysłowym oraz znajomość zasad bezpieczeństwa związanych ze stanowiskiem pracy.	P6S_UO, P6S_UU, P6S_UW06_NT
K1CB_U35	Umie skonstruować układ pomiarowy oraz wykonać pomiary przyrządami analogowymi i cyfrowymi wielkości elektrycznych.	P6U_U P6S_UW, P6S_UW01_NT P6S_UW01_INŻ
	Osiąga efekty kształcenia w kategorii UMIEJĘTNOŚCI dla jednej z następujących specjalności: - Bezpieczeństwo sieci teleinformatycznych (BST) – załącznik nr 1 - Bezpieczeństwo danych (BD) – załącznik nr 2	
KOMPETENCJE SPOŁECZNE		

K1CB_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 przekazać taką informację i opinie w sposób zrozumiały, z uzasadnieniem różnych punktów widzenia.	P6U_K, P6S_KR
K1CB_K02	Rozumie prawne aspekty i skutki działalności inżynierskiej.	P6U_K, P6S_KR
K1CB_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
K1CB_K04	Ma świadomość niezbędności aktywności indywidualnych i zespołowych wykraczających poza działalność inżynierską.	P6U_K
K1CB_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
K1CB_K06	Potrafi współpracować z zespołem przy realizacji złożonego zadania inżynierskiego.	P6U_K
K1CB_K07	Rozumie konieczność samokształcenia oraz rozwijania zdolności do samodzielnego stosowania posiadanej wiedzy i umiejętności.	P6U_K
K1CB_K08	Potrafi przedstawić efekty swojej pracy w zrozumiałej formie.	P6U_K
K1CB_K09	Ma świadomość znaczenia umiejętności wyszukiwania informacji oraz jej krytycznej analizy.	P6U_K
K1CB_K10	Ma świadomość znaczenia ochrony informacji, ochrony dostępu do informacji oraz konstrukcji systemów ochrony informacji niejawnych, danych osobowych i informacji objętych tajemnicą zawodową.	P6U_K

ZAŁĄCZNIK NR 1

Efekty kształcenia na I stopniu studiów dla specjalności CBS	OPIS KIERUNKOWYCH EFEKTÓW KSZTAŁCENIA Po zakończeniu studiów I stopnia na kierunku CYBERBEZPIECZEŃSTWO w ramach specjalności Bezpieczeństwo sieci teleinformatycznych absolwent:	Odniesienie efektów kształcenia dla obszaru nauk technicznych (T)
WIEDZA		
K1CB_W01_BST	Zna zjawiska fizyczne związane z transmisją sygnałów przez kable miedziane, światłowody i drogą radiową. Wie, jak opisać różne modele medium transmisyjnego oraz jak wybrać i wytłumaczyć zastosowanie odpowiednich mediów transmisyjnych dla różnych systemów teleinformatycznych.	P6U_W, P6S_WG
K1CB_W02_BST	Ma ogólną wiedzę na temat systematyki sieci bezprzewodowych oraz technik transmisyjnych (MAC, SS, OFDM, MIMO). Potrafi dobrać odpowiednią technikę bezprzewodowej sieci dostępowej do wymogów funkcjonalnych i prawnych oraz obliczyć jej wydajność z uwzględnieniem aspektów propagacyjnych, obciążeniowych oraz związanych z kompatybilnością elektromagnetyczną, obecnych w segmencie dostępowym.	P6U_W, P6S_WG, P6S_WG_NT, P6S_WG_INŻ
K1CB_W03_BST	Ma wiedzę z zakresu metod kompresji danych stosowanych w systemach multimedialnych oraz łączności bezprzewodowej.	P6U_W, P6S_WG
K1CB_W04_BST	Ma wiedzę dotyczącą transmisji danych we współczesnych sieciach telekomunikacyjnych, związaną z ograniczeniami fizycznymi transmisji, modelem funkcjonalnym sieci, mediami transmisyjnymi i technikami transmisyjnymi. Posiada wiedzę o rozwoju technik transmisyjnych, sieciach pakietowych oraz sposobach zapewniania jakości transmisji danych we współczesnych sieciach telekomunikacyjnych.	P6U_W, P6S_WG
K1CB_W05_BST	Ma wiedzę dotyczącą systemów i sieci komórkowych. Potrafi wymienić, scharakteryzować i porównać systemy komórkowe i bezprzewodowe różnych generacji, w tym ich obszary zastosowań, architektury i funkcje jego podstawowych elementów oraz techniki zastosowane w interfejsie radiowym. Potrafi określić zagrożenia bezpieczeństwa systemów komórkowych i wskazać zabezpieczenia stosowane do zapewnienia bezpieczeństwa funkcjonowania sieci komórkowych i realizacji usług.	P6U_W, P6S_WG, P6S_WG_NT, P6S_WG_INŻ
K1CB_W06_BST	Ma wiedzę na temat infrastruktury chmur	P6U_W,

	obliczeniowych oraz aplikacji i usług w chmurach.	P6S_WG, P6S_WG_NT, P6S_WG_INŻ
K1CB_W07_BST	Ma wiedzę ogólną dotyczącą projektowania systemów biometrycznych i zasad modelowania jego elementów. Zna podstawowe parametry charakteryzujące systemy biometryczne.	P6S_WG
K1CB_W08_BST	Ma ogólną wiedzę na temat istoty Internetu Rzeczy, telemetrii i sieci sensorowych. Zna systematykę, kierunki rozwoju oraz działanie istniejących technologii Internetu Rzeczy (IoT). Potrafi dobrać optymalny standard transmisji IoT, spełniający założone uwarunkowania funkcjonalne, zasięgowe i energetyczne.	P6U_W, P6S_WG, P6S_WG_NT, P6S_WG_INŻ
K1CB_W09_BST	Zna podstawowe zagadnienia związane z aspektami prawnymi i etycznymi w obszarze bezpieczeństwa zasobów sieci teleinformatycznych.	P6U_W, P6S_WG
K1CB_W10_BST	Zna zagadnienia realizacji bezpiecznego dostępu do usług w internecie, monitorowania go oraz polityk bezpieczeństwa w tym zakresie. Zna koncepcję tuneli szyfrowanych VPN w relacji client –to – site i site – to – site. Posiada wiedzę o rodzajach ataków i podatności na ataki stosowanych metod zabezpieczeń.	P6U_W, P6S_WG
UMIEJĘTNOŚCI		
K1CB_U01_BST	Potrafi zestawić sieć bezprzewodową na potrzeby realizacji dostępu radiowego w trybie punkt-wielopunkt z uwzględnieniem zagadnień kompatybilnościowych. Potrafi dobrać parametry transmisyjne poszczególnych stacji bazowych sieci dostępowej, aby spełnić wymagania jakościowe odbioru na obszarze pokrycia.	P6U_U, P6S_UW, P6S_UW01_NT, P6S_UW01_INŻ
K1CB_U02_BST	Umie prowadzić eksperymenty off-line na sygnałach mowy, dźwięku oraz obrazach statycznych i dynamicznych. Potrafi dobierać właściwe rozwiązania dla zadania kompresji danych przy ustalonych parametrach transmisji w kanale telekomunikacyjnym.	P6U_U, P6S_UW, P6S_UW01_NT, P6S_UW01_INŻ
K1CB_U03_BST	Potrafi konfigurować urządzenia i usługi dla wybranych technik transmisji danych, stosować narzędzia diagnostyczne, rejestrować i analizować parametry badanych łączy.	P6S_UW, P6S_UW01_NT, P6S_UW01_INŻ
K1CB_U04_BST	Potrafi stworzyć usługi chmury i dobierać modele dostarczania tej usługi z chmury a także dobrać odpowiednie technologie w chmurze i analizować czynniki wpływające na wydajność realizacji usług oraz oszacować ilość pracy do wykonania w chmurze obliczeniowej.	P6S_UW, P6S_UW01_NT, P6S_UW01_INŻ
K1CB_U05_BST	Umie wybrać i odpowiednio skonfigurować rozmaite czujniki analogowe i cyfrowe, dobrać do nich	P6U_U, P6S_UW,

	odpowiednią platformę mikroprocesorową, napisać proste oprogramowanie zarządzające pomiarami i transmisją oraz zestawić połączenie z wykorzystaniem optymalnej technologii IoT.	P6S_UW01_NT, P6S_UW01_INŻ
K1CB_U06_BST	Potrafi tworzyć bezpieczny dostęp do usług teleinformatycznych poprzez sieć z użyciem połączeń VPN. Potrafi dobrać optymalne technologie do przyjętych założeń i analizować ryzyko oraz podatność na ataki przyjętych rozwiązań.	P6U_U, P6S_UW, P6S_UW04_NT, P6S_UW04_INŻ
K1CB_U07_BST	Potrafi wykonać przydzielone zadania inżynierskie w ramach realizacji zespołowego projektu (złożonego zadania inżynierskiego) w obszarze telekomunikacji mobilnej, umie przeprowadzić analizę ekonomiczną przedsięwzięcia, potrafi opracować stosowną dokumentację	P6U_U, P6S_UO, P6S_UU, P6S_UW02_NT, P6S_UW02_INŻ P6S_UW04_NT, P6S_UW04_INŻ
K1CB_U08_BST	Potrafi przygotować prezentację zawierającą wyniki pracy dyplomowej, uzasadnić w dyskusji sposób realizacji i osiągnięte efekty projektu	P6U_U, P6S_UW, P6S_UK
K1CB_U09_BST	Potrafi wykonać pracę dyplomową w postaci projektu inżynierskiego w obszarze cyberbezpieczeństwa i opracować stosowną dokumentację, w tym: <ul style="list-style-type: none"> • potrafi pozyskiwać informacje z literatury, baz danych oraz innych źródeł, • potrafi wykorzystać do formułowania i rozwiązywania zadań metody analityczne, symulacyjne i eksperymentalne, • potrafi ocenić przydatność i możliwość wykorzystania nowych technik i technologii, • potrafi dokonać identyfikacji i sformułować specyfikację zadań, w tym zadań nietypowych, potrafi zgodnie z zadaną specyfikacją zaprojektować oraz zrealizować urządzenie, obiekt, system lub proces.	P6U_U, P6S_UW, P6S_UW02_NT, P6S_UW02_INŻ, P6S_UW04_NT, P6S_UW04_INŻ,

ZAŁĄCZNIK NR 2

Efekty kształcenia na I stopniu studiów dla specjalności CBD	OPIS KIERUNKOWYCH EFEKTÓW KSZTAŁCENIA Po zakończeniu studiów I stopnia na kierunku CYBERBEZPIECZEŃSTWO w ramach specjalności Bezpieczeństwo danych absolwent:	Odniesienie efektów kształcenia dla obszaru nauk technicznych (T)
WIEDZA		
K1CB_W01_BD	Ma wiedzę w zakresie opisu i analizy algorytmów przetwarzania sygnałów, w tym sygnałów dźwięku i obrazu oraz zabezpieczeń treści w aplikacjach multimedialnych	P6U_W, P6S_WG
K1CB_W02_BD	Ma podstawową wiedzę z zakresu transmisji danych oraz mediów używanych do transmisji, ich budowy, zjawisk wpływających na transmisję.	P6U_W, P6S_WG
K1CB_W03_BD	Ma ogólną wiedzę na temat systematyki i działania urządzeń sieci bezprzewodowych oraz technik transmisyjnych (np. SS, OFDM, MIMO). Potrafi modelować parametry wydajnościowe na podstawie znajomości ch-ki systemu, zapotrzebowania użytkowników segmentu dostępowego oraz planować w oparciu o nie sieć dostępową na zadanym obszarze.	P6U_W, P6S_WG, P6S_WG_NT, P6S_WG_INŻ
K1CB_W04_BD	Ma ogólną wiedzę dotyczącą usług multimedialnych oraz potrafi wskazać podstawowe czynniki wpływające na jakość usług w sieci, a także podstawowe zagrożenia bezpieczeństwa usług multimedialnych i sposoby przeciwdziałania tym zagrożeniom.	P6U_W, P6S_WG
K1CB_W05_BD	Zna fizyczne i logiczne składowe infrastruktury pamięci masowych oraz modele logiczne danych i algorytmy stosowane w przetwarzaniu dużych zbiorów danych.	P6U_W, P6S_WG
K1CB_W06_BD	Ma wiedzę o architekturze i zasadzie działania podstawowych komponentów SZBD. Potrafi omówić i porównać podstawowe metody organizacji danych, indeksowania danych oraz przetwarzania i optymalizacji transakcji i zapytań w SZBD. Zna kryptograficzne metody stosowane w ochronie SZBD oraz techniki projektowania bezpiecznych baz danych.	P6U_W, P6S_WG
K1CB_W08_BD	Ma podstawową wiedzę dotyczącą centrów przetwarzania danych, infrastruktury i usług.	P6U_W, P6S_WG, P6S_WG_NT, P6S_WG_INŻ
K1CB_W09_BD	Zna podstawowe pojęcia oraz elementy z zakresu Biometrii.	P6U_W, P6S_WG

K1CB_W10_BD	Ma wiedzę na temat organizacji systemów rozproszonych oraz mechanizmów łączenia użytkowników i zasobów. Zna wymagania związane zapewnieniem ciągłości i niezawodności systemów rozproszonych. Zna zagadnienia bezpieczeństwa danych w systemach rozproszonych dotyczące poufności, integralności i dostępności. Rozumie mechanizmy i sposoby realizacji ataków na systemy rozproszone oraz potrafi wskazać działania związane z zapewnieniem odpowiedniego poziomu bezpieczeństwa.	P6U_W, P6S_WG
K1CB_W11_BD	Zna zagadnienia i metody przetwarzania dowodów cyfrowych: rodzaje źródeł, sposoby pozyskiwania, rzetelność i zabezpieczanie dowodów. Rozumie opisy dowodów w informatyce śledczej. Zna metody zapewniania rzetelności i niezaprzeczalności dowodów cyfrowych.	P6U_W, P6S_WG
K1CB_W12_BD	Ma wiedzę dotyczącą: metod i technik zabezpieczania usług teleinformatycznych, rodzajów ataków i podatności na ataki stosowanych metod zabezpieczeń. Zna zagadnienia bezpiecznej realizacji usług teleinformatycznych, monitorowania ich oraz polityk bezpieczeństwa w tym zakresie.	P6U_W, P6S_WG
UMIEJĘTNOŚCI		
K1CB_U01_BD	Umie scharakteryzować sposoby przetwarzania i zabezpieczania treści multimedialnych.	P6S_UW
K1CB_U02_BD	Potrafi posługiwać się narzędziami diagnostycznymi i urządzeniami do testowania i analizy oraz skonfigurować urządzenia i usługi dla wybranych technik transmisji danych.	P6S_UW, P6S_UW01_NT, P6S_UW01_INŻ
K1CB_U03_BD	Potrafi zestawić sieć bezprzewodową na potrzeby transmisji danych różnego typu z uwzględnieniem zagadnień kompatybilnościowych. Potrafi dobrać parametry transmisyjne określonej sieci bezprzewodowej, celem spełnienia wymagań jakościowych, zestawić stanowisko pomiarowe wraz z procedurami testowymi oraz przeprowadzić testy weryfikacyjne.	P6U_U, P6S_UW, P6S_UW01_NT, P6S_UW01_INŻ
K1CB_U04_BD	Potrafi konfigurować wybrane usługi multimedialne w środowisku sieciowym oraz korzystać z dostępnych narzędzi do monitorowania zdarzeń ruchowych w sieci i analizować proces realizacji wybranych usług.	P6S_UW, P6S_UW01_NT, P6S_UW01_INŻ
K1CB_U05_BD	Potrafi zaprojektować, skonfigurować i zarządzać wybranymi rozwiązaniami sieciowych pamięci masowych oraz zaprojektować strukturę logiczną danych i przeprowadzić proces odkrywania wiedzy w dużych zbiorach danych.	P6U_U, P6S_UW, P6S_UW04_NT, P6S_UW04_INŻ
K1CB_U06_BD	Potrafi wybrać i dostosować odpowiednie do wymagań narzędzia tworzenia aplikacji baz danych	P6U_U, P6S_UW,

	oraz samodzielnie zaprojektować i zaimplementować bazę danych. Potrafi ocenić rozmiary i prawidłowo stosować systemy składowania i odzyskiwania danych. Umie wykonać analizy oraz projektować i implementować mechanizmy bezpieczeństwa w bazach danych	P6S_UW04_NT, P6S_UW04_INŻ
K1CB_U07_BD	Potrafi konfigurować i uruchamiać usługi teleinformatyczne w centrach przetwarzania danych.	P6S_UW, P6S_UW01_NT, P6S_UW01_INŻ
K1CB_U08_BD	Potrafi przeanalizować strukturę i mechanizmy działania systemu oraz sieci rozproszonej i wskazać potencjalne zagrożenia dla poufności, integralności i dostępności danych. Potrafi dobrać odpowiednie mechanizmy i narzędzia oraz określić wymagania dotyczące zabezpieczeń.	P6S_UW
K1CB_U09_BD	Potrafi stosować techniki pozyskiwania dowodów cyfrowych z różnych źródeł: obrazy dysków, logi, zrzuty, dane strumieniowe. Potrafi rozróżnić różne typy zapisu i formatów źródeł dowodów cyfrowych. Potrafi stosować zabezpieczenia dowodów cyfrowych (podpisy, skróty, kopie). Potrafi przeprowadzić i udokumentować analizę powłamanową incydentu teleinformatycznego.	P6S_UW
K1CB_U10_BD	Potrafi tworzyć i weryfikować bezpieczne usługi teleinformatyczne, dobrać optymalne technologie do przyjętych założeń i analizować ryzyko oraz podatność na ataki przyjętych rozwiązań.	P6U_U, P6S_UW, P6S_UW04_NT, P6S_UW04_INŻ
K1CB_U11_BD	Potrafi wykonać przydzielone zadania inżynierskie w ramach realizacji zespołowego projektu (złożonego zadania inżynierskiego) w obszarze cyberbezpieczeństwa, umie przeprowadzić analizę ekonomiczną przedsięwzięcia, potrafi opracować stosowną dokumentację.	P6U_U, P6S_UO, P6S_UU, P6S_UW02_NT, P6S_UW02_INŻ P6S_UW04_NT, P6S_UW04_INŻ
K1CB_U12_BD	Potrafi przygotować prezentację zawierającą wyniki pracy dyplomowej, uzasadnić w dyskusji sposób realizacji i osiągnięte efekty projektu.	P6U_U, P6S_UW, P6S_UK
K1CB_U13_BD	Potrafi wykonać pracę dyplomową w postaci projektu inżynierskiego w obszarze cyberbezpieczeństwa i opracować stosowną dokumentację, w tym: <ul style="list-style-type: none"> • potrafi pozyskiwać informacje z literatury, baz danych oraz innych źródeł, • potrafi wykorzystać do formułowania i rozwiązywania zadań metody analityczne, symulacyjne i eksperymentalne, • potrafi ocenić przydatność i możliwość wykorzystania nowych technik i technologii, • potrafi dokonać identyfikacji i sformułować specyfikację zadań, w tym zadań 	P6U_U, P6S_UW, P6S_UW02_NT, P6S_UW02_INŻ, P6S_UW04_NT, P6S_UW04_INŻ,

	nietypowych, potrafi zgodnie z zadaną specyfikacją zaprojektować oraz zrealizować urządzenie, obiekt, system lub proces.	
--	---	--