

PROGRAM STUDIÓW

WYDZIAŁ: **INFORMATYKI I TELEKOMUNIKACJI**

KIERUNEK STUDIÓW: **CYBERBEZPIECZEŃSTWO**

Przyporządkowany do dyscypliny: **D1 informatyka techniczna i telekomunikacja (dyscyplina wiodąca)**

D2*

D3*

D4*

POZIOM KSZTAŁCENIA: **studia pierwszego stopnia (licencjackie / inżynierskie) / ~~drugiego stopnia / jednolite~~ magisterskie***

FORMA STUDIÓW: **stacjonarna / niestacjonarna***

PROFIL: **ogólnoakademicki / praktyczny***

JĘZYK PROWADZENIA STUDIÓW: **polski**

OBOWIAZUJE OD CYKLU KSZTAŁCENIA: **2023/2024**

Zawartość:

1. Zakładane efekty uczenia się – zał. nr 1 do programu studiów
2. Opis programu studiów – zał. nr 2 do programu studiów
3. Plan studiów – zał. nr 3 do programu studiów

*niepotrzebne skreślić

ZAKŁADANE EFEKTY UCZENIA SIĘ

Wydział: Informatyki i Telekomunikacji

Kierunek studiów: Cyberbezpieczeństwo

Poziom studiów: studia pierwszego stopnia

Profil: ogólnoakademicki

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

P6S – charakterystyki drugiego stopnia odpowiadające kształceniu na studiach pierwszego stopnia studiów - 6 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”

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

Kierunkowe efekty uczenia się

Symbol kierunkowych efektów uczenia się	Opis efektów uczenia się dla kierunku studiów Cyberbezpieczeństwo 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 PRK	Charakterystyki dla kwalifikacji na poziomach 6 i 7 PRK, umożliwiającymi 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_INŻ
K1CBE_W02	Ma wiedzę z zakresu programowania w środowisku UNIX, komunikacji między procesami i programowania współbieżnego	P6U_W	P6S_WG	P6S_WG_INŻ
K1CBE_W03	Zna podstawy technik informatycznych, usług sieciowych oraz technologii zapewnienia bezpieczeństwa związanych z pozyskiwaniem, przetwarzaniem i prezentowaniem informacji.	P6U_W	P6S_WG	P6S_WG_INŻ
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 P6S_WK	
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	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	P6S_WG_INŻ

K1CBE_W07	Ma podstawową wiedzę o konstrukcji oraz funkcjonowaniu chmur obliczeniowych. Zna cechy charakterystyczne oraz modele dostarczania usług w chmurze obliczeniowej.	P6U_W	P6S_WG	P6S_WG_INŻ
K1CBE_W08	Ma wiedzę z zakresu metod zarządzania ryzykiem oraz sposobu ich wyznaczania a także polityki bezpieczeństwa w różnych instytucjach.	P6U_W	P6S_WG	P6S_WG_INŻ
K1CBE_W09	Zna zagadnienia i metody analizy i przetwarzania dowodów cyfrowych: rodzaje źródeł, sposoby pozyskiwania, rzetelność i zabezpieczanie dowodów, zna metody analizy artefaktów aktywności. Rozumie opisy dowodów w informatyce śledczej. Zna metody zapewniania rzetelności i niezaprzeczalności dowodów cyfrowych.	P6U_W	P6S_WG	P6S_WG_INŻ
K1CBE_W10	Ma wiedzę na temat różnych metodyk zarządzania projektami. Zna procesy związane z zarządzaniem projektami.	P6U_W	P6S_WG	
K1CBE_W11	Ma podstawową wiedzę oraz zna narzędzia i techniki z zakresu wykonywania testów penetracyjnych w celu znalezienia i wyeliminowania słabych punktów - elementów podatnych na ataki, zarówno w obszarze infrastruktury teleinformatycznej jak i na poziomie aplikacji internetowych.	P6U_W	P6S_WG	P6S_WG_INŻ
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_INŻ
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_INŻ
K1CBE_W14	Zna metody sztucznej inteligencji (AI) i metody uczenia maszynowego (ML) wykorzystywane w modelowaniu i wykrywaniu zagrożeń / ataków na systemy komputerowe a także metody wykrywania anomalii / nietypowych profili w oparciu o dane z monitoringu ruchu sieciowego, monitoringu zdarzeń i obciążenia urządzeń i z innych źródeł.	P6U_W	P6S_WG	P6S_WG_INŻ
K1CBE_W15	Posiada wiedzę na temat systemów kryptograficznych w telekomunikacji oraz wiedzę umożliwiającą rozróżnianie metod szyfrowania informacji.	P6U_W	P6S_WG	P6S_WG_INŻ

K1CBE_W16	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_INŻ
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_INŻ
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_INŻ
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_INŻ
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_INŻ
K1CBE_W21	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_INŻ

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.	P6U_W	P6S_WG	P6S_WG_INŻ
UMIEJĘTNOŚCI (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	P6S_UW_INŻ
K1CBE_U05	Potrafi posługiwać się metodami matematyki i fizyki do rozwiązywania szczegółowych problemów w obszarze cyberbezpieczeństwa	P6U_U	P6S_UW	
K1CBE_U06	Potrafi wybrać i dostosować odpowiednie do wymagań narzędzia tworzenia aplikacji baz danych oraz samodzielnie zaprojektować i zaimplementować bazę danych. Umie wykonać analizy oraz projektować i implementować mechanizmy bezpieczeństwa w bazach danych	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U07	Potrafi uruchamiać i konfigurować usługi serwerowe oraz komunikacyjne w środowisku wirtualnym oraz dobierać odpowiednie technologie dla usług świadczonych przez chmury obliczeniowe.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U08	Potrafi stosować mechanizmy synchronizacji procesów oraz programować komunikację sieciową w trybach klient-serwer i peer-to-peer	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U09	Potrafi stosować techniki pozyskiwania dowodów cyfrowych z różnych źródeł: obrazy dysków, logi, zrzuty, dane strumieniowe. Potrafi stosować zabezpieczenia dowodów cyfrowych (podpisy, skróty, kopie) oraz artefaktów aktywności. Potrafi przeprowadzić i udokumentować analizę powłamaniamiw incydentu teleinformatycznego.	P6U_U	P6S_UW	P6S_UW_INŻ

K1CBE_U10	Potrafi wybrać i zastosować odpowiednią metodykę zarządzania projektami dla konkretnego zadania. Potrafi zdefiniować projekt i nim zarządzać.	P6U_U	P6S_UW, P6S_UO	
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	Potrafi zaplanować oraz przeprowadzić test penetracyjny.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U14	Potrafi dobrać i zastosować właściwe metod analizy danych w zadaniu analizy zagrożeń / wykrywania anomalii w zależności od specyfiki analizowanych danych.	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 zdarzenia sieciowe. Potrafi zaplanować adresację IP, podłączyć i skonfigurować routery i przełączniki, użyć protokoły dynamicznego routowania.	P6U_U	P6S_UW	P6S_UW_INŻ
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 odpowiedniego poziomu języka obcego; 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	P6U_U	P6S_UW	P6S_UW_INŻ

	rozwiązywania podstawowych problemów związanych z KEM i bezpieczeństwem elektromagnetycznym, wyznaczać ich parametry techniczne stosowanych zabezpieczeń, dokonywać ich klasyfikacji oraz ocenić skuteczność zastosowania.			
K1CBE_U19	Potrafi opracować wybraną analizę ryzyka oraz politykę bezpieczeństwa różnych instytucji	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	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_U22	Potrafi skonfigurować i uruchomić mechanizmy bezpieczeństwa na ruterach i urządzeniach firewall, tunele szyfrowane i mechanizmy IDS.	P6U_U	P6S_UW	P6S_UW_INŻ
K1CBE_U23	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_U24	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_U25	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 przekazać taką informację i opinie w sposób zrozumiały, z uzasadnieniem różnych punktów widzenia.	P6U_K	P6S_KR	
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	P6S_KK_INŻ

*niepotrzebne usunąć