Program studiów

Kierunek studiów:	cyberbezpieczeństwo systemów komputerowych
Poziom studiów:	studia drugiego stopnia
Profil studiów:	ogólnoakademicki
Formy studiów:	studia stacjonarne
Liczba semestrów:	3
Liczba punktów ECTS konieczna do ukończenia studiów:	90
Tytuł zawodowy nadawany absolwentom:	magister inżynier
Kierunek studiów jest przyporządkowany do dyscyplin:	informatyka techniczna i telekomunikacja: 100% - dyscyplina wiodąca
Łączna liczba godzin zajęć:	960
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia:	45
Liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć z dziedziny nauk humanistycznych lub nauk społecznych – w przypadku kierunków studiów przyporządkowanych do dyscyplin w ramach dziedzin innych niż odpowiednio nauki humanistyczne lub nauki społeczne:	5
Wymiar oraz liczba punktów ECTS, jaką student musi uzyskać w ramach praktyk zawodowych:	program studiów nie przewiduje praktyk zawodowych
Zasady i forma odbywania praktyk zawodowych:	program studiów nie przewiduje praktyk zawodowych

Efekty uczenia się

Symbol	Zakładane efekty uczenia się	Odniesienie do charakterystyk drugiego stopnia efektów uczenia się Polskiej Ramy Kwalifikacji
Wiedza: zna i rozumie		
K2A_W1	w pogłębionym stopniu zagadnienia z zakresu fizyki, matematyki, statystyki i innych obszarów nauk oraz dyscyplin inżynieryjno-technicznych, przydatne do formułowania i rozwiązywania złożonych zadań inżynierskich z obszaru różnego typu systemów informatycznych	P7S_WG
K2A_W2	podstawowe, podbudowane teoretycznie procesy zachodzące w cyklu życia systemów informatycznych oraz ich komponentów sprzętowo-programowych, a także metody, techniki i narzędzia stosowane przy rozwiązywaniu złożonych zadań inżynierskich związanych z uwzględnianiem zagadnień bezpieczeństwa podczas ich projektowania i implementacji oraz zapewnianiem bezpieczeństwa ich użytkowania i utrzymania	P7S_WG inż.
K2A_W3	podstawowe zasady tworzenia, funkcjonowania i rozwoju różnych form przedsiębiorczości ze świadomością ryzyka występującego w środowiskach cyfrowych	P7S_WK inż.
K2A_W4	społeczne, ekonomiczne, prawne, etyczne i inne, pozatechniczne uwarunkowania działalności inżynierskiej, w tym zasady ochrony własności przemysłowej i prawa autorskiego oraz powiązane z nimi oddziaływania, zasady i standardy funkcjonujące w technicznie zorientowanym społeczeństwie informacyjnym	P7S_WK
K2A_W5	zagadnienia dotyczące wykorzystania odpowiednich form projektowania, implementacji, weryfikacji i utrzymania systemów informatycznych dla zapewnienia bezpieczeństwa zarówno ich wewnętrznej interakcji, jak i interakcji z człowiekiem	P7S_WK
K2A_W6	główne tendencje rozwojowe informatyki technicznej i telekomunikacji, role człowieka i systemów komputerowych w bezpieczeństwie funkcjonowania społeczeństwa	P7S_WG
K2A_W7	podstawowe problemy współczesnej cywilizacji w odniesieniu do osiągnięć nauki i techniki	P7S_WK

Umiejętności: potrafi		
K2A_U1	identyfikować, formułować i rozwiązywać złożone i nietypowe problemy inżynierskie związane ze studiowanym kierunkiem przez zastosowanie zasad inżynieryjno-technicznych oraz nauk matematyczno-fizycznych, a także innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach, przystosowując istniejące lub opracowując nowe metody i narzędzia	P7S_UW
K2A_U2	formułować i testować hipotezy związane z prostymi problemami badawczymi	P7S_UW
K2A_U3	planować i przeprowadzić eksperyment, w tym obserwacje, analizy i symulacje komputerowe, interpretować uzyskane wyniki i wyciągać wnioski, stosować narzędzia i metody zapewniania i zwiększania bezpieczeństwa podczas projektowania rozwiązań oraz analizy i mitygacji zagrożeń podczas ich działania	P7S_UW inż.
K2A_U4	przy identyfikacji i formułowaniu specyfikacji zadań inżynierskich oraz ich rozwiązaniu: – wykorzystywać metody analityczne, symulacyjne i eksperymentalne, – dostrzegać ich aspekty systemowe i pozatechniczne, w tym aspekty etyczne, – dokonywać wstępnej oceny ekonomicznej proponowanych rozwiązań i podejmowanych działań inżynierskich. Potrafi dokonywać krytycznej analizy sposobu funkcjonowania istniejących rozwiązań technicznych i oceniać te rozwiązania	P7S_UW inż.
K2A_U5	zaprojektować zgodnie z zadaną specyfikacją oraz wykonać typowy dla studiowanego kierunku, złożony system lub proces bezpieczeństwa, używając stosownych metod, technik, technologii i narzędzi, przeprowadzić weryfikację funkcjonalną i/lub formalną uzyskanego rozwiązania, projektować i tworzyć oprogramowanie różnego rodzaju ze świadomością konieczności wbudowywania funkcji bezpieczeństwa, wykorzystać techniki bezpieczeństwa w projektowaniu i weryfikacji systemów informatycznych różnego rodzaju	P7S_UW inż.
K2A_U6	pracować indywidualnie i w zespole, przyjmując w nim różne role, w tym rolę wiodącą, kierować pracą zespołu	P7S_UO
K2A_U7	właściwie dobierać źródła i informacje z nich pochodzące, dokonywać oceny, krytycznej analizy, syntezy, twórczej interpretacji i prezentacji tych informacji, komunikować się na tematy specjalistyczne ze zróżnicowanymi kręgami odbiorców, z użyciem specjalistycznej terminologii i nowoczesnych technologii informacyjno-komunikacyjnych, prowadzić debatę	P7S_UK
K2A_U8	dobierać i korzystać z właściwych, zaawansowanych technik, umiejętności i nowoczesnych narzędzi inżynierskich w zakresie projektowania, implementacji i analizy systemów informatycznych i oprogramowania ich komponentów	P7S_UW P7S_UW inż.
K2A_U9	samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkować innych w tym zakresie	P7S_UU
K2A_U10	wybrać i użyć zaawansowanych narzędzi w projektowaniu i weryfikacji systemów cyfrowych, zaadaptować i/lub stworzyć narzędzia inżynierskie wspomagające projektowanie i weryfikację systemów cyfrowych, zaplanować architekturę systemu cyfrowego	P7S_UW
K2A_U11	posługiwać się językiem obcym na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego oraz specjalistyczną terminologią związaną z kierunkiem studiów, a także posługiwać się drugim językiem obcym na poziomie A1 lub wyższym Europejskiego Systemu Opisu Kształcenia Językowego	P7S_UK
Kompetencje społeczne: jest gotów do		
K2A_K1	krytycznej oceny posiadanej wiedzy i odbieranych treści, uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu	P7S_KK
K2A_K2	wypełniania zobowiązań społecznych, inspirowania i organizowania działalności na rzecz środowiska społecznego, inicjowania działań na rzecz interesu publicznego, myślenia i działania w sposób kreatywny i przedsiębiorczy	P7S_KO
K2A_K3	odpowiedzialnego pełnienia ról zawodowych, z uwzględnieniem zmieniających się potrzeb społecznych, rozwijania dorobku zawodu, podtrzymywania etosu zawodu, przestrzegania i rozwijania etyki zawodowej oraz działania na rzecz przestrzegania tych zasad; ma świadomość ważności i zrozumienie pozatechnicznych aspektów i skutków działalności inżynierskiej	P7S_KR

Zajęcia i grupy zajęć

Nazwa zajęć lub grupy zajęć	Liczba punktów ECTS	Efekty uczenia się (symbol) przypisane do zajęć lub grupy zajęć	Treści programowe zapewniające uzyskanie efektów uczenia się
Język obcy	4	K2A_U11	Język, słownictwo, funkcje komunikacyjne i struktury gramatyczne na wybranym poziomie biegłości językowej.
Zajęcia z dziedziny nauk humanistyczno-społecznych (HES)	5	K2A_W3 K2A_W4 K2A_W5 K2A_K2 K2A_K3	Prawo autorskie, prawo patentowe, ochrona własności intelektualnej, elementy prawa pracy i formy prowadzenia działalności gospodarczej, aspekty prawne, certyfikacja; audyty, standaryzacja i narzędzia bezpieczeństwa, certyfikacje Common Criteria i Protection Profiles, socjotechnika, biały wywiad.

			Podstawowe elementy zarządzania projektami, proces zarządzania, proces planowania; proces rozwijania projektów informatycznych, organizacja pracy w grupie; klasyfikacja projektów, fazy projektów, cykl życia projektu, harmonogramowanie projektu, techniki prowadzenia projektów.
Zajęcia podstawowe o charakterze matematyczno-fizycznym	5	K2A_W1 K2A_U1	Zaawansowane systemy kodowania i reprezentacji danych w systemach cyfrowych, w tym reprezentacje liczbowe w urządzeniach cyfrowych, systemy liczbowe. Reprezentacja informacji i danych; różnice w implementacji operacji arytmetycznych przy użyciu różnych reprezentacji; podstawy statystyki matematycznej, opisowej, wnioskowania i rachunku prawdopodobieństwa. Pojęcie zmiennych losowych oraz ich rozkłady i relacje. Zbieranie danych i estymacje, cechy i badania statystyczne, organizacja badań statystycznych, opracowanie danych, w tym mechanizmy statystyczne do czyszczenia i analizy danych. Testy statystyczne, modelowanie i eksperymenty, korelacja i analiza regresji, analiza współzależności i dynamiki zjawisk, analiza szeregów czasowych, poziomy istotności. Pojęcia podstawowe w stopniu zaawansowanym. Podstawy informatyki kwantowej i jej zastosowania w kryptografii, w tym: wprowadzenie do informatyki kwantowej, podstawowe bramki kwantowe, protokoły podstawowe, stochastyczne układy kwantowe, dyskryminacja stanów kwantowych, symulacje i eksperymenty kwantowe, podstawowe algorytmy kwantowe. Elementy kryptografii kwantowej, ataki kwantowe na klasyczne prymitywy kryptograficzne.
Zajęcia kierunkowe obowiązkowe	20	K2A_W1 K2A_W2 K2A_W5 K2A_U5 K2A_U8 K2A_U11	Zagadnienia współczesnej informatyki (wyrównanie poziomów), maszynowa reprezentacja danych i realizacja operacji arytmetycznych, organizacja jednostki centralnej, elementy konstrukcyjne komputera, system przerwań, systemy wymiany informacji, system operacyjny i jego zadania, metody dostępu do danych, algorytmy i struktury danych, wielozadaniowość i klasyczne problemy synchronizacji, wybrane zagadnienia programowania, wybrane, zaawansowane paradygmaty i metodyki programowania, wybrane języki programowania. Elementy systemów kryptograficznych, szyfry symetryczne, funkcje skrótu, szyfry strumieniowe, algorytmy asymetryczne, zastosowania algorytmów asymetrycznych, zarządzanie hasłami, ataki słownikowe, tęczowe tablice, kryptografia w sieciach WLAN, protokoły kryptograficzne, infrastruktura klucza publicznego, hashowanie, przedstawienie programów do łamania haseł. Risk modeling issues and risk analysis in IT systems. Introduction to machine learning, neural networks, convolutional neural networks, transfer learning and fine tuning, recurrent neural networks, adversarial attacks, generative adversarial networks, transformers, large language models, explainability and security of deep models. Zagadnienia niskopoziomowego bezpieczeństwa oprogramowania, bezpieczeństwo systemów operacyjnych i ich mechanizmów, kontrola dostępu, użytkownicy i uprawnienia, procesy, biblioteki i wywołania systemowe, izolacja procesów, pojęcia namespaces i kontenery, podpisywanie, audytowanie, rozszerzenia i modyfikacje bezpieczeństwa, hardening, Active Directory, metody eskalacji uprawnień, narzędzia do wyszukiwania podatności. Zagadnienia obszarów zadaniowych zarządzania bezpieczeństwem, zakres zarządzania, warstwy zabezpieczeń, analiza i ocena stanu ochrony fizycznej, strefy bezpieczeństwa i krytyczne punkty w systemie ochrony, reagowanie na incydenty i zarządzenie kryzysowe, zarządzanie tożsamością i kontrola dostępu, bezpieczeństwo danych, zarządzanie łańcuchem dostaw, zarządzanie zmianami, procesy audytowania i certyfikacji, ciągłość działania, system zarządzania bezpieczeństwem informacji. Dwa przedmioty w ramach tej grupy prowadzone są w języku angielskim.

Zajęcia obieralne realizowane jako Project Based Learning	6	K2A_W6 K2A_U1 K2A_U4 K2A_U5 K2A_U6 K2A_U7 K2A_U8	Zadania inżynierskie realizowane jako interdyscyplinarny projekt grupowy o tematyce zgodnej z wybraną specjalnością dyplomowania.
Grupa zajęć wybieralnych realizowanych w ramach specjalności: cyberbezpieczeństwo oprogramowania	26	K2A_W1 K2A_W2 K2A_W6 K2A_U2 K2A_U3 K2A_U4 K2A_U5 K2A_U6 K2A_U9 K2A_U10 K2A_K1	Zagrożenia, podatności i ataki na oprogramowanie, inżynieria wsteczna, metody testowania oprogramowania, architektura i automatyczne testowanie oprogramowania. Uwierzytelnienie i autoryzacja, modele federacyjne, zarządzanie tożsamością, zarządzanie dostępem, uwierzytelnienie, autoryzacja, sesja, trust model. Zagadnienia integracji programowania, zabezpieczeń i operacji, continous integration, continous deployment, zaawansowane testowanie pod kątem bezpieczeństwa. Wprowadzenie do bezpieczeństwa mobilnego, bezpieczeństwo mobilnych systemów operacyjnych, uprawnienia aplikacji mobilnych i ryzyko związane z prywatnością, sandboksowanie aplikacji mobilnych i izolacja, zarządzanie urządzeniami mobilnymi i rozwiązania bezpieczeństwa, bezpieczeństwo sieciowe i urządzenia mobilne, testowanie penetracyjne aplikacji mobilnych, bezpieczne aktualizacje oprogramowania mobilnego, bezpieczeństwo aplikacji mobilnych w chmurze, aspekty prawne i regulacyjne bezpieczeństwa mobilnego, nowe trendy i przyszłość bezpieczeństwa mobilnego. Zagadnienia analizy incydentów, inżynieria wsteczna, analiza powłamaniowa, kod poli- i metamorficzny, szyfrowane binaria. Zaawansowane zagadnienia bezpieczeństwa w oprogramowaniu sieciowym, bezpieczeństwo aplikacji internetowych, tokeny, projektowanie aplikacji internetowych, proces hakowania aplikacji webowych oraz ich zabezpieczenia, przetwarzanie danych i plików od użytkownika, oprogramowanie sieciowe/ internetowe, metodologie, aplikacje webowe, technologie tworzenia oprogramowania, architektura aplikacji webowych, specyfika bezpiecznego uwierzytelnienia. Omówienie identyfikacji i eksploatacji podatności w stopniu zaawansowanym, zagadnienia różnych klas podatności i ich wariantów, metody bezpieczeństwa i metody ich omijania, eksploatacja i identyfikacja. Zagadnienia teoretyczne i praktyczne związane z testami penetracyjnymi, metodyki bezpieczeństwa, rodzaje testów i definicja zakresu, rekonesans, modelowanie zagrożeń, wykrywanie podatności, eksploatacja podatności, eksploatacja powłamaniowa i raportowanie.
Grupa zajęć wybieralnych realizowanych w ramach specjalności: cyberbezpieczeństwo systemów i urządzeń	26	K2A_W1 K2A_W2 K2A_W6 K2A_U2 K2A_U3 K2A_U4 K2A_U5 K2A_U6 K2A_U9 K2A_U10 K2A_K1	Zaawansowane zagadnienia projektowania i konfiguracji sieci komputerowych ze świadomością zagrożeń i w kontekście bezpieczeństwa, zabezpieczanie sieci, testowanie sieci, standardowe porty i aplikacje, sposoby łączenia się do różnych aplikacji, ataki sieciowe, analiza sieci bezprzewodowych, zasady przesyłu danych w sieci Internet, mechanizmy zapewnienia bezpieczeństwa. Zaawansowane zagadnienia związane z bezpieczeństwem zdecentralizowanych aplikacji (DApp), systemy rozproszone, zagadnienia podstawowe aplikacji zdecentralizowanych, blockchainy i architektura aplikacji, język Solidity i wzorce bezpieczeństwa, podatności interfejsu użytkownika, ochrona kluczy prywatnych i zarządzanie tożsamością, bezpieczeństwo DeFi i NFT, proces audytu smart kontraktów, wprowadzenie do systemów chmurowych, aplikacje w rozwiązanych chmurowych. Podstawy pojęciowe zaawansowanych systemów OT, komponenty OT i IT w fabrykach oraz ich podatności, przemysłowe systemy klasy CPS, sieci komunikacyjne OT, sieci komputerowe IT, zagadnienia bezpieczeństwa przemysłowego Internetu rzeczy (IIOT), analiza przypadków i znanych metod atakowania, dobre praktyki projektowania z wbudowanym bezpieczeństwem.

			Złożone aspekty bezpieczeństwa urządzeń, aplikacji, systemów komputerowych i cyberzagrożeń, bezpieczeństwo systemów informatycznych, modelowanie zagrożeń, ataki na oprogramowanie, inżynieria wsteczna, bezpieczeństwo aplikacji internetowych, metodologie, komunikacja i izolacja procesów itp. Zaawansowane zagadnienia bezpieczeństwa baz danych, metody zabezpieczeń, metody komunikacji z aplikacjami, studium przypadku. Wprowadzenie do zagadnień bezpieczeństwa dotyczących rozwiązań IoT, zagadnienia bezpieczeństwa podczas tworzenia systemu IoT, charakterystyka systemów IoT, koncepcje cyberbezpieczeństwa w odniesieniu do IoT, sprzęt IoT i cyberbezpieczeństwo, wyzwania cyberbezpieczeństwa IoT, luki w zabezpieczeniach systemów IoT, wektory ataków IoT, technologie bezpieczeństwa IoT, zabezpieczanie i ochrona systemów IoT przed cyberatakami, bezpieczeństwo przechowywania danych IoT. Najlepsze praktyki cyberbezpieczeństwa w systemach IoT. Zagadnienia ciągłego monitorowania zdolności systemów do działania bezpiecznego, proaktywne wyszukiwanie zagrożeń (thread hunting) i reagowanie na incydenty, koncepty SIEM, SOAR, Cyber Threat Intelligence, zaawansowane koncepty i technologie monitorowania. Zagadnienia bezpieczeństwa w pojazdach autonomicznych, drony i pojazdy autonomiczne (AGV), metody sterowania bezzałogowymi statkami powietrznymi (UAV), komunikacja z pojazdami AGV, mechanizmy symulacji statków i pojazdów autonomicznych, systemy rojowe, bezpieczeństwo komunikacji, zabezpieczenie przed inżynierią wsteczną.
Seminarium dyplomowe	2	K2A_W6 K2A_U2 K2A_U4 K2A_U7 K2A_U8 K2A_U11 K2A_K1 K2A_K3	Teoretyczne i praktyczne aspekty przygotowywania pracy dyplomowej. Metodyka opracowywania i prezentowania wyników. Prezentacja postępów oraz wyników prowadzonych prac.
Praca dyplomowa magisterska	20	K2A_W6 K2A_U1 K2A_U2 K2A_U3 K2A_U4 K2A_U5 K2A_U7 K2A_U8 K2A_U10 K2A_K1 K2A_K3	Zidentyfikowanie, sformułowanie i rozwiązanie złożonego i nietypowego problemu naukowego związanego z bezpieczeństwem oprogramowania oraz systemów komputerowych przez zastosowanie metod zapewniania bezpieczeństwa systemów komputerowych oraz zasad nauki i techniki. Założenia zadania wymuszą zastosowanie innowacyjnego podejścia poprzez przystosowanie istniejących lub opracowanie nowych metod i narzędzi oraz skłonią do szerokiego włączania wątków badawczych w zakresie podjętego tematu. Prezentacja postępów oraz wyników prowadzonych prac.
Zajęcia z uczelnianej bazy zajęć obieralnych	2	K2A_W7 K2A_U9 K2A_K1	Zapoznanie się z najnowszymi, interdyscyplinarnymi zagadnieniami z zakresu wybranej dyscypliny.

Sposoby weryfikacji i oceny efektów uczenia się osiągniętych przez studenta w trakcie całego cyklu kształcenia

Nazwa sposobu weryfikacji i oceny efektów uczenia się	Opis sposobu weryfikacji i oceny efektów uczenia się
Egzamin pisemny	Egzamin pisemny obejmuje pisemne odpowiedzi na pytania/zadania dotyczące zagadnień obejmujących treści programowe danego przedmiotu. Czas trwania egzaminu jest ograniczony i jest podawany przez egzaminatora przed rozpoczęciem egzaminu.
Egzamin ustny	Egzamin ustny obejmuje ustne odpowiedzi na pytania dotyczące zagadnień obejmujących treści programowe danego przedmiotu. Student ma prawo do ograniczonego czasowo przygotowania się do odpowiedzi oraz sporządzania notatek.
Sprawdzian pisemny	Sprawdzian pisemny obejmuje fragment treści programowych przedmiotu, np. jedno ćwiczenie laboratoryjne, określony typ zadań itp.

Egzamin dyplomowy	Egzamin składa się z trzech części: przedstawienia pracy dyplomowej w formie prezentacji, dyskusji nad przedstawionymi wynikami pracy oraz odpowiedzi na pytania otwarte postawione przez członków komisji egzaminacyjnej.
Test	Test polega na wyborze jednej lub kilku podanych odpowiedzi na postawione pytanie.
Kolokwium pisemne	Kolokwium pisemne obejmuje opisowe odpowiedzi na pytania dotyczące zagadnień obejmujących treści programowe danego przedmiotu. Czas trwania kolokwium jest ograniczony i jest podawany przez egzaminatora przed jego rozpoczęciem. Ta forma weryfikacji może być stosowana w przypadku przedmiotów niekończących się egzaminem.
Kolokwium ustne	Kolokwium ustne obejmuje ustne odpowiedzi na pytania dotyczące zagadnień obejmujących treści programowe danego przedmiotu. Student ma prawo do ograniczonego czasowo przygotowania się do odpowiedzi oraz sporządzania notatek. Ta forma weryfikacji może być stosowana w przypadku przedmiotów niekończących się egzaminem.
Prezentacje multimedialne/referat	Prezentacja, najczęściej multimedialna, na określony temat. Jest przedstawiana przez studenta indywidualnie lub w zespole.
Praca dyplomowa	Student przygotowuje pisemne opracowanie, liczące od kilkudziesięciu do kilkuset stron, będące sprawozdaniem z przeprowadzonych przez studenta działań. Praca dyplomowa może mieć charakter teoretyczny, praktyczny, konstrukcyjny lub może zawierać opis wykonanych eksperymentów i obserwacji. Praca dyplomowa może mieć charakter projektu badawczo-naukowego.
Sprawozdanie	Sprawozdanie zawiera opis pomiarów, badań, obserwacji itp. przeprowadzonych w ramach ćwiczenia laboratoryjnego, wyjazdu terenowego itp. Sprawozdanie może podlegać zaliczeniu bez wystawiania oceny.
Projekt	Projekt stanowi potwierdzenie realizacji konkretnego zadania (najczęściej inżynierskiego) wykonanego po przyjęciu narzuconych przez prowadzącego założeń wstępnych. Dopuszcza się m.in. następujące formy projektów: opracowanie pisemne, program komputerowy, opis HDL, rysunek, model matematyczny itp.
Obserwacja aktywności i umiejętności studenta	Prowadzący, na podstawie obserwacji zachowania studenta, jego aktywności i umiejętności wykazanych w trakcie zajęć, może uznać osiągnięcie zakładanych efektów uczenia się.