Program studiów

Kierunek: Cyberbezpieczeństwo

Spis treści

Charakterystyka kierunku

Informacje podstawowe

Nazwa wydziału:	Wydział Informatyki, Elektroniki i Telekomunikacji
Nazwa kierunku:	Cyberbezpieczeństwo
Poziom:	Studia magisterskie inżynierskie II stopnia
Profil:	Ogólnoakademicki
Forma:	Stacjonarne
Klasyfikacja ISCED:	0619
Liczba punktów ECTS konieczna do ukończenia studiów na danym poziomie:	90
Tytuł zawodowy nadawany absolwentom:	magister inżynier
Termin rozpoczęcia cyklu:	2025/2026, semestr letni
Czas trwania studiów (liczba semestrów):	3

Dziedzina/-y nauki, do której/-ych przyporządkowany jest kierunek studiów:

Dziedzina nauk inżynieryjno-technicznych

Dyscyplina/-y naukowa/-e, do której/-ych przyporządkowany jest kierunek studiów:

Dyscyplina	Udział procentowy	ECTS
Informatyka techniczna i telekomunikacja	100%	90

Wskazanie związku kierunku studiów ze strategią rozwoju i misją uczelni

AGH rozwijając się jako uniwersytet przyszłości powołuje nowatorskie kierunki kształcenia, których absolwenci będą zdolni do podejmowania najważniejszych wyzwań współczesności, stając się liderami rozwoju gospodarki i społeczeństwa. Kierunek Cyberbezpieczeństwo doskonale wpisuje się w misję uczelni – przede wszystkim poprzez kształcenie, które umożliwia tworzenie innowacji, pomagających rozwiązywać najważniejsze problemy współczesności. Bez wątpienia potrzeba zapewnienia bezpieczeństwa w cyberprzestrzeni jest jedną z palących potrzeb współczesnego świata.

Jednym ze strategicznych celów AGH jest nowoczesne kształcenie, które zarówno pod względem merytorycznym jak i sposobem prowadzenia zajęć jest atrakcyjne dla studentów. Na kierunku Cyberbezpieczeństwo studiów II stopnia zajęcia prowadzą naukowcy i eksperci, którzy nie tylko tworzą nową wiedzę, ale także mają doświadczenie w jej zastosowaniach praktycznych. Podczas zajęć używane są nowoczesne metody kształcenia.

Mając na uwadze fakt, że wysoka jakość edukacji studentów w AGH wiąże się nie tylko z profesjonalizmem i wiedzą prowadzących, uczelnia dba także o odpowiedni system wsparcia dla studentów. Dzięki temu realizowany jest kolejny cel strategiczny – uczelnia otwarta dla studentów, ich rozwoju zawodowego i realizacji pasji. Kierunek Cyberbezpieczeństwo został opracowany tak, aby wspomagać rozwój indywidualnych zainteresowań i kompetencji studentów. Realizowane jest to m.in. poprzez szeroki zakres poruszanej tematyki dotyczącej cyberbezpieczeństwa, indywidualny wybór przedmiotów obieralnych, wsparcie przedsiębiorczości czy rozwój własnych projektów naukowych.

Informacja na temat uwzględnienia w programie studiów potrzeb społeczno-gospodarczych oraz zgodności zakładanych efektów uczenia się z tymi potrzebami

Kierunek Cyberbezpieczeństwo na poziomie studiów magisterskich oferuje kształcenie o profilu ogólnoakademickim i odbywa się w systemie stacjonarnym. Program kształcenia przygotowano uwzględniając potrzeby społeczno-gospodarcze nie tylko na poziomie

regionu i kraju, ale także globalnym. Trudno wyobrazić sobie rozwój gospodarczy bez bezpiecznego dostępu do danych cyfrowych i powszechnych dziś usług elektronicznych. Jednak wysoki poziom informatyzacji stawia wysokie wymagania odnośnie cyberbezpieczeństwa, zarówno przed podmiotami publicznymi jak i przedsiębiorstwami. Poza tym, coraz więcej aspektów życia społecznego jest bezpośrednio związane z dostępem do globalnej sieci Internet, co sprawia że bezpieczeństwo w cyberprzestrzeni staje się coraz poważniejszym wyzwaniem. Jednocześnie rynek IT wciąż boryka się z problemem braku wysokiej klasy specjalistów mających szeroką wiedzę z zakresu cyberbezpieczeństwa. Opracowany i wciąż udoskonalany program studiów zapewnia zgodność efektów kształcenia z bieżącymi potrzebami społeczno-gospodarczymi.

Program studiów na kierunku Cyberbezpieczeństwo został przygotowany uwzględniając prognozy rozwoju rynku IT oraz wiedzę i doświadczenie pracowników Wydziału IET, które wynikają z prowadzenia badań w ramach krajowych i międzynarodowych projektów naukowo-badawczych oraz aktywnej współpracy z przemysłem. Ważnym wyrazicielem potrzeb odnośnie programu jest Rada Społeczna działającej przy Wydziale IET. W kontekście tych studiów warto pamiętać o strategii cyberbezpieczeństwa Rzeczpospolitej Polskiej, która wskazuje na potrzebę budowania świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa.

Ścieżki kształcenia - zakres w języku polskim oraz w języku angielskim

Brak ściśle wyodrębnionych ścieżek kształcenia. Studenci mogą indywidualnie dopasowywać zakres tematyczny poprzez wybór przedmiotów obieralnych.

Ścieżki dyplomowania - zakres w języku polskim oraz w języku angielskim

Nazwy specjalności w języku polskim oraz w języku angielskim

Nazwa [pl]	Nazwa [en]

Ogólne informacje o programie studiów

Kierunek: Cyberbezpieczeństwo

Ogólne informacje związane z programem studiów (ogólne cele kształcenia oraz możliwości zatrudnienia, typowe miejsca pracy i możliwości kontynuacji kształcenia przez absolwentów)

Studia magisterskie na kierunku Cyberbezpieczeństwo mają na celu kształcenie specjalistów, którzy będą posiadać kompetencje w zakresie szeroko pojętego bezpieczeństwa danych cyfrowych w systemach informatycznych, zabezpieczania sieci komputerowych oraz ochrony użytkowników w cyberprzestrzeni. Jednak kształcenie nie jest ograniczone do ciasnych ram wąskiej specjalizacji, gdyż absolwent studiów drugiego stopnia powinien mieć szerokie horyzonty i zróżnicowane kompetencje. Z tego względu w programie studiów znajdują się moduły poruszające różne aspekty cyberbezpieczeństwa, przedstawiające możliwe zastosowania praktyczne, rozwijające kompetencje techniczne i umiejętności miękkie, wspierające przedsiębiorczość i organizację pracy zespołowej czy odkrywające metodykę prowadzenia prac badawczo-rozwojowych w celu tworzenia innowacji.

Program studiów uwzględnia prognozy rozwoju rynku IT oraz opinie ekspertów z otoczenia gospodarczego (np. Rada Społeczna), z którymi aktywnie współpracuje Wydział IET. Dlatego absolwenci kierunku Cyberbezpieczeństwo będą poszukiwanymi specjalistami na rynku pracy – zarówno jako kompetentni inżynierowie jak i specjaliści na szczeblu kierowniczym, chętnie zatrudniani w firmach mających świadomość wagi cyberbezpieczeństwa w działalności gospodarczej czy instytucjach publicznych i organach odpowiedzialnych za bezpieczeństwo. Warto wspomnieć tu o stałej współpracy w zakresie unowocześniania kształcenia z takimi firmami jak: Akamai, Cisco, Comarch, ESET, EY, IBM, Intel, Motorola, Nokia, Orange czy Palo Alto Networks.

Absolwenci będą mieli możliwość dalszego kontynuowania kształcenia. Zdobyta wiedza umożliwi odbywanie specjalistycznych szkoleń i zdobywanie certyfikatów z zakresu cyberbezpieczeństwa. Chętni będą mogli kontynuować kształcenie na studiach trzeciego stopnia, czyli w Szkole Doktorskiej AGH i prowadzić badania w zespołach naukowych, pod okiem doświadczonych naukowców.

Informacja na temat uwzględnienia w programie studiów wniosków z analizy wyników monitoringu karier zawodowych studentów i absolwentów

Podczas opracowywania programu studiów na kierunku Cyberbezpieczeństwo brano pod uwagę losy absolwentów Wydziału IET – badania potwierdzają ich świetną pozycję na rynku pracy. Bardzo duży odsetek studentów stwierdza, że drugi raz wybraliby te same studia. Prawie wszyscy podejmują pracę po zakończeniu studiów, a bardzo wiele osób pracuje już podczas studiów. Wielu absolwentów zakłada własne firmy i rozpoczyna działalność gospodarczą (ten aspekt również wzięto pod uwagę w programie studiów). Absolwenci kierunku Cyberbezpieczeństwo będą specjalistami z cenionymi i poszukiwanymi kompetencjami na rynku pracy, na co wskazują opinie ekspertów z otoczenia gospodarczego i bieżące trendy w branży IT.

Wnioski z analizy wyników monitoringu karier zawodowych studentów i absolwentów są brane pod uwagę m.in. dlatego, że kierunek podlega regulacjom Uczelnianego Systemu Zapewnienia Jakości Kształcenia. System ten ma na celu dostosowywanie procesu kształcenia do zmieniających się potrzeb i wymagań oraz jeszcze lepsze diagnozowanie i eliminację zjawisk niepożądanych w procesie kształcenia. Dzięki takiemu podejściu możliwe jest udoskonalenie kształcenia poprzez monitorowanie jakości nauczania, tworzenie stosownych procedur oceny metod i warunków kształcenia, czy podejmowanie działań korygujących oraz nowych inicjatyw dydaktycznych.

Informacja na temat uwzględnienia w programie studiów wymagań i zaleceń komisji akredytacyjnych, w szczególności Polskiej Komisji Akredytacyjnej i środowiskowych komisji akredytacyjnych

Wydział IET prowadzi kierunki studiów, które mają przyznaną akredytację z wyróżnieniem. Doświadczenia zdobyte podczas przygotowywania do poprzednich akredytacji oraz zalecenia otrzymane dla innych kierunków po wizycie Polskiej Komisji Akredytacyjnej zostały uwzględnione podczas opracowywania programu studiów magisterskich na kierunku Cyberbezpieczeństwo.

Ponadto ulepszenia w programie kształcenia są wprowadzane na wniosek ekspertów zewnętrznych z otoczenia gospodarczego oraz samych studentów (np. studenci uczestniczą w procesie tworzenia planów zajęć). Uwzględniane są opinie Wydziałowej Rady Samorządu Studentów (WRSS).

Informacja na temat uwzględnienia w programie studiów przykładów dobrych praktyk

Program kształcenia na kierunku Cyberbezpieczeństwo uwzględnienia bogate doświadczenie dydaktyczne i naukowe pracowników wydziału IET, w tym zdobyte podczas prac w ramach międzynarodowych projektów badawczych. Kształcenie kładzie nacisk na rozwiązywanie praktycznych problemów w sposób twórczy, a różnorodność poruszanej tematyki umożliwia szerokie spojrzenie na problematykę cyberbezpieczeństwa i łączenie zdobytej wiedzy. Nie bez znaczenia jest zastosowanie szerokiego wachlarza metod i narzędzi dydaktycznych. Student może samodzielnie wybrać przedmioty kierunkowe z szerokiej oferty przedmiotów obieralnych, przez co rozwijać indywidualne zainteresowania i kompetencje.

Prowadzący zajęcia dydaktyczne udoskonalają swoje kompetencje dydaktyczne (np. program POWER, szkolenia Centrum e-Learningu AGH). W realizację programu studiów zaangażowani są doświadczeni dydaktycy, w tym nagradzani za osiągnięcia na polu kształcenia (np. Laur Dydaktyka AGH, Rektorskie Nagrody Dydaktyczne, itp.). Wielu prowadzących jest otwartych na potrzeby i inicjatywy studentów, chętnie angażując się w dodatkowe działania i wydarzenia. Studenci są zapraszani do rozwijania zdolności naukowych, poprzez prowadzenie badań naukowych pod okiem doświadczonych naukowców i uczestnictwo w konferencjach naukowych. Kierunek ma wyznaczonego opiekuna, który jest w kontakcie z organami studenckimi i dba o jakość kształcenia oraz wprowadzanie udoskonaleń do programu studiów.

Informacja na temat współdziałania w zakresie przygotowania programu studiów z interesariuszami zewnętrznymi, w szczególności stowarzyszeniami i organizacjami zawodowymi, społecznymi

Wydział IET aktywnie współpracuje w zakresie kształtowania programów dydaktycznych z Radą Społeczną – kolegialnym ciałem doradczym, które składa się z przedstawicieli przedsiębiorstw, instytucji, urzędów administracji państwowej i samorządowej oraz osób fizycznych działających w szeroko pojętej branży IT. Współpraca w zakresie kształcenia z otoczeniem gospodarczym, stowarzyszeniami oraz organizacjami zawodowymi i społecznymi rozwija się i przynosi wymierne efekty. Przedstawiciele czołowych firm z branży IT potwierdzają potrzebę kształcenia specjalistów z zakresu cyberbezpieczeństwa. Potwierdzeniem współdziałania z interesariuszami zewnętrznymi jest aktywne zaangażowanie ekspertów z przedsiębiorstw w kształcenie na kierunku Cyberbezpieczeństwo. Eksperci zewnętrzni wyrazili gotowość wsparcia kształcenia, m.in. w ramach zajęć dotyczących zaawansowanej detekcji oprogramowania złośliwego, obsługiwania incydentów czy pozyskiwania wiedzy związanej z zagrożeniami w cyberprzestrzeni.

Wymiar, zasady i forma odbywania praktyk zawodowych

Program studiów nie przewiduje odbywania obowiązkowych praktyk zawodowych.

Warunki rekrutacji na studia

Kierunek: Cyberbezpieczeństwo

Opis kompetencji oczekiwanych od kandydata ubiegającego się o przyjęcie na studia

Warunkiem przystąpienia do rekrutacji na studia drugiego stopnia jest posiadanie tytułu inżyniera lub magistra inżyniera. Dyplom ukończenia studiów inżynierkich (studiów I stopnia) powinien być uzyskany na kierunku Cyberbezpieczeństwo, Teleinformatyka, Informatyka, Elektronika i Telekomunikacja lub pokrewnych.

Warunki rekrutacji, z uwzględnieniem laureatów oraz finalistów olimpiad stopnia centralnego, a także laureatów konkursów międzynarodowych oraz ogólnopolskich

Zasady i warunki rekrutacji określają odpowiednie Uchwały i Zarządzenia. Szczegółowe informacje są dostępne na stronie internetowej dla kandydatów:

https://rekrutacja.agh.edu.pl

Przewidywany limit przyjęć na studia wraz ze wskazaniem minimalnej liczby osób przyjętych, warunkującej uruchomienie edycji studiów

Minimalna liczba studentów: 24

Maksymalna liczba studentów: 48

Efekty uczenia się

Kierunek: Cyberbezpieczeństwo

Wiedza

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
CBZ2A_W01	Absolwent ma pogłębioną wiedzę dotyczącą metod prowadzenia badań w zakresie informatyki i telekomunikacji: modelowania, symulacji, analizy, obliczeń i prowadzenia eksperymentów	P7S_WG_A
CBZ2A_W02	Absolwent ma pogłębioną wiedzę w zakresie zabezpieczania urządzeń i sieci komputerowych oraz wpływu stosowania mechanizmów bezpieczeństwa na wydajność i koszty systemów informatycznych	P7S_WG_A, P7S_WG_A_Inz
CBZ2A_W03	Absolwent ma pogłębioną wiedzę na temat tworzenia/integracji oprogramowania oraz projektów informatycznych, obejmującą również kwestie zarządzania złożonymi projektami	P7S_WG_A, P7S_WG_A_Inz
CBZ2A_W04	Absolwent zna i rozumie trendy rozwojowe w zakresie cyberbezpieczeństwa oraz ich wpływ na gospodarkę i społeczeństwo	P7S_WG_A
CBZ2A_W05	Absolwent zna i rozumie zasady prowadzenia działalności gospodarczej w branży IT, ma wiedzę dotyczącą pozatechnicznych aspektów działalności w tej branży, w tym zasad własności intelektualnej i etyki	P7S_WK_A, P7S_WK_A_Inz

Umiejętności

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
CBZ2A_U01	Absolwent potrafi definiować oraz realizować zadania związane z zapewnieniem bezpieczeństwa danych cyfrowych i użytkowników systemów informatycznych, w tym również wymagające podejścia innowacyjnego, poprzez dobór, krytyczną analizę i właściwą interpretację danych pozyskanych z wiarygodnych źródeł informacji oraz pozyskanych poprzez wykonanie własnych badań	P7S_UW_A_Inz_01, P7S_UW_A
CBZ2A_U02	Absolwent potrafi wykryć podatności lub ataki na zasoby chronionego systemu, wykonać analizę ryzyka, a także opracować i wykonać odpowiednią procedurę działania w celu ochrony systemu bądź sieci teleinformatycznej	P7S_UW_A_Inz_01, P7S_UW_A
CBZ2A_U03	Absolwent potrafi opracować raport, przedstawić specjalistyczną prezentację i poprowadzić dyskusję na temat zadania czy projektu związanego z cyberbezpieczeństwem, również w języku obcym na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego	P7S_UK_A
CBZ2A_U04	Absolwent potrafi pracować indywidualnie, zespołowo oraz kierować zespołem projektowym lub badawczym i planować jego pracę, komunikując się przy użyciu technik właściwych dla branży IT	P7S_UO_A
CBZ2A_U05	Absolwent ma umiejętność samokształcenia, potrafi planować swój dalszy rozwój zawodowy w branży IT, jak również wspomagać innych w tym zakresie	P7S_UU_A
CBZ2A_U06	Absolwent potrafi planować i prowadzić badania naukowe z dziedziny informatyki i telekomunikacji oraz przeprowadzić krytyczną analizę danego rozwiązania z zakresu cyberbezpieczeństwa, w tym sformułować i testować hipotezy związane z problemami badawczymi	P7S_UW_A
CBZ2A_U07	Absolwent potrafi realizować i kierować realizacją projektów informatycznych uwzględniając aspekty techniczne i pozatechniczne (np. ekonomiczne, prawne) oraz ocenić innowacyjność danego rozwiązania i możliwość zrealizowania go jako przedsięwzięcie komercyjne	P7S_UW_A, P7S_UW_A_Inz_02

Kompetencje społeczne

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
CBZ2A_K01	Absolwent rozumie jakie znaczenie ma wiedza w rozwiązywaniu praktycznych problemów oraz rozumie potrzebę krytycznej oceny posiadanej wiedzy i potrzebę ciągłego dokształcania się, a także zasięgania opinii innych ekspertów z branży IT	P7S_KK_A
CBZ2A_K02	Absolwent jest gotów działać na rzecz środowiska społecznego i inspirować innych do takich działań - w szczególności dotyczących bezpieczeństwa w cyberprzestrzeni, a także myśleć i działać w sposób przedsiębiorczy	P7S_KO_A
CBZ2A_K03	Absolwent ma świadomość roli zawodowej i społecznej absolwenta uczelni technicznej oraz wagi przestrzegania i rozwijania zasad etyki zawodowej w branży IT, szczególnie w obszarze cyberbezpieczeństwa	P7S_KR_A

Tabela zgodności kompetencji inżynierskich (Inz) z kierunkowymi efektami uczenia się (KEU)

Kierunek: Cyberbezpieczeństwo

Wiedza

Symbol CEU	Efekty uczenia się dla kwalifikacji obejmujących kompetencje inżynierskie	Odniesienia do KEU
P7S_WG_A_Inz	Absolwent zna i rozumie podstawowe procesy zachodzące w cyklu życia urządzeń, obiektów i systemów technicznych	CBZ2A_W02, CBZ2A_W03
P7S_WK_A_Inz	Absolwent zna i rozumie podstawowe zasady tworzenia i rozwoju różnych form indywidualnej przedsiębiorczości	CBZ2A_W05

Umiejętności

Symbol CEU	Efekty uczenia się dla kwalifikacji obejmujących kompetencje inżynierskie	Odniesienia do KEU
P7S_UW_A_Inz_01	Absolwent potrafi planować i przeprowadzać eksperymenty, w tym pomiary i symulacje komputerowe, interpretować uzyskane wyniki i wyciągać wnioski; przy identyfikacji i formułowaniu specyfikacji zadań inżynierskich oraz ich rozwiązywaniu: - 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; dokonywać krytycznej analizy sposobu funkcjonowania istniejących rozwiązań technicznych i oceniać te rozwiązania	CBZ2A_U01, CBZ2A_U02
P7S_UW_A_Inz_02	Absolwent potrafi projektować – zgodnie z zadaną specyfikacją – oraz wykonywać typowe dla kierunku studiów proste urządzenia, obiekty, systemy lub realizować procesy, używając odpowiednio dobranych metod, technik, narzędzi i materiałów	CBZ2A_U07

Matryca pokrycia efektów kierunkowych

Kierunek: Cyberbezpieczeństwo

2025/2026/S/IIi/IEiT/CBZ/all

Przedmiot	Kod	Semestr	CBZ2A_W01	CBZ2A_W02	CBZ2A_W03	CBZ2A_W04	CBZ2A_W05	CBZ2A_U01	CBZ2A_U02	CBZ2A_U03	CBZ2A_U04	CBZ2A_U05	CBZ2A_U06	CBZ2A_U07	CBZ2A_K01	CBZ2A_K02	CBZ2A_K03
Analiza kryminalistyczna danych cyfrowych	ICBZS.IIi1K.15726.25	1s	x	x				x	x						x		
Capture the Flag (CTF)	ICBZS.IIi1K.15650.25	1s		x		x		x	x		x	x			x	x	
Analiza danych i uczenie maszynowe	ICBZS.IIi1K.08565.25	1s	x		x			x						x	x		
Badanie wydajności systemów	ICBZS.IIi1K.15727.25	1s	x	x						x			x		x		x
Ochrona systemów i sieci	ICBZS.IIi1K.16324.25	1s		x		x		x	x							x	x
Zarządzanie i ekonomia projektów	ICBZS.IIi1HS.05705.25	1s			x		x			x	x		x	x	x	x	
Etyka i prawo w cyberbezpieczeństwie	ICBZS.IIi1HS.15728.25	1s				x	x							x	x	x	x
Detekcja i analiza zagrożeń komputerowych	ICBZS.IIi2K.15730.25	2s		x	x			x	x	x	x				x		x
Kryptografia postkwantowa	ICBZS.IIi2K.15725.25	2s	x	x	x	x		x	x	x		x	x		x	x	x
Threat Intelligence	ICBZS.IIi2K.15651.25	2s		x	x	x	x	x	x	x		x		x		x	x
Deep Learning Algorithms for Cybersecurity Applications	ICBZS.IIi2K.15652.25	2s	x	x		x	x	x	x	x	x		x		x	x	x
Szeregi czasowe	ICBZS.IIi2K.14153.25	2s	x	x									x		x	x	
Metodyki projektów z zakresu cyberbezpieczeństwa	ICBZS.IIi2K.15731.25	2s				x	x				x			x			x
Metodyka prowadzenia prac B+R	ICBZS.IIi2O.15729.25	2s	x				x	x		x	x		x	x	x	x	x
Bezpieczeństwo w systemach 5G i 6G	ICBZS.IIi2K.15732.25	2s	x	x		x		x	x	x	x		x		x	x	x
Bezpieczeństwo treści multimedialnych	ICBZS.IIi2K.15733.25	2s		x	x	x							x		x		

Przedmiot	Kod	Semestr	CBZ2A_W01	CBZ2A_W02	CBZ2A_W03	CBZ2A_W04	CBZ2A_W05	CBZ2A_U01	CBZ2A_U02	CBZ2A_U03	CBZ2A_U04	CBZ2A_U05	CBZ2A_U06	CBZ2A_U07	CBZ2A_K01	CBZ2A_K02	CBZ2A_K03
Wyzwania i kierunki rozwoju cyberbezpieczeństwa	ICBZS.IIi2K.15734.25	2s	x	x		x		x	x			x	x		x	x	x
Psychologiczne aspekty cyberbezpieczeństwa	ICBZS.IIi2K.15735.25	2s	x			x		x	x				x	x		x	
Język angielski B2+ - obowiązkowy kurs języka specjalistycznego na studiach II stopnia dla studentów Wydziału Informatyki, Elektroniki i Telekomunikacji	ICBZS.IIi2JO.04744.25	2s								x							
Praca w kole naukowym	ICBZS.IIi2K.05333.25	2s	x	x	x		x	x		x		x		x	x	x	
Purple Teaming	ICBZS.IIi2K.18595.25	2s		x		x		x	x			x	x	x	x	x	x
Działalność naukowa	ICBZS.IIi4K.07501.25	3s	x			x		x		x	x		x	x	x		x
Warsztaty dyplomowe	ICBZS.IIi4O.06764.25	3s	x			x				x		x	x	x	x		
Cybersecurity Operations	ICBZS.IIi4K.15653.25	3s		x	x		x	x	x			x		x		x	x
Architektura korporacyjna i zarządzanie ryzykiem	ICBZS.IIi4K.15808.25	3s				x	x	x			x				x	x	x
Przetwarzanie języka naturalnego metodami AI/ML	ICBZS.IIi4K.15736.25	3s	x		x						x				x		
Technologia blockchain	ICBZS.IIi4K.17198.25	3s	x		x	x	x	x			x	x	x	x	x	x	x
Praca dyplomowa	ICBZS.IIi4K.00163.25	3s	x			x				x	x	x	x		x	x	x
Odpowiedzialność prawna za cyberataki i ochronę zasobów	ICBZS.IIi4HS.18605.25	3s				x	x							x			x
Suma (obowiązkowy):			7	5	3	6	3	6	4	7	4	4	6	5	10	7	6
Suma (fakultatywny):			9	10	7	12	8	12	8	6	8	6	9	9	12	11	12
Suma:			16	15	10	18	11	18	12	13	12	10	15	14	22	18	18

Matryca charakterystyk efektów uczenia się w odniesieniu do modułów zajęć

Kierunek: Cyberbezpieczeństwo

2025/2026/S/IIi/IEiT/CBZ/all

Przedmiot	Kod	Semestr	P7S_WG_A	P7S_WG_A_Inz	P7S_WK_A	P7S_WK_A_Inz	P7S_UW_A_Inz_01	P7S_UW_A	P7S_UK_A	P7S_UO_A	P7S_UU_A	P7S_UW_A_Inz_02	P7S_KK_A	P7S_KO_A	P7S_KR_A
Analiza kryminalistyczna danych cyfrowych	ICBZS.IIi1K.15726.25	1s	x	x			x	x					x		
Capture the Flag (CTF)	ICBZS.IIi1K.15650.25	1s	x	x			x	x		x	x		x	x	
Analiza danych i uczenie maszynowe	ICBZS.IIi1K.08565.25	1s	x	x			x	x				x	x		
Badanie wydajności systemów	ICBZS.IIi1K.15727.25	1s	x	x				x	x				x		x
Ochrona systemów i sieci	ICBZS.IIi1K.16324.25	1s	x	x			x	x						x	x
Zarządzanie i ekonomia projektów	ICBZS.IIi1HS.05705.25	1s	x	x	x	x		x	x	x		x	x	x	
Etyka i prawo w cyberbezpieczeństwie	ICBZS.IIi1HS.15728.25	1s	x		x	x		x				x	x	x	x
Detekcja i analiza zagrożeń komputerowych	ICBZS.IIi2K.15730.25	2s	x	x			x	x	x	x			x		x
Kryptografia postkwantowa	ICBZS.IIi2K.15725.25	2s	x	x			x	x	x		x		x	x	x
Threat Intelligence	ICBZS.IIi2K.15651.25	2s	x	x	x	x	x	x	x		x	x		x	x
Deep Learning Algorithms for Cybersecurity Applications	ICBZS.IIi2K.15652.25	2s	x	x	x	x	x	x	x	x			x	x	x
Szeregi czasowe	ICBZS.IIi2K.14153.25	2s	x	x				x					x	x	
Metodyki projektów z zakresu cyberbezpieczeństwa	ICBZS.IIi2K.15731.25	2s	x		x	x		x		x		x			x
Metodyka prowadzenia prac B+R	ICBZS.IIi2O.15729.25	2s	x		x	x	x	x	x	x		x	x	x	x
Bezpieczeństwo w systemach 5G i 6G	ICBZS.IIi2K.15732.25	2s	x	x			x	x	x	x			x	x	x

Przedmiot	Kod	Semestr	P7S_WG_A	P7S_WG_A_Inz	P7S_WK_A	P7S_WK_A_Inz	P7S_UW_A_Inz_01	P7S_UW_A	P7S_UK_A	P7S_UO_A	P7S_UU_A	P7S_UW_A_Inz_02	P7S_KK_A	P7S_KO_A	P7S_KR_A
Bezpieczeństwo treści multimedialnych	ICBZS.IIi2K.15733.25	2s	x	x				x					x		
Wyzwania i kierunki rozwoju cyberbezpieczeństwa	ICBZS.IIi2K.15734.25	2s	x	x			x	x			x		x	x	x
Psychologiczne aspekty cyberbezpieczeństwa	ICBZS.IIi2K.15735.25	2s	x				x	x				x		x	
Język angielski B2+ - obowiązkowy kurs języka specjalistycznego na studiach II stopnia dla studentów Wydziału Informatyki, Elektroniki i Telekomunikacji	ICBZS.IIi2JO.04744.25	2s							x						
Praca w kole naukowym	ICBZS.IIi2K.05333.25	2s	x	x	x	x	x	x	x		x	x	x	x	
Purple Teaming	ICBZS.IIi2K.18595.25	2s	x	x			x	x			x	x	x	x	x
Działalność naukowa	ICBZS.IIi4K.07501.25	3s	x				x	x	x	x		x	x		x
Warsztaty dyplomowe	ICBZS.IIi4O.06764.25	3s	x					x	x		x	x	x		
Cybersecurity Operations	ICBZS.IIi4K.15653.25	3s	x	x	x	x	x	x			x	x		x	x
Architektura korporacyjna i zarządzanie ryzykiem	ICBZS.IIi4K.15808.25	3s	x		x	x	x	x		x			x	x	x
Przetwarzanie języka naturalnego metodami AI/ML	ICBZS.IIi4K.15736.25	3s	x	x						x			x		
Technologia blockchain	ICBZS.IIi4K.17198.25	3s	x	x	x	x	x	x		x	x	x	x	x	x
Praca dyplomowa	ICBZS.IIi4K.00163.25	3s	x					x	x	x	x		x	x	x
Odpowiedzialność prawna za cyberataki i ochronę zasobów	ICBZS.IIi4HS.18605.25	3s	x		x	x		x				x			x
Suma (obowiązkowy):			11	7	3	3	6	11	7	4	4	5	10	7	6
Suma (fakultatywny):			17	12	8	8	12	16	6	8	6	9	12	11	12
Suma:			28	19	11	11	18	27	13	12	10	14	22	18	18

Matryca kierunkowych efektów uczenia się w odniesieniu do form zajęć i sposobu zaliczenia, które pozwalają na ich uzyskanie

Kierunek: Cyberbezpieczeństwo

2025/2026/S/IIi/IEiT/CBZ/all

Nazwa modułu zajęć	Forma zajęć dydaktycznych	Sposób weryfikacji i oceny efektów uczenia się osiągniętych przez studenta w ramach poszczególnych form zajęć i dla całego modułu zajęć	Odniesienia do KEU
Analiza kryminalistyczna danych cyfrowych	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Egzamin, Wykonanie ćwiczeń laboratoryjnych, Studium przypadków , Zaliczenie laboratorium, Projekt, Sprawozdanie	CBZ2A_W01, CBZ2A_W02, CBZ2A_U01, CBZ2A_U02, CBZ2A_K01
Capture the Flag (CTF)	Ćwiczenia projektowe, Zajęcia warsztatowe	Projekt, Zaangażowanie w pracę zespołu, Wykonanie projektu	CBZ2A_W02, CBZ2A_W04, CBZ2A_U01, CBZ2A_U02, CBZ2A_U04, CBZ2A_U05, CBZ2A_K01, CBZ2A_K02
Analiza danych i uczenie maszynowe	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Zaliczenie laboratorium	CBZ2A_W01, CBZ2A_W03, CBZ2A_U01, CBZ2A_U07, CBZ2A_K01
Badanie wydajności systemów	Ćwiczenia audytoryjne, Ćwiczenia projektowe	Wykonanie ćwiczeń, Kolokwium, Wykonanie projektu	CBZ2A_W02, CBZ2A_W01, CBZ2A_U06, CBZ2A_U03, CBZ2A_K01, CBZ2A_K03
Ochrona systemów i sieci	Zajęcia seminaryjne, Ćwiczenia laboratoryjne	Kolokwium, Wykonanie ćwiczeń laboratoryjnych	CBZ2A_W02, CBZ2A_W04, CBZ2A_U01, CBZ2A_U02, CBZ2A_K02, CBZ2A_K03
Zarządzanie i ekonomia projektów	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Aktywność na zajęciach, Egzamin, Sprawozdanie, Projekt	CBZ2A_W03, CBZ2A_W05, CBZ2A_U03, CBZ2A_U04, CBZ2A_U06, CBZ2A_U07, CBZ2A_K01, CBZ2A_K02
Etyka i prawo w cyberbezpieczeństwie	Wykład, Zajęcia seminaryjne	Kolokwium, Aktywność na zajęciach, Udział w dyskusji, Zaangażowanie w pracę zespołu, Prezentacja	CBZ2A_W04, CBZ2A_W05, CBZ2A_U07, CBZ2A_K02, CBZ2A_K03, CBZ2A_K01
Detekcja i analiza zagrożeń komputerowych	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Udział w dyskusji, Kolokwium, Studium przypadków , Zaliczenie laboratorium, Wykonanie ćwiczeń laboratoryjnych	CBZ2A_W02, CBZ2A_W03, CBZ2A_U01, CBZ2A_U02, CBZ2A_U03, CBZ2A_U04, CBZ2A_K01, CBZ2A_K03
Kryptografia postkwantowa	Wykład, Ćwiczenia audytoryjne, Ćwiczenia projektowe	Egzamin, Wykonanie ćwiczeń, Kolokwium, Udział w dyskusji, Wykonanie projektu, Projekt, Zaangażowanie w pracę zespołu	CBZ2A_W02, CBZ2A_W04, CBZ2A_W01, CBZ2A_W03, CBZ2A_U01, CBZ2A_U03, CBZ2A_U05, CBZ2A_U02, CBZ2A_U06, CBZ2A_K01, CBZ2A_K02, CBZ2A_K03
Threat Intelligence	Wykład, Ćwiczenia projektowe	Aktywność na zajęciach, Wykonanie projektu, Kolokwium, Studium przypadków , Projekt, Zaangażowanie w pracę zespołu	CBZ2A_W02, CBZ2A_W04, CBZ2A_W05, CBZ2A_W03, CBZ2A_U01, CBZ2A_U02, CBZ2A_U03, CBZ2A_U05, CBZ2A_U07, CBZ2A_K02, CBZ2A_K03

Nazwa modułu zajęć	Forma zajęć dydaktycznych	Sposób weryfikacji i oceny efektów uczenia się osiągniętych przez studenta w ramach poszczególnych form zajęć i dla całego modułu zajęć	Odniesienia do KEU
Deep Learning Algorithms for Cybersecurity Applications	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Wykonanie projektu, Wykonanie ćwiczeń laboratoryjnych, Zaliczenie laboratorium	CBZ2A_W01, CBZ2A_W02, CBZ2A_W04, CBZ2A_W05, CBZ2A_U01, CBZ2A_U02, CBZ2A_U04, CBZ2A_U06, CBZ2A_U03, CBZ2A_K01, CBZ2A_K02, CBZ2A_K03
Szeregi czasowe	Konwersatorium, Ćwiczenia projektowe	Aktywność na zajęciach, Kolokwium, Prezentacja	CBZ2A_W01, CBZ2A_W02, CBZ2A_U06, CBZ2A_K01, CBZ2A_K02
Metodyki projektów z zakresu cyberbezpieczeństwa	Wykład, Ćwiczenia projektowe	Kolokwium, Aktywność na zajęciach, Projekt	CBZ2A_W05, CBZ2A_W04, CBZ2A_U04, CBZ2A_U07, CBZ2A_K03
Metodyka prowadzenia prac B+R	Wykład, Ćwiczenia projektowe	Projekt, Prezentacja	CBZ2A_W01, CBZ2A_W05, CBZ2A_U04, CBZ2A_U06, CBZ2A_U07, CBZ2A_U01, CBZ2A_U03, CBZ2A_K02, CBZ2A_K03, CBZ2A_K01
Bezpieczeństwo w systemach 5G i 6G	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Kolokwium, Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych, Zaangażowanie w pracę zespołu, Zaliczenie laboratorium, Przygotowanie i przeprowadzenie badań, Projekt, Sprawozdanie	CBZ2A_W01, CBZ2A_W02, CBZ2A_W04, CBZ2A_U01, CBZ2A_U02, CBZ2A_U03, CBZ2A_U04, CBZ2A_U06, CBZ2A_K01, CBZ2A_K02, CBZ2A_K03
Bezpieczeństwo treści multimedialnych	Zajęcia seminaryjne, Ćwiczenia projektowe	Aktywność na zajęciach, Kolokwium, Projekt	CBZ2A_W02, CBZ2A_W03, CBZ2A_W04, CBZ2A_U06, CBZ2A_K01
Wyzwania i kierunki rozwoju cyberbezpieczeństwa	Konwersatorium, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Udział w dyskusji, Studium przypadków , Odpowiedź ustna, Zaangażowanie w pracę zespołu	CBZ2A_W02, CBZ2A_W04, CBZ2A_W01, CBZ2A_U01, CBZ2A_U02, CBZ2A_U05, CBZ2A_U06, CBZ2A_K01, CBZ2A_K02, CBZ2A_K03
Psychologiczne aspekty cyberbezpieczeństwa	Konwersatorium, Ćwiczenia projektowe	Aktywność na zajęciach, Udział w dyskusji, Prezentacja, Studium przypadków	CBZ2A_W01, CBZ2A_W04, CBZ2A_U02, CBZ2A_U06, CBZ2A_U07, CBZ2A_U01, CBZ2A_K02
Język angielski B2+ - obowiązkowy kurs języka specjalistycznego na studiach II stopnia dla studentów Wydziału Informatyki, Elektroniki i Telekomunikacji	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Sprawozdanie, Referat, Wynik testu zaliczeniowego, Wypracowania pisane na zajęciach, Prezentacja	CBZ2A_U03
Praca w kole naukowym	Praca w kole naukowym	Projekt, Sprawozdanie, Referat, Zaangażowanie w pracę zespołu, Prezentacja, Udział w pracach badawczych, konferencjach, dodatkowych stażach i szkoleniach, Udział w konkursach i festiwalach nauki i techniki, promocja wydziału, uczelni	CBZ2A_W01, CBZ2A_W02, CBZ2A_W03, CBZ2A_W05, CBZ2A_U01, CBZ2A_U05, CBZ2A_U03, CBZ2A_U07, CBZ2A_K01, CBZ2A_K02

Nazwa modułu zajęć	Forma zajęć dydaktycznych	Sposób weryfikacji i oceny efektów uczenia się osiągniętych przez studenta w ramach poszczególnych form zajęć i dla całego modułu zajęć	Odniesienia do KEU
Purple Teaming	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Wykonanie ćwiczeń, Zaliczenie laboratorium	CBZ2A_W02, CBZ2A_W04, CBZ2A_U01, CBZ2A_U02, CBZ2A_U05, CBZ2A_U06, CBZ2A_U07, CBZ2A_K01, CBZ2A_K02, CBZ2A_K03
Działalność naukowa	Ćwiczenia projektowe	Projekt, Udział w pracach badawczych, konferencjach, dodatkowych stażach i szkoleniach, Przygotowanie i przeprowadzenie badań, Koordynacja, realizacja projektu badawczego, przygotowanie referatu/publikacji, organizacja konferencji, obozów i wycieczek naukowych	CBZ2A_W01, CBZ2A_W04, CBZ2A_U01, CBZ2A_U04, CBZ2A_U06, CBZ2A_U07, CBZ2A_U03, CBZ2A_K01, CBZ2A_K03
Warsztaty dyplomowe	Wykład, Ćwiczenia projektowe	Udział w dyskusji, Prezentacja, Przygotowanie i przeprowadzenie badań	CBZ2A_W01, CBZ2A_W04, CBZ2A_U05, CBZ2A_U06, CBZ2A_U07, CBZ2A_U03, CBZ2A_K01
Cybersecurity Operations	Wykład, Ćwiczenia projektowe	Wykonanie projektu, Projekt, Wynik testu zaliczeniowego	CBZ2A_W02, CBZ2A_W03, CBZ2A_W05, CBZ2A_U01, CBZ2A_U02, CBZ2A_U05, CBZ2A_U07, CBZ2A_K02, CBZ2A_K03
Architektura korporacyjna i zarządzanie ryzykiem	Wykład, Ćwiczenia projektowe	Kolokwium, Koordynacja, realizacja projektu badawczego, przygotowanie referatu/publikacji, organizacja konferencji, obozów i wycieczek naukowych	CBZ2A_W04, CBZ2A_W05, CBZ2A_U01, CBZ2A_U04, CBZ2A_K01, CBZ2A_K02, CBZ2A_K03
Przetwarzanie języka naturalnego metodami AI/ML	Zajęcia seminaryjne, Ćwiczenia projektowe	Aktywność na zajęciach, Kolokwium, Projekt, Prezentacja	CBZ2A_W01, CBZ2A_W03, CBZ2A_U04, CBZ2A_K01
Technologia blockchain	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Aktywność na zajęciach, Kolokwium, Projekt, Prezentacja	CBZ2A_W03, CBZ2A_W04, CBZ2A_W05, CBZ2A_W01, CBZ2A_U05, CBZ2A_U06, CBZ2A_U07, CBZ2A_U01, CBZ2A_U04, CBZ2A_K01, CBZ2A_K02, CBZ2A_K03
Praca dyplomowa	Praca dyplomowa	Praca dyplomowa	CBZ2A_W01, CBZ2A_W04, CBZ2A_U03, CBZ2A_U05, CBZ2A_U04, CBZ2A_U06, CBZ2A_K01, CBZ2A_K02, CBZ2A_K03
Odpowiedzialność prawna za cyberataki i ochronę zasobów	Wykład, Ćwiczenia audytoryjne	Udział w dyskusji, Kolokwium, Aktywność na zajęciach	CBZ2A_W05, CBZ2A_W04, CBZ2A_U07, CBZ2A_K03

ECTS

Kierunek: Cyberbezpieczeństwo

Łączna liczba punktów ECTS, którą student musi uzyskać w ramach:

zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	45
zajęć z zakresu nauk podstawowych właściwych dla danego kierunku studiów	8
zajęć o charakterze praktycznym, kształtujących umiejętności praktyczne, w tym zajęć laboratoryjnych, projektowych, praktycznych i warsztatowych	61
zajęć podlegających wyborowi przez studenta (w wymiarze nie mniejszym niż 30% liczby punktów ECTS koniecznych do uzyskania kwalifikacji odpowiadających poziomowi kształcenia)	48
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	9
zajęć z języka obcego	2
praktyk zawodowych	0
zajęć związanych z prowadzoną w Uczelni działalnością naukową w dyscyplinie lub dyscyplinach, do których przyporządkowany jest kierunek studiów, w wymiarze większym niż 50% liczby punktów ECTS wymaganej do ukończenia studiów na danym poziomie, z uwzględnieniem udziału studentów w zajęciach przygotowujących do prowadzenia działalności naukowej lub udziału w tej działalności (dotyczy tylko studiów o profilu ogólnoakademickim)	54
zajęć kształtujących umiejętności praktyczne w wymiarze większym niż 50% liczby punktów ECTS wymaganej do ukończenia studiów na danym poziomie (dotyczy tylko studiów o profilu praktycznym)	0

Szczegółowe zasady realizacji programu studiów ustalone przez dziekana wydziału (tzw. zasady studiowania)

Kierunek: Cyberbezpieczeństwo

Zasady wpisu na kolejny semestr

Student uzyskuje wpis na kolejny semestr po uzyskaniu zaliczeń ze wszystkich modułów przewidzianych programem studiów.

Zasady wpisu na kolejny semestr studiów w ramach tzw. dopuszczalnego deficytu punktów ECTS

Student zgodnie z Regulaminem Studiów w AGH może uzyskać wpis na kolejny semestr przy deficycie nie większym niż 15 punktów ECTS. Wniosek w tej sprawie należy złożyć do Prodziekana ds. Kształcenia dla kierunku Cyberbezpieczeństwo.

Dopuszczalny deficyt punktów ECTS

15

Organizacja zajęć w ramach tzw. bloków zajęć (tj. taka organizacja przedmiotów lub poszczególnych form zajęć, która zakłada odstępstwa od cykliczności prowadzenia zajęć w poszczególnych tygodniach w danym semestrze studiów)

Program studiów nie przewiduje prowadzenia zajęć w ramach bloków.

Semestry kontrolne

-

Zasady odbywania studiów według indywidualnej organizacji studiów

Sytuacje uprawniające do ubiegania się o indywidualną ogranizację studiów oraz możliwości indywidualizacji określa Regulamin Studiów AGH. Student za zgodą Prodziekana ds. Kształcenia dla kierunku Cyberbezpieczeństwo ma prawo do odbywania studiów według indywidualnej organizacji studiów. Odbywanie takich studiów nie może prowadzić do zmiany w zakresie kierunkowych efektów uczenia się oraz obowiązkowych modułów zajęć. Zasady odbywania takich studiów określa Prodziekan w oparciu o pisemny wniosek studenta. Wniosek powinien określać zakres indywidualizacji i uzasadnienie.

Warunki realizacji praktyk zawodowych, w tym w szczególności system kontroli praktyk i ich zaliczania

Program studiów nie przewiduje odbywania obowiązkowych praktyk zawodowych.

Zasady obieralności modułów zajęć

Kształcenie kierunkowe na drugim i trzecim semestrze studiów bazuje na przedmiotach obieralnych. Przed rozpoczęciem semestru studenci przekazują informacje co do preferowanych przedmiotów kierunkowych. W przypadku limitów miejsc podczas zapisów brane są pod uwagę takie wskaźniki jak: wartość wskaźnika rekrutacyjnego na studia II stopnia czy inne określone przez prowadzących dany przedmiot obieralny.

Zasady obieralności ścieżek kształcenia, ścieżek dyplomowania lub specjalności albo kwalifikacji na nie

Nie ma wyodrębnionych ścieżek kształcenia, ani ścieżek dyplomowania lub specjalności.

Warunki i wymagania związane z przygotowaniem projektów dyplomowych i prac dyplomowych oraz realizacją procesu dyplomowania

Obowiązkowym elementem programu studiów jest wykonanie przez studenta pracy dyplomowej magisterskiej. Warunkiem złożenia pracy dyplomowej jest zaliczenie wszystkich przewidzianych programem studiów przedmiotów oraz pozytywna ocena pracy dyplomowej przez opiekuna i recenzenta.

Proces dyplomowania prowadzony jest zgodnie z Regulaminem Studiów AGH oraz szczegółowymi zasadami przyjętymi na Wydziale Informatyki, Elektroniki i Telekomunikacji. Egzamin dyplomowy obejmuje prezentację i dyskusję nad pracą dyplomową oraz sprawdzenie poziomu wiedzy z zakresu studiów w formie ustnych odpowiedzi.

Zasady ustalania ogólnego wyniku ukończenia studiów

Zasady ustalania ogólnego wyniku ukończenia studiów precyzuje obowiązujący Regulamin Studiów AGH oraz przepisy szczegółowe obowiązujące na Wydziale Informatyki, Elektroniki i Telekomunikacji. Ocena końcowa studiów jest średnią ważoną: średniej ze studiów, oceny z egzaminu dyplomowego oraz oceny z pracy dyplomowej:

60% to średnia ze studiów,
20% to ocena z pracy dyplomowej,
20% ocena z egzaminu dyplomowego.

Inne wymagania związane z realizacją programu studiów wynikające z Regulaminu studiów albo innych przepisów obowiązujących w Uczelni

Nie ma innych wymagań.