Program studiów

Kierunek: Informatyka - Zarządzanie Bezpieczeństwem Informacji

Spis treści

Charakterystyka kierunku

Informacje podstawowe

Nazwa wydziału:	Wydział Informatyki
Nazwa kierunku:	Informatyka - Zarządzanie Bezpieczeństwem Informacji
Poziom:	Studia inżynierskie I stopnia
Profil:	Ogólnoakademicki
Forma:	Stacjonarne
Klasyfikacja ISCED:	0613
Liczba punktów ECTS konieczna do ukończenia studiów na danym poziomie:	210 ECTS
Tytuł zawodowy nadawany absolwentom:	inżynier
Termin rozpoczęcia cyklu:	2026/2027, semestr zimowy
Czas trwania studiów (liczba semestrów):	7

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%	210

Wskazanie związku kierunku studiów ze strategią rozwoju i misją uczelni

Misją AGH jest rozwijanie badań i kształcenie w zakresie nauk technicznych, ścisłych oraz społecznych i humanistycznych, zapewniając tworzenie innowacji technologicznych i społecznych, służących rozwiązywaniu najważniejszych problemów współczesności (za Strategią AGH). Funkcjonowanie społeczeństwa w świecie, w którym informacja jest najcenniejszym zasobem, a zagrożenia jej bezpieczeństwa i wiarygodności wydają się być nieopanowane i dotykają nie tylko osoby fizycznie i firmy, ale także instytucje państwa - należy właśnie do tej kategorii problemów. Nowy kierunek studiów Informatyka – Zarządzanie Bezpieczeństwem Informacji wpisuje się w pełni w tę misję, łącząc kształcenie w dziedzinach nauk technicznych i ścisłych (informatyka, matematyka, fizyka) oraz nauk społecznych (bezpieczeństwo, prawo, zarządzanie, psychologia i socjologia).

Od kilkunastu lat resorty bezpieczeństwa i obronności RP powierzają AGH realizację projektów o charakterze strategicznym dla egzystencji państwa i znaczenia na arenie międzynarodowej. Dobre postrzeganie tego zaangażowania doprowadziło między innymi do ustanowienia AGH jako części sieci DIANA (Defence Innovation Accelerator for the North Atlantic) - polskiego oddziału akceleratora innowacji NATO. Nowy kierunek dołącza do tych działań oferując kształcenie w zakresie ochrony społeczeństwa i struktur Państwa przed zagrożeniami dla bezpieczeństwa informacji w cyberprzestrzeni i poza nią.

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

W ostatnich latach dokonuje się bezprecedensowa rewolucja cywilizacyjna polegająca na migracji przemysłu, usług i rozrywki do cyberprzestrzeni. Przestrzeń ta staje się niestety coraz bardziej niebezpieczna – korzystanie z niej może się dla użytkowników oraz firm wiązać z utratą środków finansowych, cennych i poufnych danych, a nawet tożsamości, zaś dla instytucji państwowych stanowić istotne zagrożenie obronności całego kraju. W cyberprzestrzeni obserwowany jest nie tylko drastyczny wzrost natężenia działań o charakterze przestępczym, lecz również intensyfikacja działań prowadzonych przez agencje wywiadowcze i grupy hakerskie powiązane z rządami

państw, których polityka charakteryzuje się agresywną postawą – godzących w funkcjonowanie państw i organizacji międzynarodowych. Korzystanie z przestrzeni wirtualnej musi wymagać podejmowania podobnych kroków jakie podejmowane są od wieków w świecie realnym, by zapewnić jego bezpieczeństwo – tj. uchwalania i wdrażania odpowiednich regulacji prawnych, standardów i zasad postępowania (oraz ich egzekwowanie). Potrzebę skutecznego nadzoru legislacyjnego nad funkcjonowaniem cyberprzestrzeni dostrzegają rządy większości krajów, a także instytucje międzynarodowe, takie jak Unia Europejska. Odpowiednim regulacjom poddaje się np. operatorów usług i infrastruktury krytycznej. Niezbędne jest szybkie i skuteczne egzekwowanie wprowadzonych regulacji, a także działania prewencyjne – zatem policja musi intensywnie rozwijać oddziały do wykrywania i zwalczania cyberprzestępczości, a specjalistyczne wojska obrony cyberprzestrzeni stają się kolejnym komponentem sił zbrojnych wielu krajów (w Polsce – od 2019 roku). Wzrost zagrożenia przestrzeni wirtualnej w najbliższych latach wydaje się nieunikniony – co wynika z coraz lepszej organizacji grup przestępczych, nasilającymi się konfliktami zbrojnymi tak w Europie jak i w skali globalnej oraz szybkim postępem technicznym, który może być wykorzystany do coraz skuteczniejszego atakowania w cyberprzestrzeni obywateli, firm i państw.

Dynamiczna transformacja technologiczna i skomplikowana sytuacja geopolityczna Polski wprowadzające poważne zagrożenie w obszarze bezpieczeństwa systemów informatycznych dla jednostek prywatnych, przedsiębiorstw oraz całego państwa stawiają pilne i ambitne zadania instytucjom edukacyjnym. Rosnące zapotrzebowanie na wyspecjalizowane usługi, nowoczesne i skuteczne rozwiązania z zakresu bezpieczeństwa sieci komputerowych i systemów informatycznych oraz operacyjnych nie jest bowiem wystarczająco dobrze zaspokajane przez dostępnych obecnie specjalistów w tych obszarach. Zauważalny jest brak centrów kompetencji, inkubatorów technologicznych i centrów szkoleniowych specjalizujących się w dziedzinie szeroko rozumianego bezpieczeństwa systemów informatycznych. Według różnych ocen w Polsce obecnie brakuje ponad 10 tys. specjalistów z zakresu bezpieczeństwa systemów informatycznych i cyberprzestrzeni (w przypadku całej Europy mówi się o liczbie 200-500 tys., a w skali światowej ta luka sięga w przybliżeniu 2,7 mln).

Ochrona systemów informatycznych nie sprowadza się jedynie do typowo inżynierskich zadań jak: tworzenie bezpiecznego oprogramowania, zabezpieczanie istniejących usług sieciowych i wykrywanie zagrożeń bezpieczeństwa systemów informatycznych. Dla skutecznego zapewnienia bezpieczeństwa informacji niezbędne jest posiadanie również rozległych kompetencji społecznych (tzw. miękkich), np. aby móc prowadzić skuteczny audyt zachowań członków organizacji, którzy bardzo często stanowią podstawowy wektor ataków – nieświadomy zagrożeń użytkownik systemu jest jego najsłabszym ogniwem. W społeczeństwie migrującym do cyberprzestrzeni niebagatelną rolę odgrywa edukacja w zakresie dobrych praktyk ochrony informacji prowadzona w profesjonalny ale i przystępny sposób.

Kierunek Informatyka – Zarządzanie Bezpieczeństwem Informacji adresuje zidentyfikowane wyzwania. Da on absolwentom głęboką, techniczną wiedzę informatyczną sprofilowaną na zagadnienia bezpieczeństwa informacji – w tym wykrywania cyberataków i przeciwdziałania im. Wiedza techniczna będzie uzupełniona o:

a) szczegółową wiedzę w zakresie zasad funkcjonowania systemów bezpieczeństwa w cyberprzestrzeni, w tym zagadnień prawnych odnoszących się do obowiązków i praw podmiotów działających w cyberprzestrzeni,

b) szczegółową wiedzę na temat struktur i działania zespołów monitorujących bezpieczeństwo i reagujących na zagrożenia,

c) szczegółową wiedzę w zakresie zagrożeń i wyzwań dla obronności Polski oraz sojuszy i organizacji, których Polska jest członkiem,

d) wiedzę o strategii bezpieczeństwa systemów informatycznych oraz cyberobrony RP,

e) szczegółową wiedzą w zakresie ochrony zasobów, w tym krytycznych oraz polityk i procedur o znaczeniu podstawowym dla obronności Polski i jej sojuszy,

f) podstawową wiedzę na temat prawa własności i ochrony danych osobowych,

g) podstawową wiedzę w zakresie socjologii, psychologii, socjotechniki, metod manipulacji oraz weryfikacji informacji,

h) wiedzę na temat metod organizacji pracy, także badawczej oraz zarządzania zespołami i projektami,

i) wiedzę na temat pozatechnicznych metod pozyskiwania informacji.

Ścieżki kształcenia - zakres w języku polskim oraz w języku angielskim

Brak.

Ścieżki dyplomowania - zakres w języku polskim oraz w języku angielskim

Brak.

Nazwy specjalności w języku polskim oraz w języku angielskim

Nazwa [pl]	Nazwa [en]

Ogólne informacje o programie studiów

Kierunek: Informatyka - Zarządzanie Bezpieczeństwem Informacji

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

Celem kształcenia na kierunku Informatyka – Zarządzanie Bezpieczeństwem Informacji jest dostarczenie studentom wiedzy oraz umiejętności praktycznych i kompetencji społecznych pozwalających im na podjęcie pracy na różnorodnych stanowiskach związanych z ochroną informacji. Ważniejszymi zagadnieniami występującymi w programie studiów są: programowanie w różnych językach programowania, kryptologia, kryptografia postkwantowa, infrastruktura sieciowa, informatyka śledcza, sztuczna inteligencji i jej zastosowania w ochronie systemów informatycznych, testy penetracyjne, analiza oprogramowania malware, infrastruktura ochrony systemów informatycznych i cyberprzestrzeni, zagadnienia prawne cyberbezpieczeństwa, bezpieczeństwo informacji w obszarze obronności, bezpieczeństwo i obronność państwa oraz organizacji i sojuszy, w których uczestniczy Polska, socjotechniki i techniki manipulacji, testy bezpieczeństwa fizycznego, analiza i modelowanie ryzyka w organizacjach i systemach informatycznych, komunikacja i praca w zespole, zarządzanie projektami i zespołem.

Absolwenci kierunku znajdą pracę w różnego rodzaju instytucjach prywatnych i publicznych dbających o bezpieczeństwo posiadanych przez nich informacji, a w szczególności u operatorów usług kluczowych – instytucji świadczących usługi o istotnym znaczeniu dla utrzymania działalności społecznej lub gospodarczej: energetyka, transport, bankowość, ochrona zdrowia, zaopatrzenie w wodę pitną i infrastruktura cyfrowa – zobligowanych prawnie do ciągłego monitorowania cyberzagrożeń i reagowanie na nie. Potencjalnym miejscem zatrudnienia absolwentów mogą być także Wojska Obrony Cyberprzestrzeni (specjalistyczny komponentu Sił Zbrojnych RP powołany do życia w 2022 r.) oraz organy ścigania, w tym Centralne Biuro Zwalczania Cyberprzestępczości.

Absolwenci kierunku chcący kontynuować swoją edukację i zdobywać dodatkową wiedzę domenową będą mogli podjąć studia drugiego stopnia w Akademii Górniczo-Hutniczej lub innych uczelniach wyższych. Interesującym kierunkiem rozwoju zawodowego może być także specjalizacja w obszarze informatyki lub cyberbezpieczeństwa.

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

Podczas tworzenia programu kierunku Informatyka – Zarządzanie Bezpieczeństwem Informacji brano pod uwagę wyniki analiz monitoringu karier zawodowych studentów pokrewnych kierunków. Jakkolwiek zapotrzebowanie na specjalistów z zakresu szeroko rozumianego bezpieczeństwa systemów informatycznych jest ogromne, zarówno pracodawcy jak i niezależne raporty wskazują na istotne deficyty w zakresie kompetencji miękkich kandydatów: komunikacja interpersonalna, umiejętność zarządzania zespołem, podejmowanie decyzji w sytuacjach kryzysowych. O wieloaspektowości problemu zarządzania bezpieczeństwem informacji świadczy także strona internetowa Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni informująca o rekrutacji pracowników w dziesięciu obszarach, m.in.: matematyka i kryptologia, informatyka śledcza i inżynieria wsteczna, cyberbezpieczeństwo, inżynieria oprogramowania, eksploracja i analiza danych (stan: listopad 2024).

Kierunek Informatyka – Zarządzanie Bezpieczeństwem Informacji ma na celu wypełnienie tych luk kompetencyjnych (opisane powyżej). Dodatkowo szerokie podjęcie w tematyce studiów zagadnień obronności Polski i zawartych przez nią sojuszy pozwoli absolwentom znaleźć prestiżowe zatrudnienie w służbach mundurowych.

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

Uwagi i zalecenia z raportów Polskiej Komisji Akredytacyjnej są konsekwentnie uwzględniane przy kształtowaniu programu, w tym planów studiów. Realizacja kształcenia w ramach kierunku Informatyka – Zarządzanie Bezpieczeństwem Informacji podlega regulacjom Uczelnianego Systemu Zapewnienia Jakości Kształcenia. Procedury wdrożonych systemów zapewniania jakości gwarantują stały monitoring sposobu prowadzenia zajęć i poziomu przekazywanych treści. Kluczowym elementem systemów jest udział samych studentów w procesie zapewniania jakości poprzez ich udział w ciałach decyzyjnych, szczegółowe badania ankietowe i obieralność przedmiotów.

Informacja na temat uwzględnienia w programie studiów przykładów dobrych praktyk

Zgodnie z założeniami realizowanej koncepcji kształcenia ciągłemu ulepszaniu podlegają zarówno programy studiów, jak i stosowane metody dydaktyczne. Inspiracją w tym zakresie jest stała współpraca z renomowanymi uniwersytetami oraz coroczne, liczne wyjazdy pracowników w ramach programu Erasmus+. Ciągła poprawa jakości programów i stosowanych metod dydaktycznych jest częścią realizowanych na Wydziale i na Uczelni projektów finansowanych w ramach Programu Operacyjnego Wiedza Edukacja Rozwój (POWER) oraz programu podnoszenia kompetencji dydaktycznych pracowników naukowo-dydaktycznych i dydaktycznych (POWER-WIET). Konsekwencją tych programów było wdrożenie szeregu działań unowocześniających prowadzenie zajęć dydaktycznych, szczególnie w kontekście uczenia aktualnych pokoleń studentów (tzw. Pokolenie Z a także nadchodzące Pokolenie Alfa), np. grywalizacja, webquest czy design thinking, odpowiednio zmodyfikowanych dla potrzeb naszych studentów.

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

Kształcenie na kierunku Informatyka – Zarządzanie Bezpieczeństwem Informacji wymaga niezwykłej uważności na szybko zmieniające się potrzeby przemysłu i biznesu. Program kierunku był konsultowany z wiodącymi na rynku firmami oferującymi produkty i usługi z obszaru cyberbezpieczeństwa takimi jak Apius, Clico, Securing, Motorola. Podczas tworzenia studiów intensywnie współpracowano z inicjatywą Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland oraz Centrum Cyberbezpieczeństwa AGH. W kontekście wykorzystania nowych technik na uwagę zasługuje także współpraca z Fundacją Bezpieczna Cyberprzestrzeń w zakresie wykorzystania w procesie dydaktycznym unikalnej platformy edukacyjnej CyberBastion łączącej grywalizację z modelowaniem i symulacją zagrożeń dla informacji i zasobów informatycznych. Pracownicy podnoszą stale swoje kompetencje dydaktyczne korzystając także z kursów, szkoleń i zasobów Centrum e_Learningu i Innowacyjnej Dydaktyki AGH – CeLID (https://www.cel.agh.edu.pl/).

Wymiar, zasady i forma odbywania praktyk zawodowych

Obowiązkowa praktyka zawodowa na studiach stacjonarnych I stopnia trwa co najmniej cztery tygodnie i jest integralną częścią planu studiów. Odbywa się w czasie letniej przerwy wakacyjnej, po 6 semestrze studiów. Studenci kierunku Informatyka – Zarządzanie Bezpieczeństwem Informacji mogą wybierać miejsca praktyk z bogatej oferty ponieważ są bardzo chętnie przyjmowani na praktyki w kraju i za granicą. Liczba ofert zwykle przewyższa liczbę studentów. Studenci odbywają także praktyki w działach IT/Cybersecurity firm z innych branż, które chętnie oferują im miejsca praktyk (są to np. banki). Studenci realizują praktyki w m.in. w takich firmach jak: Apius, Clico, ABB, ASSECO, AILLERON, AKAMAI, CISCO Polska, Ericpol, Erlang Solutions, Google Poland, IBM Polska, Nokia Solutions and Networks, Sabre, Schibsted, Software Mansion, Ubiquiti, Virtus Labs, CISO4U, 4Prime. Ponadto część studentów wybiera ośrodki akademickie, np. ACK Cyfronet czy laboratoria AGH (np. na Wydziale Informatyki).

Warunki rekrutacji na studia

Kierunek: Informatyka - Zarządzanie Bezpieczeństwem Informacji

Opis kompetencji oczekiwanych od kandydata ubiegającego się o przyjęcie na studia

Kandydat na studia I stopnia na kierunku Informatyka - Zarządzanie Bezpieczeństwem Informacji powinien posiadać kompetencje w zakresie matematyki i fizyki typowe dla absolwenta szkoły średniej, po ukończeniu klasy matematyczno-fizycznej.

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

Zasady i warunki rekrutacji określa stosowna Uchwała Senatu AGH w sprawie warunków, trybu oraz terminu rozpoczęcia i zakończenia rekrutacji na pierwszy rok studiów pierwszego i drugiego stopnia rozpoczynających cykl kształcenia w danym roku akademickim.

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: Informatyka - Zarządzanie Bezpieczeństwem Informacji

Wiedza

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
IZB1A_W01	Ma wiedzę w zakresie algebry w szczególności teorii liczb, teorii grup i teorii ciał, analizy oraz elementów logiki i matematyki dyskretnej. Ma wiedzę w zakresie podstaw statystyki. Ma wiedzę w zakresie fizyki, w szczególności fizyki kwantowej potrzebnej do zrozumienia podstaw informatyki kwantowej i kryptografii kwantowej.	P6S_WG_A
IZB1A_W02	Ma szczegółową wiedzę w zakresie podstaw matematycznych kryptologii oraz konstrukcji systemów kryptograficznych i technik kryptoanalitycznych. Ma wiedzę w zakresie kryptografii kwantowej. Ma wiedzę na temat zagrożeń wobec kryptografii wynikających z rozwoju komputerów kwantowych oraz działań mających na celu przeciwstawienie się tym zagrożeniom.	P6S_WG_A
IZB1A_W03	Ma szczegółową wiedzę w zakresie zasad funkcjonowania systemów zarządzania bezpieczeństwem informacji, w tym zagadnień prawnych odnoszących się do obowiązków i praw podmiotów działających w cyberprzestrzeni. Ma szczegółową wiedzę na temat struktur i działania zespołów monitorujących bezpieczeństwo i reagujących na zagrożenia.	P6S_WK_A, P6S_WG_A
IZB1A_W04	Ma wiedzę w zakresie socjologii, psychologii, socjotechniki, metod manipulacji oraz weryfikacji informacji. Ma szczegółową wiedzę na temat pozatechnicznych metod pozyskiwania informacji.	P6S_WK_A, P6S_WG_A
IZB1A_W05	Ma szczegółową wiedzę w zakresie wybranych języków i technik programowania, włączając w to informatykę kwantową. Ma wiedzę w zakresie projektowania, testowania oraz zapewniania bezpieczeństwa systemów informatycznych. Ma wiedzę na temat metod organizacji pracy w tym zarządzania zespołami i projektami informatycznymi.	P6S_WG_A_Inz, P6S_WG_A
IZB1A_W06	Ma szczegółową wiedzę w zakresie podstaw algorytmiki, struktur danych oraz złożoności obliczeniowej. Ma szczegółową wiedzę w zakresie podstaw teoretycznych budowy wybranych narzędzi i systemów informatycznych.	P6S_WG_A
IZB1A_W07	Ma szczegółową wiedzę w zakresie budowy i zarządzania infrastrukturą systemów informatycznych działających w środowiskach rozproszonych i chmurowych ze szczególnym uwzględnieniem zagadnień bezpieczeństwa.	P6S_WG_A_Inz, P6S_WG_A
IZB1A_W08	Ma szczegółową wiedzę na temat pozyskiwania, przetwarzania i wykorzystywania informacji, w tym także analizy dowodowej oraz analizy danych wywiadowczych o zagrożeniach (threat intelligence).	P6S_WG_A
IZB1A_W09	Ma szczegółową wiedzę na temat metod analizy i oceny jakości systemów informatycznych i infrastruktury z punktu widzenia bezpieczeństwa, w tym metod realizacji audytu technicznego i testów penetracyjnych oraz narzędzi monitorowania i detekcji zagrożeń.	P6S_WK_A_Inz, P6S_WG_A
IZB1A_W10	Ma szczegółową wiedzę w zakresie zagrożeń i wyzwań dla obronności Polski oraz sojuszy i organizacji, których Polska jest członkiem, a także posiada wiedzę o strategii cyberbezpieczeństwa oraz cyberobrony RP.	P6S_WK_A
IZB1A_W11	Ma szczegółową wiedzą w zakresie ochrony zasobów, w tym krytycznych oraz polityk i procedur o znaczeniu podstawowym dla obronności Polski i jej sojuszy.	P6S_WG_A, P6S_WK_A
IZB1A_W12	Ma wiedzę odnośnie bezpieczeństwa informacji jako podstawowej wartości dla obronności RP.	P6S_WG_A, P6S_WK_A
IZB1A_W13	Ma wiedzę o metodach sztucznej inteligencji i uczenia maszynowego oraz wieloaspektowej analizy danych. Ma wiedzę na temat stosowania metod sztucznej inteligencji w zarządzaniu bezpieczeństwem informacji. Ma wiedzę związaną z bezpieczeństwem użytkowania systemów sztucznej inteligencji.	P6S_WG_A
IZB1A_W14	Ma podstawową wiedzę w zakresie ochrony własności intelektualnej i przemysłowej z szczególnym uwzględnieniem ochrony innowacji.	P6S_WG_A, P6S_WK_A

Umiejętności

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
IZB1A_U01	Potrafi pozyskiwać informacje pochodzące z literatury naukowej i fachowej, baz danych oraz innych źródeł. Potrafi weryfikować uzyskane informacje, integrować i dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie.	P6S_UU_A
IZB1A_U02	Posługuje się językiem obcym na poziomie B2 ESOKJ w stopniu wystarczającym do porozumiewania się, a także czytania dokumentacji narzędzi informatycznych oraz podobnych dokumentów, potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego i przygotować tekst zawierający omówienie wyników oraz prezentację poświęconą realizacji zadania.	P6S_UU_A, P6S_UK_A
IZB1A_U03	Potrafi wykorzystywać różne techniki komunikacji, organizacji pracy i zarządzania dla potrzeb realizacji zadań związanych z zarządzaniem bezpieczeństwem informacji.	P6S_UO_A
IZB1A_U04	Potrafi zrealizować studium wykonalności zleconego zadania, w tym przygotować plan testu penetracyjnego lub audytu, a także oszacować czas potrzebny na realizację zleconego zadania oraz opracować i zrealizować harmonogram prac.	P6S_UW_A_Inz_02 , P6S_UO_A
IZB1A_U05	Potrafi analizować zdarzenia zachodzące w systemach organizacji, wskazywać ich krytyczność, przeprowadzać analizę działań podmiotów atakujących organizację, a także przeprowadzić audyt procedur bezpieczeństwa w biznesie lub przemyśle.	P6S_UW_A
IZB1A_U06	Potrafi wykorzystać poznane języki i techniki programowania do tworzenia ergonomicznych, efektywnych i bezpiecznych aplikacji i systemów informatycznych w tym adekwatnie wykorzystywać znane algorytmy i struktury danych.	P6S_UW_A
IZB1A_U07	Potrafi ocenić, dobrać i stosować właściwe metody i narzędzia do realizacji zadań związanych z monitorowaniem i wdrażaniem mechanizmów bezpieczeństwa informacji.	P6S_UW_A_Inz_02 , P6S_UW_A
IZB1A_U08	Potrafi przeprowadzić analizę istniejących systemów informatycznych ze względu na zadane kryteria użytkowe, ekonomiczne i bezpieczeństwa.	P6S_UW_A_Inz_01 , P6S_UW_A
IZB1A_U09	Potrafi przeprowadzić analizę czynników wpływających na cyberbezpieczeństwo i cyberobronę RP, wynikających z systemu zarządzania bezpieczeństwem informacji.	P6S_UW_A, P6S_UW_A_Inz_01
IZB1A_U10	Potrafi zaprojektować podstawowe elementy zarządzania bezpieczeństwem informacji dla systemu cyberbezpieczeństwa i cyberobrony RP.	P6S_UW_A, P6S_UW_A_Inz_02

Kompetencje społeczne

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
IZB1A_K01	Potrafi myśleć i działać w sposób przedsiębiorczy, rozumie potrzebę i zna możliwości podnoszenia kompetencji zawodowych, osobistych i społecznych, potrafi inspirować i organizować proces uczenia siebie oraz innych osób	P6S_KK_A
IZB1A_K02	Ma świadomość znaczenia pozatechnicznych aspektów i skutków działalności inżyniera specjalisty w zakresie bezpieczeństwa systemów informatycznych. Ma świadomość konieczności edukowania społeczeństwa cyfrowego w zakresie zasad funkcjonowania w cyberprzestrzeni i bezpieczeństwa informacji	P6S_KO_A
IZB1A_K03	Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role, szczególnie związane z aspektami bezpieczeństwa, ma świadomość odpowiedzialności za pracę własną i za wspólnie realizowane zadania	P6S_KO_A
IZB1A_K04	Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania oraz adekwatnie zaplanować pracę	P6S_KK_A
IZB1A_K05	Ma świadomość roli społecznej absolwenta uczelni technicznej, rozumie potrzebę formułowania i przekazywania społeczeństwu informacji i opinii dotyczących reguł i standardów bezpieczeństwa w cyberprzestrzeni, wagi profesjonalnego zachowania i przestrzegania zasad etyki zawodowej, prawidłowej identyfikacji i rozstrzygania dylematów związanych z wykonywaniem zawodu inżynieria specjalisty w zakresie bezpieczeństwa systemów informatycznych	P6S_KO_A, P6S_KR_A

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
IZB1A_K06	Ma świadomość wyzwań i zagrożeń dotyczących bezpieczeństwa Polski w cyberprzestrzeni wynikających z sytuacji geopolitycznej oraz przynależności do sojuszy i organizacji międzynarodowych oraz znaczenia roli, jaką w tym obszarze pełnią specjaliści w zakresie bezpieczeństwa informacji	P6S_KR_A, P6S_KO_A

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

Kierunek: Informatyka - Zarządzanie Bezpieczeństwem Informacji

Wiedza

Symbol CEU	Efekty uczenia się dla kwalifikacji obejmujących kompetencje inżynierskie	Odniesienia do KEU
P6S_WG_A_Inz	Absolwent zna i rozumie podstawowe procesy zachodzące w cyklu życia urządzeń, obiektów i systemów technicznych	IZB1A_W05, IZB1A_W07
P6S_WK_A_Inz	Absolwent zna i rozumie podstawowe zasady tworzenia i rozwoju różnych form indywidualnej przedsiębiorczości	IZB1A_W09

Umiejętności

Symbol CEU	Efekty uczenia się dla kwalifikacji obejmujących kompetencje inżynierskie	Odniesienia do KEU
P6S_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	IZB1A_U08, IZB1A_U09
P6S_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	IZB1A_U04, IZB1A_U07, IZB1A_U10

Matryca pokrycia efektów kierunkowych

Kierunek: Informatyka - Zarządzanie Bezpieczeństwem Informacji

2026/2027/S/Ii/WI/ICB/all

Przedmiot	Kod	Semestr	IZB1A_W01	IZB1A_W02	IZB1A_W03	IZB1A_W04	IZB1A_W05	IZB1A_W06	IZB1A_W07	IZB1A_W08	IZB1A_W09	IZB1A_W10	IZB1A_W11	IZB1A_W12	IZB1A_W13	IZB1A_W14	IZB1A_U01	IZB1A_U02	IZB1A_U03	IZB1A_U04	IZB1A_U05	IZB1A_U06	IZB1A_U07	IZB1A_U08	IZB1A_U09	IZB1A_U10	IZB1A_K01	IZB1A_K02	IZB1A_K03	IZB1A_K04	IZB1A_K05	IZB1A_K06
Algebra	WIIZBS.Ii1.00371.26	1s	x																								x			x		
Analiza matematyczna	WIIZBS.Ii1.00773.26	1s	x														x										x		x			
Kompetencje interpersonalne i komunikacja 1	WIIZBS.Ii1.16803.26	1s				x													x								x		x	x	x	
Wstęp do informatyki	WIIZBS.Ii1.01848.26	1s					x	x														x	x				x					
Wprowadzenie do systemu UNIX	WIIZBS.Ii1.02252.26	1s						x	x		x											x	x	x					x		x	
Wprowadzenie do nauk penalnych	WIIZBS.Ii1.16842.26	1s			x					x		x	x						x		x				x				x			x
Wprowadzenie do zarządzania bezpieczeństwem informacji	WIIZBS.Ii1.18387.26	1s		x	x	x			x			x	x	x							x	x			x	x		x			x	x
Język angielski B-2 – kurs obowiązkowy 135 godzin - semestr 1/3	WIIZBS.IiE.05075.26	2s i 3s i 4s																x														
Matematyka dyskretna	WIIZBS.Ii2.00425.26	2s	x	x				x									x	x									x		x	x		

Przedmiot	Kod	Semestr	IZB1A_W01	IZB1A_W02	IZB1A_W03	IZB1A_W04	IZB1A_W05	IZB1A_W06	IZB1A_W07	IZB1A_W08	IZB1A_W09	IZB1A_W10	IZB1A_W11	IZB1A_W12	IZB1A_W13	IZB1A_W14	IZB1A_U01	IZB1A_U02	IZB1A_U03	IZB1A_U04	IZB1A_U05	IZB1A_U06	IZB1A_U07	IZB1A_U08	IZB1A_U09	IZB1A_U10	IZB1A_K01	IZB1A_K02	IZB1A_K03	IZB1A_K04	IZB1A_K05	IZB1A_K06
Język hiszpański B-2 – kurs obowiązkowy 135 godzin - semestr 1/3	WIIZBS.IiE.02182.26	2s i 3s i 4s																x														
Algebra w kryptografii	WIIZBS.Ii2.16805.26	2s	x	x													x													x		
Język rosyjski B-2 – kurs obowiązkowy 135 godzin - semestr 1/3	WIIZBS.IiE.05110.26	2s i 3s i 4s																x														
Język niemiecki B-2 – kurs obowiązkowy 135 godzin - semestr 1/3	WIIZBS.IiE.12064.26	2s i 3s i 4s																x														
Język francuski B-2 – kurs obowiązkowy 135 godzin - semestr 1/3	WIIZBS.IiE.02181.26	2s i 3s i 4s																x														
Logika matematyczna	WIIZBS.Ii2.02255.26	2s	x			x		x									x	x						x			x	x			x	
Fizyka 1	WIIZBS.Ii2.00318.26	2s	x														x															
Kompetencje interpersonalne i komunikacja 2	WIIZBS.Ii2.16806.26	2s				x													x								x		x	x	x	
Sieci komputerowe	WIIZBS.Ii2.00436.26	2s			x				x		x						x		x				x							x		
Języki i narzędzia programowania	WIIZBS.Ii2.15506.26	2s					x	x									x	x				x								x		

Przedmiot	Kod	Semestr	IZB1A_W01	IZB1A_W02	IZB1A_W03	IZB1A_W04	IZB1A_W05	IZB1A_W06	IZB1A_W07	IZB1A_W08	IZB1A_W09	IZB1A_W10	IZB1A_W11	IZB1A_W12	IZB1A_W13	IZB1A_W14	IZB1A_U01	IZB1A_U02	IZB1A_U03	IZB1A_U04	IZB1A_U05	IZB1A_U06	IZB1A_U07	IZB1A_U08	IZB1A_U09	IZB1A_U10	IZB1A_K01	IZB1A_K02	IZB1A_K03	IZB1A_K04	IZB1A_K05	IZB1A_K06
Strategia bezpieczeństwa i cyberbezpieczeństwa w Polsce, UE i NATO	WIIZBS.li2.18107.26	2s			x							x	x	x			x								x							x
Wstęp do zwalczania cyberprzestępczości	WIIZBS.li4.08325.26	3s			x	x						x	x	x			x		x		x	x	x		x	x				x	x	x
Rachunek prawdopodobieństwa i statystyka	WIIZBS.li4.00939.26	3s	x	x				x									x														x	
Metody wywierania wpływu	WIIZBS.li4.16811.26	3s				x											x	x	x								x	x	x		x	
Cyberterroryzm - wyzwania dla obronności państwa	WIIZBS.li4.18114.26	3s								x		x	x				x	x			x				x	x		x	x			x
Projekty naukowo-badawcze i innowacyjne w obszarze obronności	WIIZBS.li4.18115.26	3s			x	x						x	x	x		x	x			x					x		x		x	x		x
Fizyka 2	WIIZBS.li4.00058.26	3s	x														x										x			x		
Ryzyko w zarządzaniu bezpieczeństwem informacji	WIIZBS.li4.18217.26	3s			x	x			x	x	x	x					x					x	x	x	x		x	x	x	x	x	x
Kompetencje społeczne w zmieniającym się społeczeństwie	WIIZBS.li4.16809.26	3s				x											x	x	x					x			x		x	x	x	
Podstawy programowania niskopoziomowego	WIIZBS.li4.18118.26	3s					x	x	x								x						x						x	x		

Przedmiot	Kod	Semestr	IZB1A_W01	IZB1A_W02	IZB1A_W03	IZB1A_W04	IZB1A_W05	IZB1A_W06	IZB1A_W07	IZB1A_W08	IZB1A_W09	IZB1A_W10	IZB1A_W11	IZB1A_W12	IZB1A_W13	IZB1A_W14	IZB1A_U01	IZB1A_U02	IZB1A_U03	IZB1A_U04	IZB1A_U05	IZB1A_U06	IZB1A_U07	IZB1A_U08	IZB1A_U09	IZB1A_U10	IZB1A_K01	IZB1A_K02	IZB1A_K03	IZB1A_K04	IZB1A_K05	IZB1A_K06
Bezpieczeństwo komunikacji multimedialnej	WIIZBS.li4.18129.26	3s							x													x	x	x					x	x		
Administracja systemów komputerowych	WIIZBS.li4.03243.26	3s			x				x										x				x	x								
Kryptografia i podstawy kryptoanalizy	WIIZBS.li4.16810.26	3s	x	x				x									x		x				x	x				x		x		
Prywatność i ochrona danych osobowych	WIIZBS.li4.16555.26	3s			x	x				x			x						x									x				
Teoria kodów	WIIZBS.li8.16575.26	4s	x	x				x	x								x			x		x	x	x				x				
Filozoficzne i etyczne aspekty cyberprzestrzeni	WIIZBS.li8.16813.26	4s				x		x									x											x			x	
Programowanie w języku Rust	WIIZBS.li8.15986.26	4s					x										x	x						x					x	x		
Programowanie w języku C++	WIIZBS.li8.08700.26	4s					x	x									x					x	x						x			
Bezpieczeństwo sieci komputerowych i usług sieciowych	WIIZBS.li8.16814.26	4s							x			x	x										x	x	x				x			x
Programowanie w języku JavaScript	WIIZBS.li8.08656.26	4s					x	x														x							x	x		
Programowanie w języku Python	WIIZBS.li8.01885.26	4s					x	x														x	x	x								
Systemy i technologie wirtualizacji	WIIZBS.li8.03583.26	4s					x	x	x	x	x									x	x	x	x					x	x	x		

Przedmiot	Kod	Semestr	IZB1A_W01	IZB1A_W02	IZB1A_W03	IZB1A_W04	IZB1A_W05	IZB1A_W06	IZB1A_W07	IZB1A_W08	IZB1A_W09	IZB1A_W10	IZB1A_W11	IZB1A_W12	IZB1A_W13	IZB1A_W14	IZB1A_U01	IZB1A_U02	IZB1A_U03	IZB1A_U04	IZB1A_U05	IZB1A_U06	IZB1A_U07	IZB1A_U08	IZB1A_U09	IZB1A_U10	IZB1A_K01	IZB1A_K02	IZB1A_K03	IZB1A_K04	IZB1A_K05	IZB1A_K06
Budowa aplikacji internetowych	WIIZBS.li8.16816.26	4s					x	x	x													x		x								
Bazy danych	WIIZBS.li8.00396.26	4s					x	x	x								x	x					x							x		
Kryptografia kwantowa	WIIZBS.li8.18219.26	4s	x	x													x			x			x			x		x			x	x
Podstawy testów penetracyjnych	WIIZBS.li8.16815.26	4s			x					x	x								x	x	x	x	x	x			x		x	x		
Kryptografia postkwantowa	WIIZBS.li10.15725.26	5s	x	x	x			x				x					x		x				x	x	x			x				
Warsztat kompetencji akademickich i naukowych	WIIZBS.li10.16817.26	5s				x										x	x	x	x								x		x	x		
Informatyka kwantowa	WIIZBS.li10.18220.26	5s	x	x			x															x						x				
Zaawansowane testy penetracyjne	WIIZBS.li10.16822.26	5s			x		x	x	x	x	x		x							x		x	x	x			x			x		
Dezinformacja i weryfikacja wiadomości	WIIZBS.li10.16823.26	5s				x						x	x	x			x		x		x				x			x			x	x
Socjotechnika	WIIZBS.li10.05502.26	5s				x				x	x	x	x	x									x	x	x			x	x			x
Prywatność w sieci Internet	WIIZBS.li10.18106.26	5s		x					x		x													x					x	x		
Podstawy bezpieczeństwa oprogramowania	WIIZBS.li10.16818.26	5s					x	x			x												x	x				x	x		x	
Inżynieria wymagań i jakości	WIIZBS.li10.08696.26	5s					x															x		x			x		x			

Przedmiot	Kod	Semestr	IZB1A_W01	IZB1A_W02	IZB1A_W03	IZB1A_W04	IZB1A_W05	IZB1A_W06	IZB1A_W07	IZB1A_W08	IZB1A_W09	IZB1A_W10	IZB1A_W11	IZB1A_W12	IZB1A_W13	IZB1A_W14	IZB1A_U01	IZB1A_U02	IZB1A_U03	IZB1A_U04	IZB1A_U05	IZB1A_U06	IZB1A_U07	IZB1A_U08	IZB1A_U09	IZB1A_U10	IZB1A_K01	IZB1A_K02	IZB1A_K03	IZB1A_K04	IZB1A_K05	IZB1A_K06
Technologie mobilne w obszarze bezpieczeństwa i obronności	WIIZBS.li10.18116.26	5s							x			x	x				x	x					x					x		x	
Podstawy sztucznej inteligencji	WIIZBS.li10.00647.26	5s						x							x		x											x				
UNIX Administration	WIIZBS.li10.04803.26	5s					x	x	x													x		x					x			
Evolutionary Algorithms	WIIZBS.li10.05817.26	5s					x	x									x	x											x	x	x	
Bezpieczeństwo informacji	WIIZBS.li10.07209.26	5s			x							x	x	x			x		x		x				x	x			x		x	x
Metody i narzędzia detekcji incydentów	WIIZBS.li10.16819.26	5s			x				x	x	x										x	x	x	x				x	x	x	x	
Wykorzystanie SI w wykrywaniu zagrożeń	WIIZBS.li20.16828.26	6s						x		x		x		x	x							x	x				x					
Ochrona własności intelektualnej	WIIZBS.li20.00147.26	6s				x						x	x	x		x	x								x	x		x			x	x
Technologie internetu rzeczy	WIIZBS.li20.02844.26	6s					x	x												x		x									x	
Pracownia projektowa 1	WIIZBS.li20.02797.26	6s					x													x		x	x				x		x			
Bezpieczeństwo fizyczne obiektów użyteczności publicznej	WIIZBS.li20.16830.26	6s			x						x	x	x	x			x		x	x	x	x	x		x	x	x	x	x	x	x	x
Modelowanie zagrożeń	WIIZBS.li20.18112.26	6s			x	x	x		x	x	x	x	x	x						x	x	x	x	x	x		x	x		x	x	x

Przedmiot	Kod	Semestr	IZB1A_W01	IZB1A_W02	IZB1A_W03	IZB1A_W04	IZB1A_W05	IZB1A_W06	IZB1A_W07	IZB1A_W08	IZB1A_W09	IZB1A_W10	IZB1A_W11	IZB1A_W12	IZB1A_W13	IZB1A_W14	IZB1A_U01	IZB1A_U02	IZB1A_U03	IZB1A_U04	IZB1A_U05	IZB1A_U06	IZB1A_U07	IZB1A_U08	IZB1A_U09	IZB1A_U10	IZB1A_K01	IZB1A_K02	IZB1A_K03	IZB1A_K04	IZB1A_K05	IZB1A_K06
Zarządzanie incydentami SOC i CERT	WIIZBS.li20.16832.26	6s			x				x	x	x	x	x									x	x								x	x
Zarządzanie projektami informatycznymi	WIIZBS.li20.06841.26	6s			x	x										x		x	x			x							x			
Wywiad przemysłowy	WIIZBS.li20.16833.26	6s			x	x				x	x	x	x	x			x		x			x		x	x		x	x	x		x	x
Praktyka zawodowa	WIIZBS.li20.00035.26	6s															x		x	x											x	
Analiza malware	WIIZBS.li20.08350.26	6s					x				x										x		x								x	
Systemy informatyczne do przetwarzania informacji niejawnych	WIIZBS.li20.18109.26	6s		x	x		x	x	x		x	x	x	x			x		x	x		x	x	x		x	x	x	x	x		x
Architektura i bezpieczeństwo Infrastruktury Data Center	WIIZBS.li20.18108.26	6s			x	x			x		x	x	x								x	x	x		x	x		x	x	x	x	x
Informatyka śledcza i analiza powłamaniowa	WIIZBS.li20.16820.26	6s		x					x	x		x	x	x							x				x						x	x
Biały wywiad	WIIZBS.li20.16835.26	6s			x	x				x		x		x			x		x				x		x			x	x	x	x	x
Projektowanie i budowa systemów zarządzania bezpieczeństwem informacji w organizacji	WIIZBS.li20.18389.26	6s			x				x		x		x	x			x	x	x		x		x	x	x	x	x	x	x	x	x	x
Wprowadzenie do technologii Blockchain	WIIZBS.li40.16826.26	7s		x			x	x	x											x		x	x	x			x	x	x		x	

Przedmiot	Kod	Semestr	IZB1A_W01	IZB1A_W02	IZB1A_W03	IZB1A_W04	IZB1A_W05	IZB1A_W06	IZB1A_W07	IZB1A_W08	IZB1A_W09	IZB1A_W10	IZB1A_W11	IZB1A_W12	IZB1A_W13	IZB1A_W14	IZB1A_U01	IZB1A_U02	IZB1A_U03	IZB1A_U04	IZB1A_U05	IZB1A_U06	IZB1A_U07	IZB1A_U08	IZB1A_U09	IZB1A_U10	IZB1A_K01	IZB1A_K02	IZB1A_K03	IZB1A_K04	IZB1A_K05	IZB1A_K06
Zagrożenia dla płatności elektronicznych	WIIZBS.Ii40.15890.26	7s				x				x	x	x		x			x					x	x	x	x			x	x		x	x
Architektura rozwiązań chmurowych	WIIZBS.Ii40.08761.26	7s					x	x	x		x											x	x	x				x	x			
Pracownia projektowa 2	WIIZBS.Ii40.02800.26	7s					x		x									x		x		x	x	x					x	x		
Kryptografia wizualna i steganografia	WIIZBS.Ii40.16837.26	7s		x	x	x											x		x	x									x		x	
Bezpieczeństwo infrastruktury krytycznej	WIIZBS.Ii40.16838.26	7s			x				x			x	x	x			x				x	x		x	x	x			x	x		x
Analiza informacji	WIIZBS.Ii40.16839.26	7s				x				x							x		x								x	x			x	
Projekt dyplomowy	WIIZBS.Ii40.00034.26	7s															x	x		x							x		x			
Analiza danych	WIIZBS.Ii40.06355.26	7s				x		x		x					x		x	x			x						x		x	x		
Eksploracja danych	WIIZBS.Ii40.00481.26	7s									x				x							x	x	x			x		x	x		
Bezpieczeństwo systemów sztucznej inteligencji	WIIZBS.Ii40.18211.26	7s					x		x		x			x	x	x						x	x	x	x	x	x		x	x	x	
Bezpieczeństwo urządzeń mobilnych	WIIZBS.Ii40.16825.26	7s							x													x						x			x	
Suma (obowiązkowy):			9	7	12	11	6	11	11	6	7	8	9	7	1	3	22	10	15	5	7	9	14	12	9	4	14	11	20	18	16	9
Suma (fakultatywny):			4	7	13	13	19	17	18	12	15	17	14	12	4	2	22	11	9	11	10	28	25	20	14	8	15	20	27	18	20	15
Suma:			13	14	25	24	25	28	29	18	22	25	23	19	5	5	44	21	24	16	17	37	39	32	23	12	29	31	47	36	36	24

Matryca charakterystyk efektów uczenia się w odniesieniu do modułów zajęć

Kierunek: Informatyka - Zarządzanie Bezpieczeństwem Informacji

2026/2027/S/Ii/WI/ICB/all

Przedmiot	Kod	Semestr	P6S_WG_A	P6S_WK_A	P6S_WG_A_Inz	P6S_WK_A_Inz	P6S_UU_A	P6S_UK_A	P6S_UO_A	P6S_UW_A_Inz_02	P6S_UW_A	P6S_UW_A_Inz_01	P6S_KK_A	P6S_KO_A	P6S_KR_A
Algebra	WIIZBS.Ii1.00371.26	1s	x										x		
Analiza matematyczna	WIIZBS.Ii1.00773.26	1s	x				x						x	x	
Kompetencje interpersonalne i komunikacja 1	WIIZBS.Ii1.16803.26	1s	x	x					x				x	x	x
Wstęp do informatyki	WIIZBS.Ii1.01848.26	1s	x		x					x	x		x		
Wprowadzenie do systemu UNIX	WIIZBS.Ii1.02252.26	1s	x		x	x				x	x	x		x	x
Wprowadzenie do nauk penalnych	WIIZBS.Ii1.16842.26	1s	x	x					x		x	x		x	x
Wprowadzenie do zarządzania bezpieczeństwem informacji	WIIZBS.Ii1.18387.26	1s	x	x	x					x	x	x		x	x
Język angielski B-2 – kurs obowiązkowy 135 godzin - semestr 1/3	WIIZBS.IiE.05075.26	2s i 3s i 4s					x	x							
Matematyka dyskretna	WIIZBS.Ii2.00425.26	2s	x				x	x					x	x	
Język hiszpański B-2 – kurs obowiązkowy 135 godzin - semestr 1/3	WIIZBS.IiE.02182.26	2s i 3s i 4s					x	x							
Algebra w kryptografii	WIIZBS.Ii2.16805.26	2s	x				x						x		
Język rosyjski B-2 – kurs obowiązkowy 135 godzin - semestr 1/3	WIIZBS.IiE.05110.26	2s i 3s i 4s					x	x							
Język niemiecki B-2 – kurs obowiązkowy 135 godzin - semestr 1/3	WIIZBS.IiE.12064.26	2s i 3s i 4s					x	x							
Język francuski B-2 – kurs obowiązkowy 135 godzin - semestr 1/3	WIIZBS.IiE.02181.26	2s i 3s i 4s					x	x							
Logika matematyczna	WIIZBS.Ii2.02255.26	2s	x	x			x	x			x	x	x	x	x

Przedmiot	Kod	Semestr	P6S_WG_A	P6S_WK_A	P6S_WG_A_Inz	P6S_WK_A_Inz	P6S_UU_A	P6S_UK_A	P6S_UO_A	P6S_UW_A_Inz_02	P6S_UW_A	P6S_UW_A_Inz_01	P6S_KK_A	P6S_KO_A	P6S_KR_A
Fizyka 1	WIIZBS.Ii2.00318.26	2s	x				x								
Kompetencje interpersonalne i komunikacja 2	WIIZBS.Ii2.16806.26	2s	x	x					x				x	x	x
Sieci komputerowe	WIIZBS.Ii2.00436.26	2s	x	x	x	x	x		x	x	x		x		
Języki i narzędzia programowania	WIIZBS.Ii2.15506.26	2s	x		x		x	x			x		x		
Strategia bezpieczeństwa i cyberbezpieczeństwa w Polsce, UE i NATO	WIIZBS.Ii2.18107.26	2s	x	x			x				x	x		x	x
Wstęp do zwalczania cyberprzestępczości	WIIZBS.Ii4.08325.26	3s	x	x			x		x	x	x	x	x	x	x
Rachunek prawdopodobieństwa i statystyka	WIIZBS.Ii4.00939.26	3s	x				x							x	x
Metody wywierania wpływu	WIIZBS.Ii4.16811.26	3s	x	x			x	x	x				x	x	x
Cyberterroryzm - wyzwania dla obronności państwa	WIIZBS.Ii4.18114.26	3s	x	x			x	x		x	x	x		x	x
Projekty naukowo-badawcze i innowacyjne w obszarze obronności	WIIZBS.Ii4.18115.26	3s	x	x			x		x	x	x	x	x	x	x
Fizyka 2	WIIZBS.Ii4.00058.26	3s	x				x						x		
Ryzyko w zarządzaniu bezpieczeństwem informacji	WIIZBS.Ii4.18217.26	3s	x	x	x	x	x			x	x	x	x	x	x
Kompetencje społeczne w zmieniającym się społeczeństwie	WIIZBS.Ii4.16809.26	3s	x	x			x	x	x		x	x	x	x	x
Podstawy programowania niskopoziomowego	WIIZBS.Ii4.18118.26	3s	x		x		x			x	x		x	x	
Bezpieczeństwo komunikacji multimedialnej	WIIZBS.Ii4.18129.26	3s	x		x					x	x	x	x	x	
Administracja systemów komputerowych	WIIZBS.Ii4.03243.26	3s	x	x	x				x	x	x	x			
Kryptografia i podstawy kryptoanalizy	WIIZBS.Ii4.16810.26	3s	x				x		x	x	x	x	x	x	
Prywatność i ochrona danych osobowych	WIIZBS.Ii4.16555.26	3s	x	x					x					x	
Teoria kodów	WIIZBS.Ii8.16575.26	4s	x		x		x		x	x	x	x		x	

Przedmiot	Kod	Semestr	P6S_WG_A	P6S_WK_A	P6S_WG_A_Inz	P6S_WK_A_Inz	P6S_UU_A	P6S_UK_A	P6S_UO_A	P6S_UW_A_Inz_02	P6S_UW_A	P6S_UW_A_Inz_01	P6S_KK_A	P6S_KO_A	P6S_KR_A
Filozoficzne i etyczne aspekty cyberprzestrzeni	WIIZBS.li8.16813.26	4s	x	x			x							x	x
Programowanie w języku Rust	WIIZBS.li8.15986.26	4s	x		x		x	x			x	x	x	x	
Programowanie w języku C++	WIIZBS.li8.08700.26	4s	x		x		x			x	x			x	
Bezpieczeństwo sieci komputerowych i usług sieciowych	WIIZBS.li8.16814.26	4s	x	x	x					x	x	x		x	x
Programowanie w języku JavaScript	WIIZBS.li8.08656.26	4s	x		x						x		x	x	
Programowanie w języku Python	WIIZBS.li8.01885.26	4s	x		x					x	x	x			
Systemy i technologie wirtualizacji	WIIZBS.li8.03583.26	4s	x		x	x			x	x	x		x	x	
Budowa aplikacji internetowych	WIIZBS.li8.16816.26	4s	x		x						x	x			
Bazy danych	WIIZBS.li8.00396.26	4s	x		x		x	x		x	x		x		
Kryptografia kwantowa	WIIZBS.li8.18219.26	4s	x				x		x	x	x			x	x
Podstawy testów penetracyjnych	WIIZBS.li8.16815.26	4s	x	x		x			x	x	x	x	x	x	
Kryptografia postkwantowa	WIIZBS.li10.15725.26	5s	x	x			x		x	x	x	x		x	
Warsztat kompetencji akademickich i naukowych	WIIZBS.li10.16817.26	5s	x	x			x	x	x				x	x	
Informatyka kwantowa	WIIZBS.li10.18220.26	5s	x		x						x			x	
Zaawansowane testy penetracyjne	WIIZBS.li10.16822.26	5s	x	x	x	x			x	x	x	x	x		
Dezinformacja i weryfikacja wiadomości	WIIZBS.li10.16823.26	5s	x	x			x		x		x	x		x	x
Socjotechnika	WIIZBS.li10.05502.26	5s	x	x		x				x	x	x		x	x
Prywatność w sieci Internet	WIIZBS.li10.18106.26	5s	x		x	x					x	x	x	x	
Podstawy bezpieczeństwa oprogramowania	WIIZBS.li10.16818.26	5s	x		x	x				x	x	x		x	x

Przedmiot	Kod	Semestr	P6S_WG_A	P6S_WK_A	P6S_WG_A_Inz	P6S_WK_A_Inz	P6S_UU_A	P6S_UK_A	P6S_UO_A	P6S_UW_A_Inz_02	P6S_UW_A	P6S_UW_A_Inz_01	P6S_KK_A	P6S_KO_A	P6S_KR_A
Inżynieria wymagań i jakości	WIIZBS.li10.08696.26	5s	x		x						x	x	x	x	
Technologie mobilne w obszarze bezpieczeństwa i obronności	WIIZBS.li10.18116.26	5s	x	x	x		x	x		x	x			x	x
Podstawy sztucznej inteligencji	WIIZBS.li10.00647.26	5s	x				x							x	
UNIX Administration	WIIZBS.li10.04803.26	5s	x		x						x	x		x	
Evolutionary Algorithms	WIIZBS.li10.05817.26	5s	x		x		x	x					x	x	x
Bezpieczeństwo informacji	WIIZBS.li10.07209.26	5s	x	x			x		x	x	x	x		x	x
Metody i narzędzia detekcji incydentów	WIIZBS.li10.16819.26	5s	x	x	x	x				x	x	x	x	x	x
Wykorzystanie SI w wykrywaniu zagrożeń	WIIZBS.li20.16828.26	6s	x	x						x	x		x		
Ochrona własności intelektualnej	WIIZBS.li20.00147.26	6s	x	x			x			x	x	x		x	x
Technologie internetu rzeczy	WIIZBS.li20.02844.26	6s	x		x				x	x	x			x	x
Pracownia projektowa 1	WIIZBS.li20.02797.26	6s	x		x				x	x	x		x	x	
Bezpieczeństwo fizyczne obiektów użyteczności publicznej	WIIZBS.li20.16830.26	6s	x	x		x	x		x	x	x	x	x	x	x
Modelowanie zagrożeń	WIIZBS.li20.18112.26	6s	x	x	x	x			x	x	x	x	x	x	x
Zarządzanie incydentami SOC i CERT	WIIZBS.li20.16832.26	6s	x	x	x	x				x	x			x	x
Zarządzanie projektami informatycznymi	WIIZBS.li20.06841.26	6s	x	x			x	x	x		x			x	
Wywiad przemysłowy	WIIZBS.li20.16833.26	6s	x	x		x	x		x		x	x	x	x	x
Praktyka zawodowa	WIIZBS.li20.00035.26	6s					x		x	x				x	x
Analiza malware	WIIZBS.li20.08350.26	6s	x		x	x				x	x			x	x
Systemy informatyczne do przetwarzania informacji niejawnych	WIIZBS.li20.18109.26	6s	x	x	x	x	x		x	x	x	x	x	x	x

Przedmiot	Kod	Semestr	P6S_WG_A	P6S_WK_A	P6S_WG_A_Inz	P6S_WK_A_Inz	P6S_UU_A	P6S_UK_A	P6S_UO_A	P6S_UW_A_Inz_02	P6S_UW_A	P6S_UW_A_Inz_01	P6S_KK_A	P6S_KO_A	P6S_KR_A
Architektura i bezpieczeństwo Infrastruktury Data Center	WIIZBS.li20.18108.26	6s	x	x	x	x				x	x	x	x	x	x
Informatyka śledcza i analiza powłamaniowa	WIIZBS.li20.16820.26	6s	x	x	x						x	x		x	x
Biały wywiad	WIIZBS.li20.16835.26	6s	x	x			x		x	x	x	x	x	x	x
Projektowanie i budowa systemów zarządzania bezpieczeństwem informacji w organizacji	WIIZBS.li20.18389.26	6s	x	x	x	x	x	x	x	x	x	x	x	x	x
Wprowadzenie do technologii Blockchain	WIIZBS.li40.16826.26	7s	x		x				x	x	x	x	x	x	x
Zagrożenia dla płatności elektronicznych	WIIZBS.li40.15890.26	7s	x	x		x	x			x	x	x		x	x
Architektura rozwiązań chmurowych	WIIZBS.li40.08761.26	7s	x		x	x				x	x	x		x	
Pracownia projektowa 2	WIIZBS.li40.02800.26	7s	x		x		x	x	x	x	x	x	x	x	
Kryptografia wizualna i steganografia	WIIZBS.li40.16837.26	7s	x	x			x		x	x				x	x
Bezpieczeństwo infrastruktury krytycznej	WIIZBS.li40.16838.26	7s	x	x	x		x			x	x	x	x	x	x
Analiza informacji	WIIZBS.li40.16839.26	7s	x	x			x		x				x	x	x
Projekt dyplomowy	WIIZBS.li40.00034.26	7s					x	x	x	x			x	x	
Analiza danych	WIIZBS.li40.06355.26	7s	x	x			x	x			x		x	x	
Eksploracja danych	WIIZBS.li40.00481.26	7s	x			x				x	x	x	x	x	
Bezpieczeństwo systemów sztucznej inteligencji	WIIZBS.li40.18211.26	7s	x	x	x	x				x	x	x	x	x	x
Bezpieczeństwo urządzeń mobilnych	WIIZBS.li40.16825.26	7s	x		x						x			x	x
Suma (obowiązkowy):			38	21	15	7	24	10	18	19	25	19	23	31	19
Suma (fakultatywny):			43	23	27	15	27	11	17	30	39	26	24	39	25
Suma:			81	44	42	22	51	21	35	49	64	45	47	70	44

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

Kierunek: Informatyka - Zarządzanie Bezpieczeństwem Informacji

2026/2027/S/Ii/WI/ICB/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
Algebra	Wykład, Ćwiczenia audytoryjne	Egzamin, Odpowiedź ustna, Kolokwium	IZB1A_W01, IZB1A_K01, IZB1A_K04
Analiza matematyczna	Wykład, Ćwiczenia audytoryjne	Egzamin, Aktywność na zajęciach, Kolokwium	IZB1A_W01, IZB1A_U01, IZB1A_K01, IZB1A_K03
Kompetencje interpersonalne i komunikacja 1	Ćwiczenia audytoryjne	Aktywność na zajęciach, Wykonanie ćwiczeń, Zaangażowanie w pracę zespołu, Prezentacja	IZB1A_W04, IZB1A_U03, IZB1A_K01, IZB1A_K03, IZB1A_K04, IZB1A_K05
Wstęp do informatyki	Wykład, Ćwiczenia audytoryjne	Aktywność na zajęciach, Udział w dyskusji, Kolokwium, Egzamin, Wykonanie ćwiczeń, Odpowiedź ustna	IZB1A_W05, IZB1A_W06, IZB1A_U06, IZB1A_U07, IZB1A_K01
Wprowadzenie do systemu UNIX	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Aktywność na zajęciach	IZB1A_W07, IZB1A_W09, IZB1A_W06, IZB1A_U07, IZB1A_U06, IZB1A_U08, IZB1A_K03, IZB1A_K05
Wprowadzenie do nauk penalnych	Wykład	Wynik testu zaliczeniowego	IZB1A_W03, IZB1A_W08, IZB1A_W10, IZB1A_W11, IZB1A_U03, IZB1A_U09, IZB1A_U05, IZB1A_K03, IZB1A_K06
Wprowadzenie do zarządzania bezpieczeństwem informacji	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W03, IZB1A_W04, IZB1A_W11, IZB1A_W10, IZB1A_W12, IZB1A_W02, IZB1A_W07, IZB1A_U05, IZB1A_U06, IZB1A_U09, IZB1A_U10, IZB1A_K02, IZB1A_K05, IZB1A_K06
Język angielski B-2 – kurs obowiązkowy 135 godzin - semestr 1/3	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wynik testu zaliczeniowego, Wypracowania pisane na zajęciach, Prezentacja	IZB1A_U02
Matematyka dyskretna	Wykład, Ćwiczenia audytoryjne	Aktywność na zajęciach, Udział w dyskusji, Kolokwium	IZB1A_W01, IZB1A_W02, IZB1A_W06, IZB1A_U01, IZB1A_U02, IZB1A_K01, IZB1A_K03, IZB1A_K04

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
Język hiszpański B-2 – kurs obowiązkowy 135 godzin - semestr 1/3	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wynik testu zaliczeniowego, Wypracowania pisane na zajęciach, Prezentacja	IZB1A_U02
Algebra w kryptografii	Wykład, Ćwiczenia audytoryjne	Egzamin, Kolokwium, Prezentacja	IZB1A_W01, IZB1A_W02, IZB1A_U01, IZB1A_K04
Język rosyjski B-2 – kurs obowiązkowy 135 godzin - semestr 1/3	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wynik testu zaliczeniowego, Wypracowania pisane na zajęciach, Prezentacja	IZB1A_U02
Język niemiecki B-2 – kurs obowiązkowy 135 godzin - semestr 1/3	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wynik testu zaliczeniowego, Wypracowania pisane na zajęciach, Prezentacja	IZB1A_U02
Język francuski B-2 – kurs obowiązkowy 135 godzin - semestr 1/3	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wynik testu zaliczeniowego, Wypracowania pisane na zajęciach, Prezentacja	IZB1A_U02
Logika matematyczna	Wykład, Ćwiczenia audytoryjne	Aktywność na zajęciach, Udział w dyskusji, Kolokwium, Wynik testu zaliczeniowego	IZB1A_W01, IZB1A_W06, IZB1A_W04, IZB1A_U01, IZB1A_U02, IZB1A_U08, IZB1A_K01, IZB1A_K02, IZB1A_K05
Fizyka 1	Wykład, Ćwiczenia audytoryjne	Egzamin, Kolokwium	IZB1A_W01, IZB1A_U01
Kompetencje interpersonalne i komunikacja 2	Ćwiczenia audytoryjne	Aktywność na zajęciach, Wykonanie ćwiczeń, Zaangażowanie w pracę zespołu, Prezentacja	IZB1A_W04, IZB1A_U03, IZB1A_K01, IZB1A_K03, IZB1A_K04, IZB1A_K05
Sieci komputerowe	Wykład, Ćwiczenia laboratoryjne	Egzamin, Wykonanie ćwiczeń laboratoryjnych, Kolokwium	IZB1A_W07, IZB1A_W03, IZB1A_W09, IZB1A_U01, IZB1A_U07, IZB1A_U03, IZB1A_K04
Języki i narzędzia programowania	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Egzamin, Wykonanie ćwiczeń laboratoryjnych, Kolokwium	IZB1A_W05, IZB1A_W06, IZB1A_U06, IZB1A_U01, IZB1A_U02, IZB1A_K04
Strategia bezpieczeństwa i cyberbezpieczeństwa w Polsce, UE i NATO	Wykład, Ćwiczenia audytoryjne	Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W03, IZB1A_W10, IZB1A_W11, IZB1A_W12, IZB1A_U01, IZB1A_U09, IZB1A_K06

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
Wstęp do zwalczania cyberprzestępczości	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Prezentacja	IZB1A_W03, IZB1A_W04, IZB1A_W10, IZB1A_W11, IZB1A_W12, IZB1A_U01, IZB1A_U05, IZB1A_U09, IZB1A_U03, IZB1A_U06, IZB1A_U07, IZB1A_U10, IZB1A_K04, IZB1A_K05, IZB1A_K06
Rachunek prawdopodobieństwa i statystyka	Wykład, Ćwiczenia audytoryjne	Egzamin, Wykonanie ćwiczeń, Kolokwium	IZB1A_W01, IZB1A_W02, IZB1A_W06, IZB1A_U01, IZB1A_K05
Metody wywierania wpływu	Wykład, Ćwiczenia audytoryjne	Kolokwium, Aktywność na zajęciach, Prezentacja	IZB1A_W04, IZB1A_U01, IZB1A_U02, IZB1A_U03, IZB1A_K01, IZB1A_K02, IZB1A_K03, IZB1A_K05
Cyberterroryzm - wyzwania dla obronności państwa	Wykład, Ćwiczenia projektowe	Aktywność na zajęciach, Wykonanie projektu	IZB1A_W08, IZB1A_W10, IZB1A_W11, IZB1A_U01, IZB1A_U02, IZB1A_U05, IZB1A_U09, IZB1A_U10, IZB1A_K02, IZB1A_K03, IZB1A_K06
Projekty naukowo-badawcze i innowacyjne w obszarze obronności	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W03, IZB1A_W04, IZB1A_W10, IZB1A_W11, IZB1A_W12, IZB1A_W14, IZB1A_U01, IZB1A_U04, IZB1A_U09, IZB1A_K01, IZB1A_K03, IZB1A_K04, IZB1A_K06
Fizyka 2	Wykład, Ćwiczenia audytoryjne, Ćwiczenia laboratoryjne	Egzamin, Wykonanie ćwiczeń laboratoryjnych, Sprawozdanie	IZB1A_W01, IZB1A_U01, IZB1A_K01, IZB1A_K04
Ryzyko w zarządzaniu bezpieczeństwem informacji	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Udział w dyskusji, Wykonanie projektu, Kolokwium	IZB1A_W08, IZB1A_W09, IZB1A_W10, IZB1A_W07, IZB1A_W03, IZB1A_W04, IZB1A_U07, IZB1A_U08, IZB1A_U01, IZB1A_U06, IZB1A_U09, IZB1A_K03, IZB1A_K04, IZB1A_K06, IZB1A_K01, IZB1A_K02, IZB1A_K05
Kompetencje społeczne w zmieniającym się społeczeństwie	Ćwiczenia audytoryjne	Aktywność na zajęciach, Projekt, Prezentacja	IZB1A_W04, IZB1A_U01, IZB1A_U02, IZB1A_U03, IZB1A_U08, IZB1A_K01, IZB1A_K03, IZB1A_K04, IZB1A_K05
Podstawy programowania niskopoziomowego	Wykład, Ćwiczenia laboratoryjne	Zaliczenie laboratorium, Udział w dyskusji	IZB1A_W05, IZB1A_W06, IZB1A_W07, IZB1A_U01, IZB1A_U07, IZB1A_K03, IZB1A_K04
Bezpieczeństwo komunikacji multimedialnej	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń laboratoryjnych, Zaangażowanie w pracę zespołu	IZB1A_W07, IZB1A_U06, IZB1A_U07, IZB1A_U08, IZB1A_K03, IZB1A_K04
Administracja systemów komputerowych	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Wykonanie ćwiczeń	IZB1A_W07, IZB1A_W03, IZB1A_U08, IZB1A_U03, IZB1A_U07
Kryptografia i podstawy kryptoanalizy	Wykład, Ćwiczenia laboratoryjne	Egzamin, Wykonanie ćwiczeń, Wykonanie projektu, Kolokwium	IZB1A_W01, IZB1A_W02, IZB1A_W06, IZB1A_U01, IZB1A_U03, IZB1A_U07, IZB1A_U08, IZB1A_K02, IZB1A_K04

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
Prywatność i ochrona danych osobowych	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W03, IZB1A_W04, IZB1A_W08, IZB1A_W11, IZB1A_U03, IZB1A_K02
Teoria kodów	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W01, IZB1A_W06, IZB1A_W07, IZB1A_W02, IZB1A_U01, IZB1A_U04, IZB1A_U06, IZB1A_U08, IZB1A_U07, IZB1A_K02
Filozoficzne i etyczne aspekty cyberprzestrzeni	Ćwiczenia audytoryjne	Aktywność na zajęciach, Prezentacja	IZB1A_W04, IZB1A_W06, IZB1A_U01, IZB1A_K05, IZB1A_K02
Programowanie w języku Rust	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Kolokwium, Wykonanie ćwiczeń laboratoryjnych, Projekt	IZB1A_W05, IZB1A_U01, IZB1A_U02, IZB1A_U08, IZB1A_K03, IZB1A_K04
Programowanie w języku C++	Wykład, Ćwiczenia laboratoryjne	Wykonanie ćwiczeń laboratoryjnych, Prezentacja	IZB1A_W05, IZB1A_W06, IZB1A_U06, IZB1A_U07, IZB1A_U01, IZB1A_K03
Bezpieczeństwo sieci komputerowych i usług sieciowych	Wykład, Ćwiczenia laboratoryjne	Egzamin, Wykonanie ćwiczeń laboratoryjnych, Studium przypadków	IZB1A_W07, IZB1A_W10, IZB1A_W11, IZB1A_U07, IZB1A_U08, IZB1A_U09, IZB1A_K03, IZB1A_K06
Programowanie w języku JavaScript	Wykład, Ćwiczenia laboratoryjne	Zaliczenie laboratorium, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W05, IZB1A_W06, IZB1A_U06, IZB1A_K03, IZB1A_K04
Programowanie w języku Python	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Udział w dyskusji, Kolokwium, Projekt	IZB1A_W05, IZB1A_W06, IZB1A_U08, IZB1A_U06, IZB1A_U07
Systemy i technologie wirtualizacji	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W06, IZB1A_W07, IZB1A_W05, IZB1A_W08, IZB1A_W09, IZB1A_U04, IZB1A_U06, IZB1A_U07, IZB1A_U05, IZB1A_K02, IZB1A_K03, IZB1A_K04
Budowa aplikacji internetowych	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Zaliczenie laboratorium, Wykonanie ćwiczeń laboratoryjnych, Odpowiedź ustna	IZB1A_W05, IZB1A_W07, IZB1A_W06, IZB1A_U06, IZB1A_U08
Bazy danych	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Aktywność na zajęciach, Kolokwium, Sprawozdanie, Prezentacja, Odpowiedź ustna, Wykonanie projektu	IZB1A_W05, IZB1A_W06, IZB1A_W07, IZB1A_U01, IZB1A_U02, IZB1A_U07, IZB1A_K04
Kryptografia kwantowa	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W01, IZB1A_W02, IZB1A_U01, IZB1A_U04, IZB1A_U07, IZB1A_U10, IZB1A_K02, IZB1A_K05, IZB1A_K06
Podstawy testów penetracyjnych	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Egzamin, Prezentacja, Wykonanie ćwiczeń laboratoryjnych, Wykonanie projektu	IZB1A_W03, IZB1A_W09, IZB1A_W08, IZB1A_U08, IZB1A_U03, IZB1A_U06, IZB1A_U07, IZB1A_U04, IZB1A_U05, IZB1A_K01, IZB1A_K03, IZB1A_K04

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
Kryptografia postkwantowa	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W01, IZB1A_W02, IZB1A_W10, IZB1A_W06, IZB1A_W03, IZB1A_U07, IZB1A_U08, IZB1A_U09, IZB1A_U01, IZB1A_U03, IZB1A_K02
Warsztat kompetencji akademickich i naukowych	Ćwiczenia audytoryjne	Wykonanie ćwiczeń, Zaangażowanie w pracę zespołu, Prezentacja	IZB1A_W04, IZB1A_W14, IZB1A_U01, IZB1A_U02, IZB1A_U03, IZB1A_K01, IZB1A_K03, IZB1A_K04
Informatyka kwantowa	Wykład, Ćwiczenia laboratoryjne	Zaliczenie laboratorium, Wykonanie ćwiczeń	IZB1A_W01, IZB1A_W02, IZB1A_W05, IZB1A_U06, IZB1A_K02
Zaawansowane testy penetracyjne	Wykład, Ćwiczenia laboratoryjne	Wynik testu zaliczeniowego, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W09, IZB1A_W05, IZB1A_W07, IZB1A_W03, IZB1A_W11, IZB1A_W06, IZB1A_W08, IZB1A_U07, IZB1A_U08, IZB1A_U06, IZB1A_U04, IZB1A_K01, IZB1A_K04
Dezinformacja i weryfikacja wiadomości	Wykład, Ćwiczenia audytoryjne	Kolokwium, Aktywność na zajęciach, Wykonanie ćwiczeń, Prezentacja	IZB1A_W04, IZB1A_W10, IZB1A_W11, IZB1A_W12, IZB1A_U01, IZB1A_U09, IZB1A_U03, IZB1A_U05, IZB1A_K02, IZB1A_K05, IZB1A_K06
Socjotechnika	Wykład, Ćwiczenia audytoryjne	Kolokwium, Sprawozdanie	IZB1A_W04, IZB1A_W08, IZB1A_W09, IZB1A_W10, IZB1A_W11, IZB1A_W12, IZB1A_U07, IZB1A_U08, IZB1A_U09, IZB1A_K02, IZB1A_K03, IZB1A_K06
Prywatność w sieci Internet	Wykład, Ćwiczenia laboratoryjne	Egzamin, Wykonanie ćwiczeń laboratoryjnych, Studium przypadków	IZB1A_W02, IZB1A_W07, IZB1A_W09, IZB1A_U08, IZB1A_K03, IZB1A_K04
Podstawy bezpieczeństwa oprogramowania	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W05, IZB1A_W06, IZB1A_W09, IZB1A_U07, IZB1A_U08, IZB1A_K02, IZB1A_K03, IZB1A_K05
Inżynieria wymagań i jakości	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych, Kolokwium, Odpowiedź ustna	IZB1A_W05, IZB1A_U06, IZB1A_U08, IZB1A_K01, IZB1A_K03
Technologie mobilne w obszarze bezpieczeństwa i obronności	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Wykonanie ćwiczeń	IZB1A_W07, IZB1A_W10, IZB1A_W11, IZB1A_U01, IZB1A_U02, IZB1A_U07, IZB1A_K03, IZB1A_K05
Podstawy sztucznej inteligencji	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Wykonanie ćwiczeń, Kolokwium, Sprawozdanie, Zaliczenie laboratorium, Udział w pracach badawczych, konferencjach, dodatkowych stażach i szkoleniach	IZB1A_W06, IZB1A_W13, IZB1A_U01, IZB1A_K02
UNIX Administration	Wykład, Ćwiczenia laboratoryjne	Udział w dyskusji, Kolokwium, Zaliczenie laboratorium	IZB1A_W07, IZB1A_W05, IZB1A_W06, IZB1A_U06, IZB1A_U08, IZB1A_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
Evolutionary Algorithms	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Udział w dyskusji, Odpowiedź ustna	IZB1A_W05, IZB1A_W06, IZB1A_U01, IZB1A_U02, IZB1A_K03, IZB1A_K04, IZB1A_K05
Bezpieczeństwo informacji	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń laboratoryjnych, Odpowiedź ustna	IZB1A_W03, IZB1A_W11, IZB1A_W12, IZB1A_W10, IZB1A_U03, IZB1A_U10, IZB1A_U09, IZB1A_U01, IZB1A_U05, IZB1A_K03, IZB1A_K05, IZB1A_K06
Metody i narzędzia detekcji incydentów	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Egzamin, Sprawozdanie, Projekt	IZB1A_W03, IZB1A_W07, IZB1A_W08, IZB1A_W09, IZB1A_U05, IZB1A_U06, IZB1A_U07, IZB1A_U08, IZB1A_K02, IZB1A_K03, IZB1A_K04, IZB1A_K05
Wykorzystanie SI w wykrywaniu zagrożeń	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Aktywność na zajęciach, Wykonanie ćwiczeń, Zaliczenie laboratorium	IZB1A_W06, IZB1A_W13, IZB1A_W08, IZB1A_W10, IZB1A_W12, IZB1A_U06, IZB1A_U07, IZB1A_K01
Ochrona własności intelektualnej	Wykład	Wynik testu zaliczeniowego	IZB1A_W04, IZB1A_W11, IZB1A_W14, IZB1A_W12, IZB1A_W10, IZB1A_U01, IZB1A_U09, IZB1A_U10, IZB1A_K02, IZB1A_K05, IZB1A_K06
Technologie internetu rzeczy	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Kolokwium, Wykonanie projektu	IZB1A_W06, IZB1A_W05, IZB1A_U06, IZB1A_U04, IZB1A_K05
Pracownia projektowa 1	Ćwiczenia projektowe	Projekt inżynierski	IZB1A_W05, IZB1A_U06, IZB1A_U07, IZB1A_U04, IZB1A_K03, IZB1A_K01
Bezpieczeństwo fizyczne obiektów użyteczności publicznej	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Sprawozdanie	IZB1A_W03, IZB1A_W09, IZB1A_W10, IZB1A_W11, IZB1A_W12, IZB1A_U01, IZB1A_U03, IZB1A_U05, IZB1A_U06, IZB1A_U04, IZB1A_U07, IZB1A_U09, IZB1A_U10, IZB1A_K02, IZB1A_K04, IZB1A_K05, IZB1A_K06, IZB1A_K01, IZB1A_K03
Modelowanie zagrożeń	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Aktywność na zajęciach, Studium przypadków	IZB1A_W03, IZB1A_W08, IZB1A_W09, IZB1A_W10, IZB1A_W04, IZB1A_W05, IZB1A_W07, IZB1A_W11, IZB1A_W12, IZB1A_U04, IZB1A_U05, IZB1A_U07, IZB1A_U06, IZB1A_U08, IZB1A_U09, IZB1A_K01, IZB1A_K02, IZB1A_K04, IZB1A_K05, IZB1A_K06
Zarządzanie incydentami SOC i CERT	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Kolokwium, Wykonanie ćwiczeń, Prezentacja	IZB1A_W03, IZB1A_W07, IZB1A_W10, IZB1A_W08, IZB1A_W09, IZB1A_W11, IZB1A_U06, IZB1A_U07, IZB1A_K05, IZB1A_K06
Zarządzanie projektami informatycznymi	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Aktywność na zajęciach, Wykonanie projektu, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W04, IZB1A_W14, IZB1A_W03, IZB1A_U02, IZB1A_U06, IZB1A_U03, IZB1A_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
Wywiad przemysłowy	Wykład, Ćwiczenia projektowe	Udział w dyskusji, Kolokwium, Projekt	IZB1A_W03, IZB1A_W04, IZB1A_W08, IZB1A_W09, IZB1A_W10, IZB1A_W11, IZB1A_W12, IZB1A_U01, IZB1A_U03, IZB1A_U06, IZB1A_U08, IZB1A_U09, IZB1A_K01, IZB1A_K02, IZB1A_K03, IZB1A_K05, IZB1A_K06
Praktyka zawodowa	Praktyka zawodowa	Sprawozdanie z odbycia praktyki	IZB1A_U03, IZB1A_U04, IZB1A_U01, IZB1A_K05
Analiza malware	Wykład, Ćwiczenia laboratoryjne	Wykonanie ćwiczeń laboratoryjnych	IZB1A_W05, IZB1A_W09, IZB1A_U05, IZB1A_U07, IZB1A_K05
Systemy informatyczne do przetwarzania informacji niejawnych	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Kolokwium, Studium przypadków , Wykonanie ćwiczeń, Wykonanie projektu	IZB1A_W03, IZB1A_W10, IZB1A_W11, IZB1A_W12, IZB1A_W07, IZB1A_W09, IZB1A_W02, IZB1A_W05, IZB1A_W06, IZB1A_U01, IZB1A_U04, IZB1A_U06, IZB1A_U07, IZB1A_U10, IZB1A_U08, IZB1A_U03, IZB1A_K02, IZB1A_K03, IZB1A_K06, IZB1A_K01, IZB1A_K04
Architektura i bezpieczeństwo Infrastruktury Data Center	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Udział w dyskusji, Studium przypadków , Wykonanie projektu, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W03, IZB1A_W07, IZB1A_W09, IZB1A_W10, IZB1A_W11, IZB1A_W04, IZB1A_U05, IZB1A_U06, IZB1A_U09, IZB1A_U10, IZB1A_U07, IZB1A_K03, IZB1A_K04, IZB1A_K06, IZB1A_K02, IZB1A_K05
Informatyka śledcza i analiza powłamaniowa	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Wykonanie projektu, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W02, IZB1A_W10, IZB1A_W12, IZB1A_W07, IZB1A_W08, IZB1A_W11, IZB1A_U05, IZB1A_U09, IZB1A_K05, IZB1A_K06
Biały wywiad	Ćwiczenia laboratoryjne	Kolokwium, Projekt	IZB1A_W03, IZB1A_W04, IZB1A_W08, IZB1A_W10, IZB1A_W12, IZB1A_U01, IZB1A_U09, IZB1A_U03, IZB1A_U07, IZB1A_K02, IZB1A_K04, IZB1A_K06, IZB1A_K03, IZB1A_K05
Projektowanie i budowa systemów zarządzania bezpieczeństwem informacji w organizacji	Wykład, Ćwiczenia audytoryjne	Egzamin, Aktywność na zajęciach, Kolokwium	IZB1A_W03, IZB1A_W07, IZB1A_W09, IZB1A_W11, IZB1A_W12, IZB1A_U05, IZB1A_U07, IZB1A_U08, IZB1A_U09, IZB1A_U01, IZB1A_U02, IZB1A_U03, IZB1A_U10, IZB1A_K01, IZB1A_K03, IZB1A_K04, IZB1A_K05, IZB1A_K02, IZB1A_K06
Wprowadzenie do technologii Blockchain	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Kolokwium, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W02, IZB1A_W05, IZB1A_W06, IZB1A_W07, IZB1A_U04, IZB1A_U06, IZB1A_U07, IZB1A_U08, IZB1A_K01, IZB1A_K02, IZB1A_K03, IZB1A_K05
Zagrożenia dla płatności elektronicznych	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Kolokwium, Wykonanie ćwiczeń, Zaliczenie laboratorium	IZB1A_W04, IZB1A_W08, IZB1A_W09, IZB1A_W10, IZB1A_W12, IZB1A_U01, IZB1A_U06, IZB1A_U07, IZB1A_U08, IZB1A_U09, IZB1A_K02, IZB1A_K03, IZB1A_K05, IZB1A_K06

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
Architektura rozwiązań chmurowych	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Kolokwium, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W05, IZB1A_W07, IZB1A_W06, IZB1A_W09, IZB1A_U06, IZB1A_U07, IZB1A_U08, IZB1A_K02, IZB1A_K03
Pracownia projektowa 2	Ćwiczenia projektowe	Wykonanie projektu, Projekt	IZB1A_W05, IZB1A_W07, IZB1A_U02, IZB1A_U04, IZB1A_U06, IZB1A_U07, IZB1A_U08, IZB1A_K03, IZB1A_K04
Kryptografia wizualna i steganografia	Wykład, Ćwiczenia laboratoryjne	Prezentacja, Wykonanie projektu, Referat, Zaangażowanie w pracę zespołu	IZB1A_W02, IZB1A_W03, IZB1A_W04, IZB1A_U03, IZB1A_U04, IZB1A_U01, IZB1A_K03, IZB1A_K05
Bezpieczeństwo infrastruktury krytycznej	Wykład, Ćwiczenia laboratoryjne	Wykonanie projektu, Kolokwium, Wykonanie ćwiczeń laboratoryjnych, Przygotowanie i przeprowadzenie badań	IZB1A_W03, IZB1A_W07, IZB1A_W10, IZB1A_W11, IZB1A_W12, IZB1A_U05, IZB1A_U06, IZB1A_U08, IZB1A_U09, IZB1A_U10, IZB1A_U01, IZB1A_K03, IZB1A_K04, IZB1A_K06
Analiza informacji	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Projekt, Studium przypadków	IZB1A_W04, IZB1A_W08, IZB1A_U01, IZB1A_U03, IZB1A_K02, IZB1A_K05, IZB1A_K01
Projekt dyplomowy	Projekt dyplomowy	Wykonanie projektu	IZB1A_U01, IZB1A_U02, IZB1A_U04, IZB1A_K01, IZB1A_K03
Analiza danych	Wykład, Ćwiczenia laboratoryjne	Udział w dyskusji, Kolokwium, Potwierdzenie realizacji programu praktyki, Wykonanie ćwiczeń laboratoryjnych, Sprawozdanie	IZB1A_W04, IZB1A_W08, IZB1A_W06, IZB1A_W13, IZB1A_U01, IZB1A_U02, IZB1A_U05, IZB1A_K01, IZB1A_K03, IZB1A_K04
Eksploracja danych	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Zaliczenie laboratorium	IZB1A_W09, IZB1A_W13, IZB1A_U06, IZB1A_U07, IZB1A_U08, IZB1A_K01, IZB1A_K03, IZB1A_K04
Bezpieczeństwo systemów sztucznej inteligencji	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych, Zaangażowanie w pracę zespołu, Zaliczenie laboratorium	IZB1A_W07, IZB1A_W13, IZB1A_W12, IZB1A_W14, IZB1A_W05, IZB1A_W09, IZB1A_U07, IZB1A_U08, IZB1A_U06, IZB1A_U09, IZB1A_U10, IZB1A_K01, IZB1A_K05, IZB1A_K03, IZB1A_K04
Bezpieczeństwo urządzeń mobilnych	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Wykonanie ćwiczeń laboratoryjnych	IZB1A_W07, IZB1A_U06, IZB1A_K02, IZB1A_K05

ECTS

Kierunek: Informatyka - Zarządzanie Bezpieczeństwem Informacji

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

zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	108 ECTS
zajęć z zakresu nauk podstawowych właściwych dla danego kierunku studiów	39
zajęć o charakterze praktycznym, kształtujących umiejętności praktyczne, w tym zajęć laboratoryjnych, projektowych, praktycznych i warsztatowych	70 ECTS
zajęć podlegających wyborowi przez studenta (w wymiarze nie mniejszym niż 30% liczby punktów ECTS koniecznych do uzyskania kwalifikacji odpowiadających poziomowi kształcenia)	82 ECTS
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	6 ECTS
zajęć z języka obcego	6 ECTS
praktyk zawodowych	4 ECTS
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)	110 ECTS
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)	Nie dotyczy

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

Kierunek: Informatyka - Zarządzanie Bezpieczeństwem Informacji

Zasady wpisu na kolejny semestr

Jeżeli student nie posiada deficytu punktów ECTS jest zapisywany na kolejny semestr automatycznie. W przypadku deficytu nie przekraczającego 15 punktów ECTS, student składa do dziekanatu podanie o wpis na semestr z deficytem punktów. Jeżeli deficyt jest większy od 15 punktów student może złożyć podanie o powtarzanie semestru.

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

Jeżeli student nie posiada deficytu punktów ECTS jest zapisywany na kolejny semestr automatycznie. W przypadku deficytu nie przekraczającego 15 punktów ECTS, student składa do dziekanatu podanie o wpis na semestr z deficytem punktów. Jeżeli deficyt jest większy od 15 punktów student może złożyć podanie o powtarzanie semestru.

Dopuszczalny deficyt punktów ECTS

15 ECTS

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)

Nie występują.

Semestry kontrolne

Semestr 6 jest semestrem kontorlnym. Warunkiem wpisu na 7 semestr jest zaliczenie wszystkich przedmiotów z semestrów 1-6 oraz praktyki zawodowej.

Zasady odbywania studiów według indywidualnej organizacji studiów

Studenci mogą uzyskać zgodę na studia według Indywidualnej Organizacji Studiów (IOS). Studia według IOS prowadzone są według planu studiów na tym kierunku, dostosowanego do zainteresowań studenta, zatwierdzonego przez Dziekana ds. Kształcenia. Merytoryczny nadzór nad studiami według IOS pełni opiekun naukowy, którym może być pracownik naukowo-dydaktyczny AGH z co najmniej stopniem naukowym doktora. Opiekuna naukowego zatwierdza Dziekan ds. Kształcenia.

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

Praktyka jest zaliczana przez studenta studiów stacjonarnych, po wakacjach, w czasie sesji poprawkowej. Organizacja praktyk jest koordynowana przez opiekuna praktyk studenckich dla kierunku Informatyka - Zarządzanie Bezpieczeństwem Informacji. Na stronie wydziału dostępna jest procedura obsługi praktyk. Sprawdzenie osiągnięcia założonych w przedmiocie Praktyka Zawodowa efektów kształcenia i ich ocena są dokonywane w oparciu o zaświadczenie (zawierające sprawozdanie opisujące zakres prac realizowanych w ramach praktyki, ich wykonanie, umiejętności pracy w grupie, itd.), które są sprawdzane przez opiekuna praktyk studenckich, poświadczone przez opiekuna studentów w zakładzie pracy. W przypadkach budzących wątpliwości, rozstrzyga się je poprzez rozmowę z opiekunem w zakładzie pracy, i/lub ze studentem. Potwierdzenie praktyki zawiera opis zadań wykonanych w trakcie praktyki, wypełniany przez studenta, oraz opinię o praktykancie, wypełnianą przez opiekuna praktykanta w przedsiębiorstwie/instytucji.

Zasady obieralności modułów zajęć

Studenci składają deklarację, w której określają preferencje modułów. O pierwszeństwie zapisu na moduł decyduje średna ocen uzyskanych w dwóch poprzednich semestrach.

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

Nie dotyczy.

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

Realizując zapisy Regulaminu Studiów przyjęto, że praca dyplomowa inżynierska ma postać projektu inżynierskiego, czyli udokumentowanego przedsięwzięcia projektowego. Projekty inżynierskie realizowane są przez zespoły studenckie liczące 2-4 osób.

Proces dyplomowania rozpoczyna się na początku semestru 6 zgłoszeniem i opublikowaniem w wewnętrznym wydziałowym systemie tematów projektów inżynierskich. Opiekunem projektu inżynierskiego może być pracownik dydaktyczny Wydziału Informatyki w stopniu co najmniej doktora.

Studenci łączą się w zespoły i wybierają temat projektu inżynierskiego. Opiekun projektu po konsultacji z zespołem studentów zgłasza wniosek w systemie APD. Tematy projektów inżynierskich zatwierdza Komisja ds Jakości Dyplomowania.

Po akceptacji wniosku przez Komisję rozpoczyna się proces merytorycznych konsultacji prowadzący do osiągnięcia celu jakim jest realizacja projektu.

Z procesem dyplomowania związane są dwa przedmioty: Pracownia projektowa 1 w szóstym semestrze oraz Pracownia projektowa 2 w siódmym semestrze. Zadaniem tych przedmiotów jest dbanie o właściwe postępy w realizacji projektu, a przede wszystkim dbanie o formalną poprawność dokumentacji projektu.

Tekst pracy podlega recenzowaniu przez dwie osoby: opiekuna pracy i dodatkowego recenzenta. Recenzentów powołuje pełnomocnik Dziekana ds. Dyplomowania zgodnie z zasadą aby przynajmniej jeden z pary opiekun, recenzent był samodzielnym pracownikiem naukowym.

Po zaakceptowaniu przez opiekuna tekstu pracy studenci umieszczają go w systemie APD i po uzyskaniu dwóch pozytywnych ocen następuje rejestracja pracy w systemie APD.

Egzaminy dyplomowe odbywają się w terminach ogłoszonych na początku roku akademickiego.

Egzamin dyplomowy jest prowadzony się przed komisją, której przewodniczy samodzielny pracownik naukowy wydziału. Ma on charakter obrony projektu inżynierskiego i składa się z dwóch części. Pierwsza część obejmuje prezentację projektu przez realizujący ją zespół oraz dyskusję nad projektem inżynierskim. Część druga służy weryfikacji efektów uczenia określonych w programie studiów. W drugiej części każdy ze studentów indywidualnie odpowiada na trzy pytania, z których otrzymuje oceny. Lista ramowych zagadnień obejmujących zakres przedmiotów obowiązkowych dla kierunku studiów jest udostępniana studentom przed egzaminem dyplomowym. Na podstawie oceny prezentacji projektu oraz ocen odpowiedzi na pytania, wystawiana jest ocena z egzaminu dyplomowego.

Przyjęto zasadę, że opiekun danej pracy nie może być przewodniczącym ani członkiem komisji dyplomowania, w której odbywa się egzamin dyplomowy.

Zasady ustalania ogólnego wyniku ukończenia studiów

Ocenę ukończenia studiów, zgodnie z regulaminem studiów, wyznacza się na podstawie średniej ze studiów (waga 60%), oceny z projektu (waga 20%) oraz oceny z egzaminu dyplomowego (waga 20%).

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

Nie dotyczy.