Program studiów

Kierunek: Cyberbezpieczeństwo

Spis treści

Charakterystyka kierunku

Informacje podstawowe

Nazwa wydziału:	Wydział Informatyki, Elektroniki i Telekomunikacji
Nazwa kierunku:	Cyberbezpieczeństwo
Poziom:	Studia inżynierskie I stopnia
Profil:	Ogólnoakademicki
Forma:	Stacjonarne
Klasyfikacja ISCED:	0612
Liczba punktów ECTS konieczna do ukończenia studiów na danym poziomie:	210
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

Kierunek studiów Cyberbezpieczeństwo wpisuje się ściśle zarówno w strategie rozwoju AGH i Wydziału Informatyki, Elektroniki i Telekomunikacji, jak i w misje tych jednostek. W misji AGH zapisano: „AGH jest uniwersytetem, który od ponad stu lat przyczynia się do dobrobytu ogółu poprzez rozwijanie badań i kształcenie w zakresie nauk technicznych, ścisłych oraz społecznych i humanistycznych, zapewniając tworzenie innowacji technologicznych i społecznych, służących rozwiązywaniu najważniejszych problemów współczesności". W związku z tym, zgodnie ze światowymi trendami rozwoju uczelnia tworzy nowe kierunki kształcenia i zachowuje klasyczne - niezbędne do prawidłowego rozwoju nauki, techniki oraz gospodarki naszego kraju.

Kierunek studiów Cyberbezpieczeństwo zwiększa potencjał rozwojowy uczelni poprzez rozszerzenie i wzbogacenie oferty edukacyjnej oraz poprawę jakości kształcenia w celu udoskonalenia profilu absolwenta cyberbezpieczeństwa AGH do aktualnych potrzeb rynku pracy i wzorców europejskich. Kierunek ten jest idealnym przykładem interdyscyplinarnego podejścia do nowoczesnego kształcenia. Dominujące nauki ścisłe są bowiem uzupełnione elementami nauk społecznych. Takie połączenie pozwala absolwentom wyjść naprzeciw wielowymiarowym i złożonym problemom cyberbezpieczeństwa. Dodatkowo, biorąc pod uwagę aktualne trendy związane z wpływem nowoczesnych technologii na funkcjonowanie wszystkich sektorów - publicznego, prywatnego, kształcenie specjalistów w zakresie cyberbezpieczeństwa przyczyni się do wzmacniania bezpieczeństwa i potencjału gospodarczego kraju.

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

Cyberbezpieczeństwo uważa się za jeden z najważniejszych czynników warunkujących rozwój europejskiej gospodarki. Bez zaufania konsumentów oraz użytkowników do korzystania z Internetu, proces ten jest poważnie zagrożony. Potrzeby związane z cyberbezpieczeństwem są bezsprzeczne i stale rosnące. Jednocześnie podaż specjalistów z obszaru cyberbezpieczeństwa zupełnie nie nadąża za popytem. Co warto podkreślić - jest to trend globalny.

Wagę problemu dostrzegły zarówno organizacje międzynarodowe jak i poszczególne państwa tworząc regulacje wymagające podejmowania szerokich działań w obszarze cyberbezpieczeństwa. W 2016 roku przyjęte zostało pierwsze unijne prawo poświęcone cyberbezpieczeństwu - Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Dyrektywa stawia wielowymiarowe wymagania zarówno przed podmiotami publicznymi, jak i przedsiębiorstwami w zakresie zapewniania cyberbezpieczeństwa. Z kolei na gruncie polskim przyjęto kompleksową regulację - ustawę o krajowym systemie cyberbezpieczeństwa. Stanowi ona kluczowy dokument, który wprowadza wiele wymagań związanych z podejmowaniem działań nakierowanych na cyberbezpieczeństwo, zarówno przez sektor prywatny, jak i publiczny. Warto także wspomnieć, że specjaliści od bezpieczeństwa teleinformatycznego są niezbędni by wypełniać wymagania regulacyjne także nie wprost odnoszące się do cyberbezpieczeństwa. Dobrym przykładem jest tutaj RODO. Ochrona danych osobowych jest dzisiaj ściśle związana z zapewnieniem cyberbezpieczeństwa.

Poza wymaganiami regulacyjnymi, nie sposób wyobrazić sobie efektywne funkcjonowanie podmiotów komercyjnych bez wdrażania systemu zarządzania cyberbezpieczeństwem. Niemal każda firma, korzysta każdego dnia z nowoczesnych technologii. Coraz częściej stanowią one fundament ich biznesu. Trend ten będzie się wyłącznie pogłębiał i będzie niósł coraz poważniejsze konsekwencje - szczególnie przy postępującej automatyzacji i rozwoju Internetu Rzeczy. Dostrzegają to strategiczne koncepcje rozwoju kraju, mówiące o konieczności budowania przemysłu 4.0.

Ścieżki kształcenia - zakres w języku polskim oraz w języku angielskim

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)

Kierunek Cyberbezpieczeństwo kształci absolwentów, którzy są niezbędnymi ogniwami pozwalającymi realizować kierunki rozwoju gospodarki Polski zapisane w strategicznych dokumentach takich jak choćby w Strategii na rzecz Odpowiedzialnego Rozwoju. W ten sposób kierunek cyberbezpieczeństwo wpisuje się nie tylko w misję AGH, wydziału IEiT ale i szerzej w strategiczne kierunki rozwoju Polski a nawet Europy.

Wskazać można kilka obszarów (jest to lista przykładowa, nie wyczerpująca) zatrudnienia absolwentów.
- Podmioty gospodarcze: każda współczesna firma musi dbać o bezpieczeństwo swoich systemów i sieci teleinformatycznych, aby realizować swoje zadania. Natomiast ze względów regulacyjnych, wiele sektorów będzie musiało (pod groźbą sankcji) zatrudniać lub wynajmować specjalistów w tej dziedzinie. Ustawa o krajowym systemie cyberbezpieczeństwa wskazuje 6 sektorów podzielonych na wiele podsektorów (energia, transport, ochrona zdrowia, bankowość i infrastruktura rynków finansowych, zaopatrzenie w wodę pitną i jej dystrybucja, infrastruktura cyfrowa) oraz dostawców usług cyfrowych, którzy będą musieli realizować wiele działań w obszarze cyberbezpieczeństwa. Regulacje dotyczą także podmiotów zakwalifikowanych jako operatorzy infrastruktury krytycznej (11 sektorów) oraz przedsiębiorców telekomunikacyjnych. Warto zauważyć, że otwiera to rynek zarówno na potencjalnych pracowników tych przedsiębiorstw, ale także na rozwój nowych firm, które zewnętrznie mogą dostarczać owych usług. Wszystkie podmioty gospodarcze muszą sprostać także wyzwaniom związanym z ochroną danych osobowych.
- Instytucje publiczne, administracja publiczna: rządowa i samorządowa: ustawa o krajowym systemie cyberbezpieczeństwa jak i wcześniejsze regulacje, wymagają aby działania w zakresie cyberbezpieczeństwa podejmowały także podmioty publiczne. Możliwości w tym zakresie wykraczają jednak poza ten tradycyjny wymiar. Coraz częściej podmioty te potrzebują pracowników, którzy posiadać będą nie tylko wiedzę techniczną ale rozumieć będą procesy związane z politykami publicznymi i tym jak wpływa na nie cyberbezpieczeństwo. Otwiera to zupełnie nowe możliwości dla absolwentów, którzy kreować będą działania i decyzje związane z takimi obszarami jak bezpieczeństwo, polityka zagraniczna, polityka ekonomiczna, rozwiązania legislacyjne, itd.
- Organy odpowiedzialne za bezpieczeństwo: wszystkie organy odpowiedzialne za bezpieczeństwo - zarówno wewnętrzne oraz zewnętrzne - poszukują specjalistów mających wiedzę oraz umiejętności z zakresu cyberbezpieczeństwa. Wiąże się to z koniecznością przeciwdziałaniu takim zagrożeniom jak cyberprzestępczość, cyberterroryzm, cyberszpiegostwo itd. Potencjalne miejsca zatrudnienia absolwentów to m.in.: policja, służby specjalne, wojsko.

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

Bez wątpienia kierunek cyberbezpieczeństwo jest odpowiedzią na potrzeby rynku wynikające z przemian społeczeństwa, gospodarki, struktur państwowych. Cyberprzestrzeń przenika i warunkuje wszystkie obszary życia społecznego, biznesowego, a zapewnianie cyberbezpieczeństwa jest warunkiem realizowania wszystkich procesów. Potrzebę kształcenia specjalistów w obszarze cyberbezpieczeństwa potwierdzają zarówno wyniki badań jak i głosy płynące ze środowiska biznesowego. Potwierdza to także obserwacja trendów w rozwoju kierunków kształcenia w innych państwach - zarówno w Europie jak i w USA.

Konstruując program studiów kierunku Cyberbezpieczeństwo brano pod uwagę losy absolwentów Wydziału IEiT AGH, które wskazują na bardzo dobrą ich pozycję na rynku. Bardzo duży odsetek studentów stwierdza, że drugi raz wybraliby te same studia, a bardzo niski odsetek (kilka procent) nie podejmuje pracy po zakończeniu studiów (najczęściej z różnych powodów losowych). Kierunek Cyberbezpieczeństwo niewątpliwie rozszerza ofertę Wydziału IEIT o kształcenie studentów z bardzo poszukiwanymi kompetencjami na rynku.

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 na kierunku Cyberbezpieczeństwo.

Informacja na temat uwzględnienia w programie studiów przykładów dobrych praktyk

- Dużą wagę przywiązuje się do szerokiej oferty przedmiotów obieralnych, łącznie z ciekawymi przedmiotami kierunkowymi i humanistycznymi.
- Na wydziale i na Uczelni były realizowane programy w konkursie POWER, dzięki którym dydaktycy mają możliwość aktualizować materiały w ramach prowadzonych modułów, a także zdobyć nowe kompetencje np. dotyczące nowatorskich metod nauczania.
- Wielu prowadzących jest bardzo otwartych na potrzeby studentów oraz na umożliwienie im rozwoju, chętnie znajdując czas na konsultacje nawet poza regularnymi godzinami spotkań.
- Prodziekan ds. Kształcenia dla kierunku Cyberbezpieczeństwo oraz wyznaczony opiekun kierunku w sposób otwarty i kompetentny opiekują się studentami, pomagają rozwiązywać ich problemy i czuwają całościowo nad jakością kształcenia.
- Osoby odpowiedzialne za moduły oraz kierownictwo jest w ciągłym kontakcie z organami studenckimi, np. WRSS i z chęcią podejmują wszelkie działania na rzecz umożliwienia bezproblemowego zdobywania wiedzy przez studentow.

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

Zespół opracowujący program studiów przed rozpoczęciem prac przeprowadził ankietę wśród potencjalnych pracodawców, której wyniki zostały wzięte pod uwagę w trakcie opracowania siatki oraz efektów kształcenia. Ankiety zostały opracowane m.in. przez następujących interesariuszy: Sabre, Exatel, Komenda Stołeczna Policji - Wydział ds. Cyberbezpieczeństwa, USB Business Solutions Szwajcaria, SecuRing, Price Waterhouse Coopers, Centrum Szkolenia Sił Połączonych NATO w Bydgoszczy, Ministerstwo Spraw Zagranicznych, KPMG, Grey Wizard, DYSKRET, Cryptomage, CISCO, Accenture, NASK, mikromakro, Cyberus Labs, Komenda Wojewódzka Policji w Katowicach. Wszyscy interesariusze wyrazili chęć potencjalnego zatrudnienia absolwentów kierunku.

Wymiar, zasady i forma odbywania praktyk zawodowych

Obowiązkową praktykę zawodową w wymiarze 4 punktów ECTS, która powinna trwać co najmniej 4 tyg. (1 miesiąc), wprowadzono aby jak najlepiej przygotować do pracy przyszłych inżynierów kierunku Cyberbezpieczeństwo. Praktyki zawodowe odbywają się w trakcie wakacji letnich, po zakończeniu zajęć 6 semestru. Student ma obowiązek realizacji zajęć praktycznych w wybranym podmiocie, który realizuje projekty inżynierskie bądź badawczo-rozwojowe w zakresie IT obejmujących aspekty cyberbezpieczeństwa. Rekrutacja odbywa się zgodnie z regulaminem studiów AGH - na odpowiednim formularzu student zgłasza chęć odbycia praktyki w danej firmie/instytucji; po otrzymaniu akceptacji realizuje praktykę, której wyniki będą podsumowane w zaświadczeniu od pracodawcy, zawierającym opis wymaganych efektów kształcenia.

Warunki rekrutacji na studia

Kierunek: Cyberbezpieczeństwo

Opis kompetencji oczekiwanych od kandydata ubiegającego się o przyjęcie na studia

Osoba chętna do podjęcia studiów powinna wykazywać zainteresowanie nowoczesnymi technologiami, a w szczególności związanymi z bezpieczeństwem w sieciach komputerowych. Dodatkowym atutem będzie zainteresowanie i praktyka, choćby amatorska w administracji systemami komputerowymi.

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: 45
Maksymalna liczba studentów: 60

Efekty uczenia się

Kierunek: Cyberbezpieczeństwo

Wiedza

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
CBZ1A_W01	Ma wiedzę z matematyki i fizyki, niezbędną do zrozumienia, stosowania i opracowywania rozwiązań technicznych z zakresu cyberbezpieczeństwa	P6S_WG_A
CBZ1A_W02	Ma wiedzę z zakresu działania sieci teleinformatycznych oraz związanych z nimi uwarunkowań mających wpływ na poziom bezpieczeństwa przesyłanych danych	P6S_WG_A_Inz, P6S_WG_A
CBZ1A_W03	Ma wiedzę w zakresie algorytmów, struktur danych, baz danych i wybranych języków programowania, pozwalającą tworzyć bezpieczne oprogramowanie oraz weryfikować poziom bezpieczeństwa aplikacji i systemów informatycznych.	P6S_WG_A_Inz, P6S_WG_A
CBZ1A_W04	Zna i rozumie działanie specjalistycznych rozwiązań ochrony danych cyfrowych, w szczególności algorytmów kryptograficznych, protokołów i usług bezpieczeństwa	P6S_WG_A_Inz
CBZ1A_W05	Ma szczegółową wiedzę w zakresie technicznych środków zabezpieczania systemów informatycznych i sieci teleinformatycznych, a także wykrywania w nich podatności, zagrożeń i ataków	P6S_WG_A_Inz
CBZ1A_W06	Zna podstawowe zasady stosowania proceduralnych środków bezpieczeństwa, prowadzenia działalności gospodarczej, ochrony własności intelektualnej, zarządzania ryzykiem oraz inne pozatechniczne aspekty związane z ochroną zasobów	P6S_WK_A, P6S_WK_A_Inz
CBZ1A_W07	Posiada wiedzę z zakresu uwarunkowań prawnych i regulacyjnych wpływających na działania zespołów i jednostek zaangażowanych w zapewnianie cyberbezpieczeństwa, w tym określające ich obowiązki	P6S_WK_A
CBZ1A_W08	Zna zasady funkcjonowania kompleksowych systemów cyberbezpieczeństwa na różnym szczeblu, w tym krajowego i międzynarodowego systemu cyberbezpieczeństwa	P6S_WK_A
CBZ1A_W09	Zna i rozumie zagrożenia, wyzwania oraz szanse wynikające z funkcjonowania w świecie cyfrowym i wpływające na współczesne państwa, społeczeństwo czy podmioty publiczne i prywatne	P6S_WK_A
CBZ1A_W10	Zna standardy, normy, rekomendacje i dobre praktyki dotyczące cyberbezpieczeństwa	P6S_WK_A

Umiejętności

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
CBZ1A_U01	Potrafi pozyskać informacje dobierając odpowiednie źródła, dokonać krytycznej analizy, wyciągnąć wnioski i sformułować opinie, dzięki czemu może realizować zadania związane z cyberbezpieczeństwem, w tym z zakresu informatyki śledczej i białego wywiadu	P6S_UW_A
CBZ1A_U02	Potrafi opracować dokumentację, przedstawić prezentację i dyskutować na temat zadania inżynierskiego czy projektu z zakresu cyberbezpieczeństwa, również w języku obcym na poziomie B2 ESKOJ	P6S_UK_A
CBZ1A_U03	Potrafi pracować indywidualnie i zespołowo, planować pracę oraz komunikować się w celu realizacji zadań związanych z zapewnieniem bezpieczeństwa systemów i sieci teleinformatycznych	P6S_UO_A
CBZ1A_U04	Ma umiejętność samokształcenia, potrafi podnosić nabyte kwalifikacje inżyniera cyberbezpieczeństwa oraz planować swój dalszy rozwój zawodowy	P6S_UU_A
CBZ1A_U05	Potrafi zaplanować oraz przeprowadzić testy, eksperymenty i badania pozwalające na ocenę poziomu bezpieczeństwa wybranej aplikacji, systemu informatycznego, urządzenia lub sieci komputerowej, w tym oparte na wynikach testów penetracyjnych czy analizie zachowania i weryfikacji kodu źródłowego	P6S_UW_A_Inz_01

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
CBZ1A_U06	Potrafi projektować oraz za pomocą odpowiednich narzędzi analizować działanie algorytmów, mechanizmów, protokołów i usług bezpieczeństwa, które są stosowane w celu ochrony systemów i sieci teleinformatycznych	P6S_UW_A_Inz_02
CBZ1A_U07	Potrafi konfigurować urządzenia i systemy informatyczne, dobierając odpowiedni poziom bezpieczeństwa oraz dbać o bezpieczeństwo chronionych zasobów	P6S_UW_A_Inz_02
CBZ1A_U08	Potrafi opracować algorytmy i oprogramowanie zapewniające bezpieczeństwo aplikacji i systemów w oparciu o poznane języki programowania, bazy danych, biblioteki programistyczne i rozwiązania oparte na uczeniu maszynowym	P6S_UW_A_Inz_02
CBZ1A_U09	Potrafi analizować akty prawne, standardy i rekomendacje kluczowe z punktu widzenia cyberbezpieczeństwa oraz implementować wynikające z nich obowiązki i wymagania	P6S_UO_A, P6S_UK_A
CBZ1A_U10	Potrafi zaplanować oraz wdrożyć procedury i rozwiązania organizacyjne związane z ochroną danych i użytkowników	P6S_UW_A
CBZ1A_U11	Potrafi oszacować poziom zagrożeń i zarządzać ryzykiem związanym z wielowymiarowymi wyzwaniami płynącymi z cyberprzestrzeni	P6S_UK_A, P6S_UW_A

Kompetencje społeczne

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
CBZ1A_K01	Rozumie potrzebę krytycznej oceny posiadanej wiedzy, podnoszenia swoich kompetencji zawodowych i konsultacji z innymi ekspertami	P6S_KK_A
CBZ1A_K02	Potrafi współpracować w grupie, ma świadomość odpowiedzialności za realizowane zadania oraz umie myśleć i działać w sposób przedsiębiorczy	P6S_KO_A
CBZ1A_K03	Ma świadomość roli zawodowej i społecznej absolwenta uczelni technicznej oraz wagi przestrzegania zasad etyki zawodowej, szczególnie w obszarze cyberbezpieczeństwa	P6S_KR_A
CBZ1A_K04	Potrafi funkcjonować w złożonym ekosystemie podmiotów związanych z zapewnianiem cyberbezpieczeństwa - zarówno z punktu widzenia sektora prywatnego, jak i publicznego	P6S_KO_A
CBZ1A_K05	Ma świadomość tego jak tworzenie i wdrażanie rozwiązań z obszaru cyberbezpieczeństwa może wpływać na funkcjonowanie otoczenia gospodarczego, społecznego i politycznego oraz na funkcjonowanie jednostek	P6S_KR_A
CBZ1A_K06	Potrafi funkcjonować w interdyscyplinarnych zespołach zajmujących się wielowymiarowym analizowaniem i reagowaniem na zdarzenia mające wpływ na cyberbezpieczeństwo	P6S_KO_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
P6S_WG_A_Inz	Absolwent zna i rozumie podstawowe procesy zachodzące w cyklu życia urządzeń, obiektów i systemów technicznych	CBZ1A_W02, CBZ1A_W03, CBZ1A_W04, CBZ1A_W05
P6S_WK_A_Inz	Absolwent zna i rozumie podstawowe zasady tworzenia i rozwoju różnych form indywidualnej przedsiębiorczości	CBZ1A_W06

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	CBZ1A_U05
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	CBZ1A_U06, CBZ1A_U07, CBZ1A_U08

Matryca pokrycia efektów kierunkowych

Kierunek: Cyberbezpieczeństwo

2026/2027/S/Ii/IEiT/CBZ/all

Przedmiot	Kod	Semestr	CBZ1A_W01	CBZ1A_W02	CBZ1A_W03	CBZ1A_W04	CBZ1A_W05	CBZ1A_W06	CBZ1A_W07	CBZ1A_W08	CBZ1A_W09	CBZ1A_W10	CBZ1A_U01	CBZ1A_U02	CBZ1A_U03	CBZ1A_U04	CBZ1A_U05	CBZ1A_U06	CBZ1A_U07	CBZ1A_U08	CBZ1A_U09	CBZ1A_U10	CBZ1A_U11	CBZ1A_K01	CBZ1A_K02	CBZ1A_K03	CBZ1A_K04	CBZ1A_K05	CBZ1A_K06
Algebra	ICBZS.Ii1.00371.26	1s	x														x	x		x				x		x			
Analiza matematyczna	ICBZS.Ii1.00773.26	1s	x										x											x					
Wprowadzenie do sieci Internet	ICBZS.Ii1.02353.26	1s				x									x										x				
Podstawy programowania	ICBZS.Ii1.01049.26	1s			x															x				x	x				
Architektura komputerów i systemy operacyjne	ICBZS.Ii1.16552.26	1s			x	x	x					x							x	x				x					
Zarządzanie bezpieczeństwem informacji	ICBZS.Ii1.08321.26	1s						x	x	x		x	x		x						x	x	x	x			x	x	x
Krajowy system cyberbezpieczeństwa	ICBZS.Ii1.08314.26	1s							x	x	x					x					x			x			x	x	x
Fizyka 1	ICBZS.Ii2.00318.26	2s	x										x	x	x	x								x					
Język angielski B2 - Moduł 1	ICBZS.Ii2.19698.26	2s												x															
Bezpieczeństwo systemów i sieci teleinformatycznych	ICBZS.Ii2.08319.26	2s	x			x	x						x					x	x					x			x		
Język francuski B2 - Moduł 1	ICBZS.Ii2.19701.26	2s												x															
Wybrane zagadnienia matematyki wyższej	ICBZS.Ii2.06039.26	2s	x										x											x					
Projektowanie i analiza algorytmów	ICBZS.Ii2.08318.26	2s	x										x											x					
Język hiszpański B2 - Moduł 1	ICBZS.Ii2.19707.26	2s												x															

Przedmiot	Kod	Semestr	CBZ1A_W01	CBZ1A_W02	CBZ1A_W03	CBZ1A_W04	CBZ1A_W05	CBZ1A_W06	CBZ1A_W07	CBZ1A_W08	CBZ1A_W09	CBZ1A_W10	CBZ1A_U01	CBZ1A_U02	CBZ1A_U03	CBZ1A_U04	CBZ1A_U05	CBZ1A_U06	CBZ1A_U07	CBZ1A_U08	CBZ1A_U09	CBZ1A_U10	CBZ1A_U11	CBZ1A_K01	CBZ1A_K02	CBZ1A_K03	CBZ1A_K04	CBZ1A_K05	CBZ1A_K06
Język niemiecki B2 - Moduł 1	ICBZS.Ii2.19704.26	2s												x															
Probabilistyka i statystyka	ICBZS.Ii2.02915.26	2s	x									x	x		x									x					x
Język rosyjski B2 - Moduł 1	ICBZS.Ii2.19710.26	2s												x															
Matematyka dyskretna	ICBZS.Ii2.00425.26	2s	x										x	x	x					x					x				
Odpowiedzialność prawna za cyberataki i ochronę zasobów	ICBZS.Ii2.18605.26	2s						x	x	x	x										x	x					x	x	x
Język angielski B2 - Moduł 2	ICBZS.Ii4.19699.26	3s												x															
Fizyka 2	ICBZS.Ii4.00058.26	3s	x										x	x	x	x								x					
Język francuski B2 - Moduł 2	ICBZS.Ii4.19702.26	3s												x															
Język hiszpański B2 - Moduł 2	ICBZS.Ii4.19708.26	3s												x															
Kryptografia	ICBZS.Ii4.00756.26	3s	x		x	x	x				x		x				x	x		x				x			x	x	x
Język niemiecki B2 - Moduł 2	ICBZS.Ii4.19705.26	3s												x															
Język rosyjski B2 - Moduł 2	ICBZS.Ii4.19711.26	3s												x															
Bazy danych	ICBZS.Ii4.00396.26	3s			x										x					x					x				x
Bezpieczeństwo lokalnych sieci komputerowych	ICBZS.Ii4.08336.26	3s				x	x						x						x					x					
Informatyka śledcza	ICBZS.Ii4.08324.26	3s			x	x	x											x										x	
Bezpieczeństwo aplikacji internetowych i mobilnych	ICBZS.Ii4.14217.26	3s			x	x						x	x		x	x	x			x					x	x		x	x
Programowanie skryptowe	ICBZS.Ii4.08323.26	3s			x															x				x					
Bezpieczeństwo bezprzewodowych sieci komputerowych	ICBZS.Ii8.08329.26	4s		x		x	x					x	x				x	x	x						x	x			x

Przedmiot	Kod	Semestr	CBZ1A_W01	CBZ1A_W02	CBZ1A_W03	CBZ1A_W04	CBZ1A_W05	CBZ1A_W06	CBZ1A_W07	CBZ1A_W08	CBZ1A_W09	CBZ1A_W10	CBZ1A_U01	CBZ1A_U02	CBZ1A_U03	CBZ1A_U04	CBZ1A_U05	CBZ1A_U06	CBZ1A_U07	CBZ1A_U08	CBZ1A_U09	CBZ1A_U10	CBZ1A_U11	CBZ1A_K01	CBZ1A_K02	CBZ1A_K03	CBZ1A_K04	CBZ1A_K05	CBZ1A_K06
Bezpieczeństwo oprogramowania	ICBZS.Ii8.08330.26	4s		x	x		x					x	x	x			x						x						x
Język angielski B2 - Moduł 3	ICBZS.Ii8.19700.26	4s												x															
Wykrywanie incydentów	ICBZS.Ii8.08320.26	4s									x								x			x							x
Język francuski B2 - Moduł 3	ICBZS.Ii8.19703.26	4s												x															
Analiza złośliwego oprogramowania	ICBZS.Ii8.16556.26	4s			x	x	x											x										x	
Język hiszpański B2 - Moduł 3	ICBZS.Ii8.19709.26	4s												x															
Systemy i sieci komórkowe	ICBZS.Ii8.14288.26	4s	x	x		x	x						x		x		x	x	x					x	x				
Język niemiecki B2 - Moduł 3	ICBZS.Ii8.19706.26	4s												x															
Prywatność i ochrona danych osobowych	ICBZS.Ii8.16555.26	4s				x	x		x		x	x								x		x						x	
Język rosyjski B2 - Moduł 3	ICBZS.Ii8.19712.26	4s												x															
Wprowadzenie do białego wywiadu	ICBZS.Ii8.08351.26	4s									x				x									x				x	
Bezpieczeństwo zwirtualizowanych środowisk IT	ICBZS.Ii10.08355.26	5s				x	x							x	x			x	x			x		x					
Biometria	ICBZS.Ii10.00612.26	5s	x						x		x	x				x	x	x		x	x	x	x		x	x		x	x
Testy penetracyjne	ICBZS.Ii10.08359.26	5s										x						x								x			x
Uczenie maszynowe	ICBZS.Ii10.03622.26	5s	x	x	x								x		x		x								x			x	
Wielkoskalowe systemy dystrybucji danych w sieci Internet	ICBZS.Ii10.06785.26	5s			x	x	x								x			x	x	x				x	x	x	x	x	
Wprowadzenie do inżynierii oprogramowania	ICBZS.Ii10.08367.26	5s	x		x						x	x				x	x			x		x			x	x			
Bezpieczeństwo w sieciach rozległych	ICBZS.Ii10.08353.26	5s				x	x												x					x					

Przedmiot	Kod	Semestr	CBZ1A_W01	CBZ1A_W02	CBZ1A_W03	CBZ1A_W04	CBZ1A_W05	CBZ1A_W06	CBZ1A_W07	CBZ1A_W08	CBZ1A_W09	CBZ1A_W10	CBZ1A_U01	CBZ1A_U02	CBZ1A_U03	CBZ1A_U04	CBZ1A_U05	CBZ1A_U06	CBZ1A_U07	CBZ1A_U08	CBZ1A_U09	CBZ1A_U10	CBZ1A_U11	CBZ1A_K01	CBZ1A_K02	CBZ1A_K03	CBZ1A_K04	CBZ1A_K05	CBZ1A_K06
Inżynieria społeczna	ICBZS.Ii10.08327.26	5s									x				x						x	x			x	x			
Szpiegostwo przemysłowe	ICBZS.Ii10.08326.26	5s						x	x	x											x							x	
Wstęp do zwalczania cyberprzestępczości	ICBZS.Ii10.08325.26	5s							x	x	x				x										x				
Cyberbezpieczeństwo a przetwarzanie danych w chmurze	ICBZS.Ii10.08371.26	5s			x		x					x			x	x		x	x								x		
Bezpieczne transakcje elektroniczne i ochrona klientów	ICBZS.Ii10.17174.26	5s		x		x					x	x	x					x			x	x	x	x	x		x	x	x
Pamięci masowe i ochrona danych	ICBZS.Ii10.18598.26	5s			x	x	x	x			x							x	x	x		x	x		x	x	x		
Programowanie sieciowe wspierające aplikacje bezpieczne	ICBZS.Ii20.08370.26	6s			x	x	x										x	x	x	x				x	x				
Bezpieczeństwo infrastruktury krytycznej	ICBZS.Ii20.16838.26	6s		x			x	x		x	x											x	x	x	x				
Kryptoanaliza	ICBZS.Ii20.08375.26	6s	x		x	x	x				x		x				x	x		x				x		x		x	
Testy penetracyjne zaawansowane	ICBZS.Ii20.15987.26	6s		x			x						x	x	x		x		x									x	x
Metody i narzędzia OSINT	ICBZS.Ii20.19730.26	6s									x		x	x												x		x	x
Steganografia	ICBZS.Ii20.15889.26	6s	x						x	x	x	x	x		x	x					x			x		x			
Praktyka zawodowa	ICBZS.Ii20.00035.26	6s											x	x	x	x	x			x					x	x	x	x	x
Projekty naukowe	ICBZS.Ii20.20015.26	6s		x	x	x	x	x	x		x	x	x	x	x	x					x	x		x			x	x	
Pracownia projektowa	ICBZS.Ii20.05444.26	6s										x	x		x		x	x	x	x	x				x	x	x		
Teoria informacji i kodowania w cyberbezpieczeństwie	ICBZS.Ii20.15891.26	6s	x	x		x	x				x		x			x	x	x							x	x			
Wprowadzenie do informatyki kwantowej	ICBZS.Ii20.08481.26	6s	x				x					x			x		x							x	x	x			

Przedmiot	Kod	Semestr	CBZ1A_W01	CBZ1A_W02	CBZ1A_W03	CBZ1A_W04	CBZ1A_W05	CBZ1A_W06	CBZ1A_W07	CBZ1A_W08	CBZ1A_W09	CBZ1A_W10	CBZ1A_U01	CBZ1A_U02	CBZ1A_U03	CBZ1A_U04	CBZ1A_U05	CBZ1A_U06	CBZ1A_U07	CBZ1A_U08	CBZ1A_U09	CBZ1A_U10	CBZ1A_U11	CBZ1A_K01	CBZ1A_K02	CBZ1A_K03	CBZ1A_K04	CBZ1A_K05	CBZ1A_K06
Analiza powłamaniowa	ICBZS.Ii20.08334.26	6s					x	x	x			x			x							x			x		x		x
Środowisko regulacyjne sieci komórkowych	ICBZS.Ii20.17194.26	6s		x		x			x	x	x		x	x							x	x			x		x		x
Cyberbezpieczeństwo i prawo międzynarodowe	ICBZS.Ii40.08368.26	7s							x	x	x	x			x	x					x			x	x			x	x
Blockchain	ICBZS.Ii40.08374.26	7s	x			x	x									x	x		x	x						x	x		
Warsztaty dyplomowe	ICBZS.Ii40.06764.26	7s									x		x	x		x	x					x		x				x	
Koło naukowe	ICBZS.Ii40.03260.26	7s		x	x	x	x	x	x		x	x	x	x	x	x					x	x		x			x	x	
Secure Communications Systems	ICBZS.Ii40.06768.26	7s		x		x	x						x	x	x			x	x					x					x
Projekt dyplomowy	ICBZS.Ii40.00034.26	7s											x	x	x	x	x	x	x	x		x	x	x		x	x	x	
Ochrona informacji niejawnych	ICBZS.Ii40.08357.26	7s						x	x	x	x	x			x	x		x			x	x	x		x		x		x
Podstawy analizy informacji	ICBZS.Ii40.08328.26	7s						x			x	x	x	x							x	x	x				x		x
Krajowe zasoby informacyjne	ICBZS.Ii40.08369.26	7s							x		x	x									x								x
Organizacje międzynarodowe a cyberbezpieczeństwo	ICBZS.Ii40.08331.26	7s							x	x	x					x					x			x			x	x	
Zagrożenia dla płatności elektronicznych	ICBZS.Ii40.15890.26	7s				x					x	x	x									x	x			x	x	x	
Ethical Hacker	ICBZS.Ii40.17132.26	7s					x				x					x	x	x				x				x		x	x
5G Networks: Advanced	ICBZS.Ii40.18564.26	7s		x		x		x			x			x	x	x	x	x						x	x		x		x
Audyt bezpieczeństwa	ICBZS.Ii40.18599.26	7s							x	x		x									x	x	x		x	x		x	x
Ochrona własności intelektualnej	ICBZS.Ii40.00147.26	7s						x	x		x	x		x							x				x			x	
Suma (obowiązkowy):			12	5	11	13	13	4	5	5	9	9	21	8	14	7	12	11	10	13	5	7	4	22	12	8	8	15	13

Przedmiot	Kod	Semestr	CBZ1A_W01	CBZ1A_W02	CBZ1A_W03	CBZ1A_W04	CBZ1A_W05	CBZ1A_W06	CBZ1A_W07	CBZ1A_W08	CBZ1A_W09	CBZ1A_W10	CBZ1A_U01	CBZ1A_U02	CBZ1A_U03	CBZ1A_U04	CBZ1A_U05	CBZ1A_U06	CBZ1A_U07	CBZ1A_U08	CBZ1A_U09	CBZ1A_U10	CBZ1A_U11	CBZ1A_K01	CBZ1A_K02	CBZ1A_K03	CBZ1A_K04	CBZ1A_K05	CBZ1A_K06
Suma (fakultatywny):			7	8	7	13	14	8	13	7	21	16	11	24	15	13	9	12	7	6	14	15	7	12	16	13	14	13	13
Suma:			19	13	18	26	27	12	18	12	30	25	32	32	29	20	21	23	17	19	19	22	11	34	28	21	22	28	26

Matryca charakterystyk efektów uczenia się w odniesieniu do modułów zajęć

Kierunek: Cyberbezpieczeństwo

2026/2027/S/Ii/IEiT/CBZ/all

Przedmiot	Kod	Semestr	P6S_WG_A	P6S_WG_A_Inz	P6S_WK_A	P6S_WK_A_Inz	P6S_UW_A	P6S_UK_A	P6S_UO_A	P6S_UU_A	P6S_UW_A_Inz_01	P6S_UW_A_Inz_02	P6S_KK_A	P6S_KO_A	P6S_KR_A
Algebra	ICBZS.Ii1.00371.26	1s	x								x	x	x		x
Analiza matematyczna	ICBZS.Ii1.00773.26	1s	x				x						x		
Wprowadzenie do sieci Internet	ICBZS.Ii1.02353.26	1s		x					x					x	
Podstawy programowania	ICBZS.Ii1.01049.26	1s	x	x								x	x	x	
Architektura komputerów i systemy operacyjne	ICBZS.Ii1.16552.26	1s	x	x	x							x	x		
Zarządzanie bezpieczeństwem informacji	ICBZS.Ii1.08321.26	1s			x	x	x	x	x				x	x	x
Krajowy system cyberbezpieczeństwa	ICBZS.Ii1.08314.26	1s			x			x	x	x			x	x	x
Fizyka 1	ICBZS.Ii2.00318.26	2s	x				x	x	x	x			x		
Język angielski B2 - Moduł 1	ICBZS.Ii2.19698.26	2s						x							
Bezpieczeństwo systemów i sieci teleinformatycznych	ICBZS.Ii2.08319.26	2s	x	x			x					x	x	x	
Język francuski B2 - Moduł 1	ICBZS.Ii2.19701.26	2s						x							
Wybrane zagadnienia matematyki wyższej	ICBZS.Ii2.06039.26	2s	x				x						x		
Projektowanie i analiza algorytmów	ICBZS.Ii2.08318.26	2s	x				x						x		
Język hiszpański B2 - Moduł 1	ICBZS.Ii2.19707.26	2s						x							
Język niemiecki B2 - Moduł 1	ICBZS.Ii2.19704.26	2s						x							

Przedmiot	Kod	Semestr	P6S_WG_A	P6S_WG_A_Inz	P6S_WK_A	P6S_WK_A_Inz	P6S_UW_A	P6S_UK_A	P6S_UO_A	P6S_UU_A	P6S_UW_A_Inz_01	P6S_UW_A_Inz_02	P6S_KK_A	P6S_KO_A	P6S_KR_A
Probabilistyka i statystyka	ICBZS.li2.02915.26	2s	x		x		x		x				x	x	
Język rosyjski B2 - Moduł 1	ICBZS.li2.19710.26	2s						x							
Matematyka dyskretna	ICBZS.li2.00425.26	2s	x				x	x	x			x		x	
Odpowiedzialność prawna za cyberataki i ochronę zasobów	ICBZS.li2.18605.26	2s			x	x	x	x	x					x	x
Język angielski B2 - Moduł 2	ICBZS.li4.19699.26	3s						x							
Fizyka 2	ICBZS.li4.00058.26	3s	x				x	x	x	x			x		
Język francuski B2 - Moduł 2	ICBZS.li4.19702.26	3s						x							
Język hiszpański B2 - Moduł 2	ICBZS.li4.19708.26	3s						x							
Kryptografia	ICBZS.li4.00756.26	3s	x	x	x		x				x	x	x	x	x
Język niemiecki B2 - Moduł 2	ICBZS.li4.19705.26	3s						x							
Język rosyjski B2 - Moduł 2	ICBZS.li4.19711.26	3s						x							
Bazy danych	ICBZS.li4.00396.26	3s	x	x					x			x		x	
Bezpieczeństwo lokalnych sieci komputerowych	ICBZS.li4.08336.26	3s		x			x					x	x		
Informatyka śledcza	ICBZS.li4.08324.26	3s	x	x								x			x
Bezpieczeństwo aplikacji internetowych i mobilnych	ICBZS.li4.14217.26	3s	x	x	x		x		x	x	x	x		x	x
Programowanie skryptowe	ICBZS.li4.08323.26	3s	x	x								x	x		
Bezpieczeństwo bezprzewodowych sieci komputerowych	ICBZS.li8.08329.26	4s	x	x	x		x				x	x		x	x
Bezpieczeństwo oprogramowania	ICBZS.li8.08330.26	4s	x	x	x		x	x			x			x	
Język angielski B2 - Moduł 3	ICBZS.li8.19700.26	4s						x							

Przedmiot	Kod	Semestr	P6S_WG_A	P6S_WG_A_Inz	P6S_WK_A	P6S_WK_A_Inz	P6S_UW_A	P6S_UK_A	P6S_UO_A	P6S_UU_A	P6S_UW_A_Inz_01	P6S_UW_A_Inz_02	P6S_KK_A	P6S_KO_A	P6S_KR_A
Wykrywanie incydentów	ICBZS.li8.08320.26	4s			x		x					x		x	
Język francuski B2 - Moduł 3	ICBZS.li8.19703.26	4s						x							
Analiza złośliwego oprogramowania	ICBZS.li8.16556.26	4s	x	x								x			x
Język hiszpański B2 - Moduł 3	ICBZS.li8.19709.26	4s						x							
Systemy i sieci komórkowe	ICBZS.li8.14288.26	4s	x	x			x		x		x	x	x	x	
Język niemiecki B2 - Moduł 3	ICBZS.li8.19706.26	4s						x							
Prywatność i ochrona danych osobowych	ICBZS.li8.16555.26	4s		x	x		x					x			x
Język rosyjski B2 - Moduł 3	ICBZS.li8.19712.26	4s						x							
Wprowadzenie do białego wywiadu	ICBZS.li8.08351.26	4s			x				x				x		x
Bezpieczeństwo zwirtualizowanych środowisk IT	ICBZS.li10.08355.26	5s		x			x	x	x			x	x		
Biometria	ICBZS.li10.00612.26	5s	x		x		x	x	x	x	x	x		x	x
Testy penetracyjne	ICBZS.li10.08359.26	5s			x							x		x	x
Uczenie maszynowe	ICBZS.li10.03622.26	5s	x	x			x		x		x			x	x
Wielkoskalowe systemy dystrybucji danych w sieci Internet	ICBZS.li10.06785.26	5s	x	x					x			x	x	x	x
Wprowadzenie do inżynierii oprogramowania	ICBZS.li10.08367.26	5s	x	x	x		x			x	x	x		x	x
Bezpieczeństwo w sieciach rozległych	ICBZS.li10.08353.26	5s		x								x	x		
Inżynieria społeczna	ICBZS.li10.08327.26	5s			x		x	x	x					x	x
Szpiegostwo przemysłowe	ICBZS.li10.08326.26	5s			x	x		x	x						x
Wstęp do zwalczania cyberprzestępczości	ICBZS.li10.08325.26	5s			x				x					x	

Przedmiot	Kod	Semestr	P6S_WG_A	P6S_WG_A_Inz	P6S_WK_A	P6S_WK_A_Inz	P6S_UW_A	P6S_UK_A	P6S_UO_A	P6S_UU_A	P6S_UW_A_Inz_01	P6S_UW_A_Inz_02	P6S_KK_A	P6S_KO_A	P6S_KR_A
Cyberbezpieczeństwo a przetwarzanie danych w chmurze	ICBZS.li10.08371.26	5s	x	x	x				x	x		x		x	
Bezpieczne transakcje elektroniczne i ochrona klientów	ICBZS.li10.17174.26	5s	x	x	x		x	x	x			x	x	x	x
Pamięci masowe i ochrona danych	ICBZS.li10.18598.26	5s	x	x	x	x	x	x				x		x	x
Programowanie sieciowe wspierające aplikacje bezpieczne	ICBZS.li20.08370.26	6s	x	x							x	x	x	x	
Bezpieczeństwo infrastruktury krytycznej	ICBZS.li20.16838.26	6s	x	x	x	x	x	x					x	x	
Kryptoanaliza	ICBZS.li20.08375.26	6s	x	x	x		x				x	x	x		x
Testy penetracyjne zaawansowane	ICBZS.li20.15987.26	6s	x	x			x	x	x		x	x		x	x
Metody i narzędzia OSINT	ICBZS.li20.19730.26	6s			x		x	x						x	x
Steganografia	ICBZS.li20.15889.26	6s	x		x		x	x	x	x			x		x
Praktyka zawodowa	ICBZS.li20.00035.26	6s					x	x	x	x	x	x		x	x
Projekty naukowe	ICBZS.li20.20015.26	6s	x	x	x	x	x	x	x	x			x	x	x
Pracownia projektowa	ICBZS.li20.05444.26	6s			x		x	x	x		x	x		x	x
Teoria informacji i kodowania w cyberbezpieczeństwie	ICBZS.li20.15891.26	6s	x	x	x		x			x	x	x		x	x
Wprowadzenie do informatyki kwantowej	ICBZS.li20.08481.26	6s	x	x	x				x		x		x	x	x
Analiza powłamaniowa	ICBZS.li20.08334.26	6s		x	x	x	x		x					x	
Środowisko regulacyjne sieci komórkowych	ICBZS.li20.17194.26	6s	x	x	x		x	x	x					x	
Cyberbezpieczeństwo i prawo międzynarodowe	ICBZS.li40.08368.26	7s			x			x	x	x			x	x	x
Blockchain	ICBZS.li40.08374.26	7s	x	x						x	x	x		x	x
Warsztaty dyplomowe	ICBZS.li40.06764.26	7s			x		x	x		x	x		x		x

Przedmiot	Kod	Semestr	P6S_WG_A	P6S_WG_A_Inz	P6S_WK_A	P6S_WK_A_Inz	P6S_UW_A	P6S_UK_A	P6S_UO_A	P6S_UU_A	P6S_UW_A_Inz_01	P6S_UW_A_Inz_02	P6S_KK_A	P6S_KO_A	P6S_KR_A
Koło naukowe	ICBZS.li40.03260.26	7s	x	x	x	x	x	x	x	x			x	x	x
Secure Communications Systems	ICBZS.li40.06768.26	7s	x	x			x	x	x			x	x	x	
Projekt dyplomowy	ICBZS.li40.00034.26	7s					x	x	x	x	x	x	x	x	x
Ochrona informacji niejawnych	ICBZS.li40.08357.26	7s			x	x	x	x	x	x		x		x	
Podstawy analizy informacji	ICBZS.li40.08328.26	7s			x	x	x	x	x					x	
Krajowe zasoby informacyjne	ICBZS.li40.08369.26	7s			x			x	x					x	
Organizacje międzynarodowe a cyberbezpieczeństwo	ICBZS.li40.08331.26	7s			x			x	x	x			x	x	x
Zagrożenia dla płatności elektronicznych	ICBZS.li40.15890.26	7s		x	x		x	x						x	x
Ethical Hacker	ICBZS.li40.17132.26	7s		x	x		x			x	x	x		x	x
5G Networks: Advanced	ICBZS.li40.18564.26	7s	x	x	x	x		x	x	x	x	x	x	x	
Audyt bezpieczeństwa	ICBZS.li40.18599.26	7s			x		x	x	x					x	x
Ochrona własności intelektualnej	ICBZS.li40.00147.26	7s			x	x		x	x					x	x
Suma (obowiązkowy):			23	19	18	4	25	14	17	7	12	22	22	23	19
Suma (fakultatywny):			17	19	25	8	20	35	23	13	9	15	12	27	20
Suma:			40	38	43	12	45	49	40	20	21	37	34	50	39

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

Kierunek: Cyberbezpieczeństwo

2026/2027/S/Ii/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
Algebra	Wykład, Ćwiczenia audytoryjne	Egzamin, Aktywność na zajęciach	CBZ1A_W01, CBZ1A_U05, CBZ1A_U06, CBZ1A_U08, CBZ1A_K01, CBZ1A_K03
Analiza matematyczna	Wykład, Ćwiczenia audytoryjne	Aktywność na zajęciach, Kolokwium, Egzamin, Odpowiedź ustna	CBZ1A_W01, CBZ1A_U01, CBZ1A_K01
Wprowadzenie do sieci Internet	Wykład, Ćwiczenia laboratoryjne	Wykonanie ćwiczeń laboratoryjnych, Egzamin, Zaliczenie laboratorium	CBZ1A_W04, CBZ1A_U03, CBZ1A_K02
Podstawy programowania	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń laboratoryjnych, Zaliczenie laboratorium	CBZ1A_W03, CBZ1A_U08, CBZ1A_K01, CBZ1A_K02
Architektura komputerów i systemy operacyjne	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych	CBZ1A_W05, CBZ1A_W03, CBZ1A_W04, CBZ1A_W10, CBZ1A_U07, CBZ1A_U08, CBZ1A_K01
Zarządzanie bezpieczeństwem informacji	Wykład, Ćwiczenia projektowe	Aktywność na zajęciach, Udział w dyskusji, Prezentacja, Projekt, Zaangażowanie w pracę zespołu, Odpowiedź ustna	CBZ1A_W06, CBZ1A_W07, CBZ1A_W08, CBZ1A_W10, CBZ1A_U01, CBZ1A_U03, CBZ1A_U10, CBZ1A_U11, CBZ1A_U09, CBZ1A_K01, CBZ1A_K04, CBZ1A_K05, CBZ1A_K06
Krajowy system cyberbezpieczeństwa	Wykład, Zajęcia seminaryjne	Aktywność na zajęciach, Udział w dyskusji, Wynik testu zaliczeniowego, Odpowiedź ustna	CBZ1A_W07, CBZ1A_W08, CBZ1A_W09, CBZ1A_U04, CBZ1A_U09, CBZ1A_K01, CBZ1A_K04, CBZ1A_K06, CBZ1A_K05
Fizyka 1	Wykład, Ćwiczenia audytoryjne	Aktywność na zajęciach, Kolokwium, Egzamin, Odpowiedź ustna, Udział w dyskusji, Wykonanie ćwiczeń, Wynik testu zaliczeniowego	CBZ1A_W01, CBZ1A_U01, CBZ1A_U02, CBZ1A_U03, CBZ1A_U04, CBZ1A_K01
Język angielski B2 - Moduł 1	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Wypracowania pisane na zajęciach, Prezentacja, Odpowiedź ustna	CBZ1A_U02

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
Bezpieczeństwo systemów i sieci teleinformatycznych	Wykład, Ćwiczenia laboratoryjne	Wykonanie ćwiczeń laboratoryjnych, Egzamin, Sprawozdanie, Zaliczenie laboratorium	CBZ1A_W01, CBZ1A_W04, CBZ1A_W05, CBZ1A_U01, CBZ1A_U06, CBZ1A_U07, CBZ1A_K01, CBZ1A_K04
Język francuski B2 - Moduł 1	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Wypracowania pisane na zajęciach, Prezentacja, Odpowiedź ustna	CBZ1A_U02
Wybrane zagadnienia matematyki wyższej	Wykład, Ćwiczenia audytoryjne	Aktywność na zajęciach, Kolokwium, Egzamin, Odpowiedź ustna	CBZ1A_W01, CBZ1A_U01, CBZ1A_K01
Projektowanie i analiza algorytmów	Wykład, Ćwiczenia laboratoryjne	Egzamin, Aktywność na zajęciach, Kolokwium	CBZ1A_W01, CBZ1A_U01, CBZ1A_K01
Język hiszpański B2 - Moduł 1	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Wypracowania pisane na zajęciach, Prezentacja, Odpowiedź ustna	CBZ1A_U02
Język niemiecki B2 - Moduł 1	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Wypracowania pisane na zajęciach, Prezentacja, Odpowiedź ustna	CBZ1A_U02
Probabilistyka i statystyka	Wykład, Ćwiczenia audytoryjne	Aktywność na zajęciach, Kolokwium, Udział w dyskusji	CBZ1A_W01, CBZ1A_W10, CBZ1A_U01, CBZ1A_U03, CBZ1A_K01, CBZ1A_K06
Język rosyjski B2 - Moduł 1	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Wypracowania pisane na zajęciach, Prezentacja, Odpowiedź ustna	CBZ1A_U02
Matematyka dyskretna	Wykład, Ćwiczenia audytoryjne	Aktywność na zajęciach, Kolokwium, Odpowiedź ustna	CBZ1A_W01, CBZ1A_U02, CBZ1A_U03, CBZ1A_U01, CBZ1A_U08, CBZ1A_K02
Odpowiedzialność prawna za cyberataki i ochronę zasobów	Wykład, Ćwiczenia audytoryjne	Udział w dyskusji, Kolokwium, Aktywność na zajęciach	CBZ1A_W06, CBZ1A_W07, CBZ1A_W08, CBZ1A_W09, CBZ1A_U09, CBZ1A_U10, CBZ1A_K04, CBZ1A_K05, CBZ1A_K06
Język angielski B2 - Moduł 2	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Wypracowania pisane na zajęciach, Prezentacja, Odpowiedź ustna	CBZ1A_U02
Fizyka 2	Wykład, Ćwiczenia audytoryjne, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wynik testu zaliczeniowego, Odpowiedź ustna	CBZ1A_W01, CBZ1A_U01, CBZ1A_U02, CBZ1A_U03, CBZ1A_U04, CBZ1A_K01

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 francuski B2 - Moduł 2	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Wypracowania pisane na zajęciach, Prezentacja, Odpowiedź ustna	CBZ1A_U02
Język hiszpański B2 - Moduł 2	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Wypracowania pisane na zajęciach, Prezentacja, Odpowiedź ustna	CBZ1A_U02
Kryptografia	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Egzamin, Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych, Kolokwium, Sprawozdanie, Referat	CBZ1A_W01, CBZ1A_W03, CBZ1A_W04, CBZ1A_W05, CBZ1A_W09, CBZ1A_K05, CBZ1A_U01, CBZ1A_U08, CBZ1A_U05, CBZ1A_U06, CBZ1A_K01, CBZ1A_K04, CBZ1A_K06
Język niemiecki B2 - Moduł 2	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Wypracowania pisane na zajęciach, Prezentacja, Odpowiedź ustna	CBZ1A_U02
Język rosyjski B2 - Moduł 2	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Wypracowania pisane na zajęciach, Prezentacja, Odpowiedź ustna	CBZ1A_U02
Bazy danych	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Egzamin, Kolokwium, Projekt, Prezentacja	CBZ1A_W03, CBZ1A_U08, CBZ1A_U03, CBZ1A_K02, CBZ1A_K06
Bezpieczeństwo lokalnych sieci komputerowych	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Egzamin, Zaliczenie laboratorium	CBZ1A_W04, CBZ1A_W05, CBZ1A_U01, CBZ1A_U07, CBZ1A_K01
Informatyka śledcza	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Wykonanie projektu, Wykonanie ćwiczeń laboratoryjnych	CBZ1A_W05, CBZ1A_W03, CBZ1A_W04, CBZ1A_U06, CBZ1A_K05
Bezpieczeństwo aplikacji internetowych i mobilnych	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Wykonanie ćwiczeń laboratoryjnych, Projekt, Aktywność na zajęciach, Zaliczenie laboratorium, Wykonanie projektu, Zaangażowanie w pracę zespołu, Prezentacja	CBZ1A_W03, CBZ1A_W04, CBZ1A_W10, CBZ1A_U01, CBZ1A_U03, CBZ1A_U05, CBZ1A_U04, CBZ1A_U08, CBZ1A_K02, CBZ1A_K05, CBZ1A_K06, CBZ1A_K03
Programowanie skryptowe	Wykład, Ćwiczenia laboratoryjne	Zaliczenie laboratorium, Wykonanie ćwiczeń laboratoryjnych	CBZ1A_W03, CBZ1A_U08, CBZ1A_K01
Bezpieczeństwo bezprzewodowych sieci komputerowych	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Aktywność na zajęciach, Egzamin, Wykonanie ćwiczeń laboratoryjnych, Kolokwium, Projekt, Zaangażowanie w pracę zespołu	CBZ1A_W02, CBZ1A_W04, CBZ1A_W05, CBZ1A_W10, CBZ1A_U05, CBZ1A_U06, CBZ1A_U07, CBZ1A_U01, CBZ1A_K02, CBZ1A_K03, CBZ1A_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
Bezpieczeństwo oprogramowania	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Egzamin, Wykonanie ćwiczeń laboratoryjnych	CBZ1A_W03, CBZ1A_W05, CBZ1A_W02, CBZ1A_W10, CBZ1A_U01, CBZ1A_U11, CBZ1A_U02, CBZ1A_U05, CBZ1A_K06
Język angielski B2 - Moduł 3	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wypracowania pisane na zajęciach, Prezentacja, Odpowiedź ustna	CBZ1A_U02
Wykrywanie incydentów	Wykład, Ćwiczenia laboratoryjne	Wykonanie ćwiczeń laboratoryjnych, Kolokwium	CBZ1A_W09, CBZ1A_U10, CBZ1A_U07, CBZ1A_K06
Język francuski B2 - Moduł 3	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wypracowania pisane na zajęciach, Prezentacja, Odpowiedź ustna	CBZ1A_U02
Analiza złośliwego oprogramowania	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Aktywność na zajęciach, Projekt, Wykonanie ćwiczeń laboratoryjnych, Wykonanie projektu, Zaangażowanie w pracę zespołu	CBZ1A_W03, CBZ1A_W04, CBZ1A_W05, CBZ1A_U06, CBZ1A_K05
Język hiszpański B2 - Moduł 3	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wypracowania pisane na zajęciach, Prezentacja, Odpowiedź ustna	CBZ1A_U02
Systemy i sieci komórkowe	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Aktywność na zajęciach, Wynik testu zaliczeniowego, Wykonanie projektu, Wykonanie ćwiczeń laboratoryjnych, Kolokwium, Projekt, Prezentacja, Odpowiedź ustna, Zaliczenie laboratorium, Sprawozdanie, Zaangażowanie w pracę zespołu	CBZ1A_W02, CBZ1A_W04, CBZ1A_W05, CBZ1A_W01, CBZ1A_U01, CBZ1A_U03, CBZ1A_U05, CBZ1A_U06, CBZ1A_U07, CBZ1A_K01, CBZ1A_K02
Język niemiecki B2 - Moduł 3	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wypracowania pisane na zajęciach, Prezentacja, Odpowiedź ustna	CBZ1A_U02
Prywatność i ochrona danych osobowych	Wykład, Ćwiczenia projektowe	Aktywność na zajęciach, Projekt, Studium przypadków	CBZ1A_W07, CBZ1A_W09, CBZ1A_W10, CBZ1A_W04, CBZ1A_W05, CBZ1A_U08, CBZ1A_U10, CBZ1A_K05
Język rosyjski B2 - Moduł 3	Lektorat	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wypracowania pisane na zajęciach, Prezentacja, Odpowiedź ustna	CBZ1A_U02
Wprowadzenie do białego wywiadu	Wykład, Ćwiczenia projektowe	Aktywność na zajęciach, Projekt	CBZ1A_W09, CBZ1A_U03, CBZ1A_K01, CBZ1A_K05

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
Bezpieczeństwo zwirtualizowanych środowisk IT	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Kolokwium, Wykonanie projektu, Wykonanie ćwiczeń laboratoryjnych	CBZ1A_W04, CBZ1A_W05, CBZ1A_U03, CBZ1A_U07, CBZ1A_U02, CBZ1A_U06, CBZ1A_U10, CBZ1A_K01
Biometria	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Udział w dyskusji, Wykonanie ćwiczeń laboratoryjnych, Kolokwium, Prezentacja, Wykonanie projektu, Projekt, Sprawozdanie	CBZ1A_W01, CBZ1A_W07, CBZ1A_W09, CBZ1A_W10, CBZ1A_U04, CBZ1A_U09, CBZ1A_U05, CBZ1A_U08, CBZ1A_U06, CBZ1A_U10, CBZ1A_U11, CBZ1A_K02, CBZ1A_K06, CBZ1A_K03, CBZ1A_K05
Testy penetracyjne	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Wykonanie projektu, Wykonanie ćwiczeń laboratoryjnych, Egzamin	CBZ1A_W10, CBZ1A_U06, CBZ1A_K03, CBZ1A_K06
Uczenie maszynowe	Wykład, Ćwiczenia laboratoryjne	Egzamin, Kolokwium, Przygotowanie i przeprowadzenie badań	CBZ1A_W01, CBZ1A_W03, CBZ1A_W02, CBZ1A_U01, CBZ1A_U03, CBZ1A_U05, CBZ1A_K02, CBZ1A_K05
Wielkoskalowe systemy dystrybucji danych w sieci Internet	Wykład, Ćwiczenia audytoryjne	Kolokwium, Wykonanie ćwiczeń, Zaangażowanie w pracę zespołu	CBZ1A_W04, CBZ1A_W05, CBZ1A_W03, CBZ1A_U03, CBZ1A_U06, CBZ1A_U07, CBZ1A_U08, CBZ1A_K01, CBZ1A_K02, CBZ1A_K03, CBZ1A_K04, CBZ1A_K05
Wprowadzenie do inżynierii oprogramowania	Zajęcia seminaryjne, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Aktywność na zajęciach, Kolokwium, Wykonanie ćwiczeń laboratoryjnych, Wykonanie projektu, Prezentacja	CBZ1A_W01, CBZ1A_W03, CBZ1A_W09, CBZ1A_W10, CBZ1A_U04, CBZ1A_U08, CBZ1A_U05, CBZ1A_U10, CBZ1A_K02, CBZ1A_K03
Bezpieczeństwo w sieciach rozległych	Ćwiczenia laboratoryjne	Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych, Egzamin, Studium przypadków	CBZ1A_W04, CBZ1A_W05, CBZ1A_U07, CBZ1A_K01
Inżynieria społeczna	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Kolokwium, Prezentacja	CBZ1A_W09, CBZ1A_U03, CBZ1A_U10, CBZ1A_U09, CBZ1A_K02, CBZ1A_K03
Szpiegostwo przemysłowe	Wykład, Ćwiczenia projektowe	Odpowiedź ustna, Udział w dyskusji	CBZ1A_W06, CBZ1A_W07, CBZ1A_W08, CBZ1A_U09, CBZ1A_K05
Wstęp do zwalczania cyberprzestępczości	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Aktywność na zajęciach, Udział w dyskusji, Projekt	CBZ1A_W09, CBZ1A_W07, CBZ1A_W08, CBZ1A_U03, CBZ1A_K02
Cyberbezpieczeństwo a przetwarzanie danych w chmurze	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Wykonanie projektu, Wykonanie ćwiczeń laboratoryjnych, Kolokwium	CBZ1A_W05, CBZ1A_W03, CBZ1A_W10, CBZ1A_U07, CBZ1A_U06, CBZ1A_U03, CBZ1A_U04, CBZ1A_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
Bezpieczne transakcje elektroniczne i ochrona klientów	Wykład, Ćwiczenia projektowe	Aktywność na zajęciach, Wynik testu zaliczeniowego, Projekt	CBZ1A_W04, CBZ1A_W09, CBZ1A_W10, CBZ1A_W02, CBZ1A_U01, CBZ1A_U09, CBZ1A_U10, CBZ1A_U06, CBZ1A_U11, CBZ1A_K01, CBZ1A_K02, CBZ1A_K05, CBZ1A_K04, CBZ1A_K06
Pamięci masowe i ochrona danych	Wykład, Ćwiczenia projektowe	Aktywność na zajęciach, Udział w dyskusji, Wykonanie projektu, Sprawozdanie, Zaangażowanie w pracę zespołu, Prezentacja	CBZ1A_W05, CBZ1A_W04, CBZ1A_W03, CBZ1A_W06, CBZ1A_W09, CBZ1A_U07, CBZ1A_U06, CBZ1A_U08, CBZ1A_U11, CBZ1A_U10, CBZ1A_K02, CBZ1A_K03, CBZ1A_K04
Programowanie sieciowe wspierające aplikacje bezpieczne	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Aktywność na zajęciach, Egzamin, Wykonanie ćwiczeń laboratoryjnych, Kolokwium, Projekt, Sprawozdanie, Zaangażowanie w pracę zespołu	CBZ1A_W04, CBZ1A_W05, CBZ1A_W03, CBZ1A_U06, CBZ1A_U08, CBZ1A_U07, CBZ1A_U05, CBZ1A_K01, CBZ1A_K02
Bezpieczeństwo infrastruktury krytycznej	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Aktywność na zajęciach, Egzamin, Wykonanie ćwiczeń laboratoryjnych, Zaliczenie laboratorium, Udział w dyskusji, Wykonanie projektu, Odpowiedź ustna	CBZ1A_W06, CBZ1A_W08, CBZ1A_W09, CBZ1A_W02, CBZ1A_W05, CBZ1A_U11, CBZ1A_U10, CBZ1A_K01, CBZ1A_K02
Kryptoanaliza	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Aktywność na zajęciach, Wynik testu zaliczeniowego, Wykonanie ćwiczeń laboratoryjnych, Projekt	CBZ1A_W01, CBZ1A_W03, CBZ1A_W05, CBZ1A_W04, CBZ1A_W09, CBZ1A_K05, CBZ1A_U01, CBZ1A_U08, CBZ1A_U05, CBZ1A_U06, CBZ1A_K01, CBZ1A_K03
Testy penetracyjne zaawansowane	Wykład, Ćwiczenia laboratoryjne	Kolokwium, Wykonanie ćwiczeń laboratoryjnych, Prezentacja	CBZ1A_W02, CBZ1A_W05, CBZ1A_U07, CBZ1A_U05, CBZ1A_U02, CBZ1A_U03, CBZ1A_U01, CBZ1A_K05, CBZ1A_K06
Metody i narzędzia OSINT	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Udział w dyskusji, Zaliczenie laboratorium, Wykonanie ćwiczeń laboratoryjnych	CBZ1A_W09, CBZ1A_U01, CBZ1A_U02, CBZ1A_K03, CBZ1A_K05, CBZ1A_K06
Steganografia	Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe	Prezentacja, Wykonanie ćwiczeń laboratoryjnych, Projekt	CBZ1A_W01, CBZ1A_W10, CBZ1A_W07, CBZ1A_W09, CBZ1A_W08, CBZ1A_U01, CBZ1A_U03, CBZ1A_U04, CBZ1A_U09, CBZ1A_K01, CBZ1A_K03
Praktyka zawodowa	Praktyka zawodowa	Prezentacja, Udział w pracach badawczych, konferencjach, dodatkowych stażach i szkoleniach, Przygotowanie i przeprowadzenie badań	CBZ1A_U01, CBZ1A_U02, CBZ1A_U05, CBZ1A_U08, CBZ1A_U03, CBZ1A_U04, CBZ1A_K02, CBZ1A_K03, CBZ1A_K05, CBZ1A_K06, CBZ1A_K04
Projekty naukowe	Ćwiczenia projektowe, Konwersatorium	Koordynacja, realizacja projektu badawczego, przygotowanie referatu/publikacji, organizacja konferencji, obozów i wycieczek naukowych	CBZ1A_W07, CBZ1A_W09, CBZ1A_W10, CBZ1A_W02, CBZ1A_W03, CBZ1A_W04, CBZ1A_W05, CBZ1A_W06, CBZ1A_U03, CBZ1A_U10, CBZ1A_U02, CBZ1A_U04, CBZ1A_U09, CBZ1A_U01, CBZ1A_K01, CBZ1A_K04, CBZ1A_K05

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
Pracownia projektowa	Ćwiczenia projektowe	Projekt	CBZ1A_W10, CBZ1A_U01, CBZ1A_U03, CBZ1A_U05, CBZ1A_U08, CBZ1A_U09, CBZ1A_U06, CBZ1A_U07, CBZ1A_K02, CBZ1A_K03, CBZ1A_K04
Teoria informacji i kodowania w cyberbezpieczeństwie	Wykład, Ćwiczenia audytoryjne, Ćwiczenia projektowe	Wykonanie ćwiczeń, Projekt, Udział w dyskusji, Odpowiedź ustna, Wykonanie projektu, Sprawozdanie, Zaangażowanie w pracę zespołu	CBZ1A_W01, CBZ1A_W02, CBZ1A_W04, CBZ1A_W05, CBZ1A_W09, CBZ1A_U01, CBZ1A_U04, CBZ1A_U06, CBZ1A_U05, CBZ1A_K02, CBZ1A_K03
Wprowadzenie do informatyki kwantowej	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach	CBZ1A_W01, CBZ1A_W05, CBZ1A_W10, CBZ1A_U03, CBZ1A_U05, CBZ1A_K01, CBZ1A_K02, CBZ1A_K03
Analiza powłamaniowa	Wykład, Ćwiczenia projektowe	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń	CBZ1A_W05, CBZ1A_W06, CBZ1A_W07, CBZ1A_W10, CBZ1A_U03, CBZ1A_U10, CBZ1A_K02, CBZ1A_K04, CBZ1A_K06
Środowisko regulacyjne sieci komórkowych	Wykład, Ćwiczenia projektowe	Aktywność na zajęciach, Wynik testu zaliczeniowego, Wykonanie projektu, Sprawozdanie, Zaangażowanie w pracę zespołu, Prezentacja, Odpowiedź ustna	CBZ1A_W02, CBZ1A_W04, CBZ1A_W07, CBZ1A_W08, CBZ1A_W09, CBZ1A_U01, CBZ1A_U02, CBZ1A_U09, CBZ1A_U10, CBZ1A_K02, CBZ1A_K04, CBZ1A_K06
Cyberbezpieczeństwo i prawo międzynarodowe	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń laboratoryjnych, Kolokwium, Odpowiedź ustna	CBZ1A_W07, CBZ1A_W08, CBZ1A_W09, CBZ1A_W10, CBZ1A_U03, CBZ1A_U04, CBZ1A_U09, CBZ1A_K01, CBZ1A_K02, CBZ1A_K05, CBZ1A_K06
Blockchain	Wykład, Ćwiczenia projektowe	Wykonanie projektu, Projekt	CBZ1A_W04, CBZ1A_W05, CBZ1A_W01, CBZ1A_U04, CBZ1A_U05, CBZ1A_U07, CBZ1A_U08, CBZ1A_K03, CBZ1A_K04
Warsztaty dyplomowe	Wykład, Ćwiczenia projektowe	Dyskusja nad wynikami pracy, Prezentacja	CBZ1A_W09, CBZ1A_U02, CBZ1A_U01, CBZ1A_U04, CBZ1A_U05, CBZ1A_U10, CBZ1A_K01, CBZ1A_K05
Koło naukowe	Praca w kole naukowym	Wykonanie projektu, Projekt, Prezentacja, Udział w pracach badawczych, konferencjach, dodatkowych stażach i szkoleniach	CBZ1A_W07, CBZ1A_W09, CBZ1A_W10, CBZ1A_W02, CBZ1A_W03, CBZ1A_W04, CBZ1A_W05, CBZ1A_W06, CBZ1A_U03, CBZ1A_U10, CBZ1A_U02, CBZ1A_U04, CBZ1A_U09, CBZ1A_U01, CBZ1A_K01, CBZ1A_K04, CBZ1A_K05
Secure Communications Systems	Wykład, Ćwiczenia projektowe	Kolokwium, Projekt, Prezentacja	CBZ1A_W02, CBZ1A_W04, CBZ1A_W05, CBZ1A_U01, CBZ1A_U02, CBZ1A_U03, CBZ1A_U06, CBZ1A_U07, CBZ1A_K01, CBZ1A_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
Projekt dyplomowy	Praca dyplomowa	Wykonanie projektu	CBZ1A_U01, CBZ1A_U02, CBZ1A_U03, CBZ1A_U04, CBZ1A_U05, CBZ1A_U06, CBZ1A_U07, CBZ1A_U10, CBZ1A_U11, CBZ1A_U08, CBZ1A_K03, CBZ1A_K04, CBZ1A_K01, CBZ1A_K05
Ochrona informacji niejawnych	Wykład, Ćwiczenia audytoryjne	Udział w dyskusji, Wykonanie ćwiczeń, Odpowiedź ustna, Aktywność na zajęciach	CBZ1A_W06, CBZ1A_W07, CBZ1A_W08, CBZ1A_W09, CBZ1A_W10, CBZ1A_U06, CBZ1A_U09, CBZ1A_U10, CBZ1A_U03, CBZ1A_U04, CBZ1A_U11, CBZ1A_K02, CBZ1A_K04, CBZ1A_K06
Podstawy analizy informacji	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Udział w dyskusji, Odpowiedź ustna	CBZ1A_W09, CBZ1A_W10, CBZ1A_W06, CBZ1A_U01, CBZ1A_U02, CBZ1A_U09, CBZ1A_U10, CBZ1A_U11, CBZ1A_K04, CBZ1A_K06
Krajowe zasoby informacyjne	Wykład, Ćwiczenia laboratoryjne	Odpowiedź ustna, Udział w dyskusji	CBZ1A_W10, CBZ1A_W09, CBZ1A_W07, CBZ1A_U09, CBZ1A_K06
Organizacje międzynarodowe a cyberbezpieczeństwo	Wykład	Aktywność na zajęciach, Kolokwium, Odpowiedź ustna	CBZ1A_W08, CBZ1A_W09, CBZ1A_W07, CBZ1A_U04, CBZ1A_U09, CBZ1A_K01, CBZ1A_K04, CBZ1A_K05
Zagrożenia dla płatności elektronicznych	Wykład, Ćwiczenia laboratoryjne	Aktywność na zajęciach, Wykonanie ćwiczeń, Zaliczenie laboratorium	CBZ1A_W04, CBZ1A_W09, CBZ1A_W10, CBZ1A_U01, CBZ1A_U10, CBZ1A_U11, CBZ1A_K03, CBZ1A_K04, CBZ1A_K05
Ethical Hacker	Zajęcia warsztatowe	Wykonanie ćwiczeń, Wynik testu zaliczeniowego	CBZ1A_W05, CBZ1A_W09, CBZ1A_U04, CBZ1A_U05, CBZ1A_U06, CBZ1A_U10, CBZ1A_K03, CBZ1A_K05, CBZ1A_K06
5G Networks: Advanced	Wykład, Ćwiczenia projektowe	Aktywność na zajęciach, Udział w dyskusji, Wykonanie projektu, Zaangażowanie w pracę zespołu, Prezentacja	CBZ1A_W02, CBZ1A_W04, CBZ1A_W06, CBZ1A_W09, CBZ1A_U02, CBZ1A_U03, CBZ1A_U04, CBZ1A_U05, CBZ1A_U06, CBZ1A_K01, CBZ1A_K02, CBZ1A_K04, CBZ1A_K06
Audyt bezpieczeństwa	Wykład, Ćwiczenia projektowe	Aktywność na zajęciach, Udział w dyskusji, Wykonanie projektu, Sprawozdanie	CBZ1A_W07, CBZ1A_W08, CBZ1A_W10, CBZ1A_U09, CBZ1A_U10, CBZ1A_U11, CBZ1A_K02, CBZ1A_K06, CBZ1A_K03, CBZ1A_K05
Ochrona własności intelektualnej	Wykład	Aktywność na zajęciach, Kolokwium, Studium przypadków	CBZ1A_W06, CBZ1A_W07, CBZ1A_W10, CBZ1A_W09, CBZ1A_U02, CBZ1A_U09, CBZ1A_K02, CBZ1A_K05

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	110
zajęć z zakresu nauk podstawowych właściwych dla danego kierunku studiów	48
zajęć o charakterze praktycznym, kształtujących umiejętności praktyczne, w tym zajęć laboratoryjnych, projektowych, praktycznych i warsztatowych	156
zajęć podlegających wyborowi przez studenta (w wymiarze nie mniejszym niż 30% liczby punktów ECTS koniecznych do uzyskania kwalifikacji odpowiadających poziomowi kształcenia)	63
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	8
zajęć z języka obcego	6
praktyk zawodowych	4
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)	109
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)	

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

Kierunek: Cyberbezpieczeństwo

Zasady wpisu na kolejny semestr

Regulamin Studiów AGH określa zasady wpisu na kolejny semestr. Student uzyskuje wpis po uzyskaniu zaliczeń z modułów przewidzianych programem studiów.

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

Regulamin Studiów AGH określa zasady wpisu na kolejny semestr w ramach tzw. dopuszczalnego deficytu 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 nie przewiduje prowadzenia zajęć w ramach bloków.

Semestry kontrolne

6

Zasady odbywania studiów według indywidualnej organizacji studiów

Regulamin Studiów AGH określa zasady indywidualizacji procesu kształcenia. 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

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. Dokładny przedział czasowy jest określony co rok zarządzeniem Rektora AGH i ujęty w dokumencie „Organizacja roku akademickiego”. Studenci studiów stacjonarnych powinni uzyskać zaliczenie praktyki po wakacjach, w czasie sesji poprawkowej.

Zasady obieralności modułów zajęć

Na początkowych semestrach studenci mogą wybierać język obcy. Rozpoczynając od semestru piątego wybierane są przedmioty kierunkowe. Przed rozpoczęciem semestru zostają zebrane preferencje studentów co do zapisów na poszczególne przedmioty kierunkowe, a następnie studenci przypisywani są do konkretnych modułów. W przypadku limitów, priorytet wyboru konkretnych przedmiotów mają osoby, które osiągają lepsze rezultaty na przedmiotach prowadzonych we wcześniejszych semestrach.

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

Program nie przewiduje ścieżek kształcenia i dyplomowania ani specjalności.

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

Regulamin Studiów AGH określa zasady przygotowania projektów dyplomowych oraz dyplomowania. Student przygotowuje pracę w ramach Projektu dyplomowego realizowanego na 7 semestrze. Projekt dyplomowy prowadzony jest przez opiekuna pracy, natomiast Warsztaty dyplomowe są prowadzone przez doświadczonych pracowników naukowo-dydaktycznych, którzy pomagają w terminowej realizacji projektu dyplomowego, weryfikują postępy prac i sposób prezentacji wyników oraz udzielają rad związanych z formalną stroną projektu i prezentacji dyplomowej.

Zasady ustalania ogólnego wyniku ukończenia studiów

Zasady ustalania ogólnego wyniku ukończenia studiów określa 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.

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

brak