



Program studiów

Kierunek: Cyberbezpieczeństwo

Spis treści

| | |
|-----------------------------------------------------------------------------------------------------------------------------|----|
| Ogólna charakterystyka kierunku studiów i programu studiów | 3 |
| Ogólne informacje o programie studiów | 5 |
| Warunki rekrutacji na studia | 7 |
| Efekty kierunkowe | 8 |
| Tabela zgodności kompetencji inżynierskich (Inz) z kierunkowymi efektami uczenia się (KEU) | 10 |
| Matryca pokrycia efektów kierunkowych | 11 |
| Matryca charakterystyk efektów uczenia się w odniesieniu do modułów zajęć | 18 |
| Matryca kierunkowych efektów uczenia się w odniesieniu do form zajęć i sposobu zaliczenia, które pozwalają na ich uzyskanie | 24 |
| Łączna liczba punktów ECTS | 34 |
| Szczegółowe zasady realizacji programu studiów ustalone przez dziekana wydziału | 35 |

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: | |
| Liczba punktów ECTS konieczna do ukończenia studiów na danym poziomie: | 210 |
| Tytuł zawodowy nadawany absolwentom: | inżynier |
| Termin rozpoczęcia cyklu: | 2021/2022, 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 AGH oraz misją AGH

Kierunek studiów Cyberbezpieczeństwo w pełni wpisuje się w misję AGH, w której zapisano: „Akademia Górniczo-Hutnicza jest uniwersytetem technicznym, w którym nauki ścisłe mają bardzo silną reprezentację i stanowią podstawę rozwoju maksymalnie szerokiego spektrum nauk stosowanych oraz stopniowo wzrastającej roli nauk humanistycznych. Zgodnie ze światowymi trendami rozwoju tworzymy nowe kierunki kształcenia, ale zachowujemy klasyczne, niezbędne do prawidłowego rozwoju nauki, techniki oraz gospodarki naszego kraju”.

Celem nadrzędnym tworzonego nowego kierunku studiów Cyberbezpieczeństwo jest zwiększenie potencjału rozwojowego 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 cyberbezpieczeństwo jest idealnym przykładem interdyscyplinarnego podejścia do nowoczesnego kształcenia. Dominujące nauki ścisłe zostaną bowiem uzupełnione elementami nauk społecznych. Takie połączenie pozwoli absolwentom wyjść na przeciw 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 wzmocnienia bezpieczeństwa i potencjału gospodarczego kraju.

Tworzony nowy kierunek studiów cyberbezpieczeństwo wpisuje się ściśle zarówno w strategię rozwoju AGH i Wydziału Informatyki, Elektroniki i Telekomunikacji, jak i w misję tych jednostek.

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

Komisja Europejska szacuje, że ukończenie budowy jednolitego rynku cyfrowego przyniesie unijnej gospodarce 415 mld euro rocznie i skutkować będzie utworzeniem setek tysięcy nowych miejsc pracy. Cyberbezpieczeństwo uważa się za jeden z najważniejszych czynników warunkujących rozkwit europejskiej gospodarki. Bez zaufania konsumentów oraz użytkowników

do korzystania z Internetu, proces ten będzie poważnie zagrożony. Wskazują na to jednoznacznie przeprowadzane badania (Eurobarometer, 2012).

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. Na gruncie polskim, zaledwie kilka miesięcy temu, 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 dzisiaj funkcjonowania również 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.

Potrzeby związane z cyberbezpieczeństwem są bezsprzeczne i stale rosnące. Jednocześnie podaż specjalistów z obszaru cyberbezpieczeństwa zupełnie nie nadąża za popytem. Jest to trend globalny. Szacuje się, że w Europie do 2022 roku zabraknie nawet 350 tysięcy specjalistów od cyberbezpieczeństwa. Szacunki z 2017 roku, pokazywały, że prawie 40% europejskich firm chce rozwijać swoje zespoły cyberbezpieczeństwa o co najmniej 15% w ciągu najbliższych lat (2017 Global Information Security Workforce Study). W skali globalnej 70% badanych firm wskazało, że chce zatrudnić w najbliższym czasie specjalistów z omawianego obszaru.

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 dostarczy absolwentów, którzy będą 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, cyberterrorizm, 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 wątplenia 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. Jeden z raportów przewiduje, że globalne zapotrzebowanie na nowych specjalistów z dziedziny cyberbezpieczeństwa do 2021 osiągnie poziom 3.5 miliona pozycji (Cybersecurity Jobs Report 2018-2021). Podobnie kształtuje się także rynek w Polsce. Najnowszy raport „Barometr Cyberbezpieczeństwa”, przygotowany przez KMPG pokazuje, że największym problemem polskich firm, jeśli chodzi o budowanie cyberbezpieczeństwa, są trudności w zatrudnieniu i utrzymaniu wykwalifikowanych pracowników (Barometr Cyberbezpieczeństwa, 2018). Popyt na absolwentów istnieje i będzie mocno wzrastał.

Konstruując kierunek Cyberbezpieczeństwo brano pod uwagę losy absolwentów Wydziału IEiT AGH, które wskazują na bardzo dobrą ich pozycję na rynku. Bardzo duży odsetek (ponad 80%) studentów stwierdza, że drugi raz wybraliby te same studia, bardzo niski odsetek (kilka procent) nie podejmuje pracy po zakończeniu studiów (najczęściej z różnych powodów losowych). Kierunek Cyberbezpieczeństwo niewątpliwie rozszerzy ofertę Wydziału IEiT o absolwentów z bardzo

poszukiwanymi kompetencjami na rynku, którzy bazując na dotychczasowej historii Wydziału powinni również bardzo szybko znaleźć miejsce na rynku pracy.

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

Wszystkie kierunki prowadzone na Wydziale IEiT (Elektronika i Telekomunikacja, Elektronika, Teleinformatyka i Informatyka) przechodziły w ostatnich miesiącach 2018 roku akredytację. Teleinformatyka otrzymała akredytację z wyróżnieniem, na ocenę pozostałych kierunków oczekujemy. Doświadczenia zdobyte podczas przygotowywania dokumentacji a także zalecenia otrzymane dla innych kierunków po wizycie PKA zostały twórczo zaadaptowane do potrzeb tworzenia nowego kierunku.

Informacja na temat uwzględnienia w programie studiów przykładów dobrych praktyk

- Dużą wagę przywiązuje się do szerokiej oferty przedmiotów obieralnych, łącznie z ciekawymi przedmiotami humanistycznymi oraz przedmiotami z UBPJO AGH.
- Na wydziale i na Uczelni były i są realizowane są programy w konkursie POWER, dzięki którym dydaktycy mają możliwość otrzymać dofinansowanie za rozszerzenie i poprawę swoich 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.
- Pełnomocnik Dziekana ds. Kierunku w sposób otwarty i kompetentny opiekuje się studentami, pomaga rozwiązywać ich problemy i czuwa 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 studentów.

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 po 3-im r. studiów, 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 (tj. po zakończeniu 6 semestru). Student ma obowiązek realizacji 120 godz. (4 ECTS) w ramach 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 określa Uchwała nr 97/2019 Senatu AGH z dnia 26 czerwca 2019 r. w sprawie warunków, trybu oraz terminu rozpoczęcia i zakończenia rekrutacji na pierwszy rok studiów pierwszego i drugiego stopnia w roku akademickim 2020/2021.

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

Minimalna liczba studentów: 50

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 opisu, analizy i modelowania działania sieci i urządzeń teleinformatycznych, algorytmów przetwarzania informacji oraz sygnałów i algorytmów obliczeniowych z uwzględnieniem aspektów bezpieczeństwa. | P6S_WG_A |
| CBZ1A_W02 | Ma wiedzę w zakresie mediów telekomunikacyjnych, przetwarzania i transmisji sygnałów oraz danych, w szczególności uwzględniając bezpieczeństwo ich użytkowania. | P6S_WG_A, P6S_WG_A_Inz |
| CBZ1A_W03 | Zna i rozumie algorytmy, języki i techniki programowania oraz tworzenia aplikacji, a także zasady projektowania baz danych z uwzględnieniem wymagań bezpieczeństwa. | P6S_WG_A, P6S_WG_A_Inz |
| CBZ1A_W04 | Zna i rozumie zagadnienia w zakresie systemów i sieci teleinformatycznych, zarówno przewodowych jak i bezprzewodowych, zasady ich organizacji, administracji, aspektów bezpieczeństwa i stosowanych w nich protokołach komunikacyjnych. | P6S_WG_A_Inz |
| CBZ1A_W05 | Ma wiedzę w zakresie zabezpieczania architektury komputerów i urządzeń sieci teleinformatycznych. | P6S_WG_A_Inz |
| CBZ1A_W06 | Zna zasady prowadzenia działalności gospodarczej oraz ochrony własności intelektualnej, rozumie również pozatechniczne, np. społeczne, ekonomiczne czy prawne uwarunkowania działalności inżynierskiej w branży bezpieczeństwa teleinformatycznego. | P6S_WK_A_Inz, P6S_WK_A |
| CBZ1A_W07 | Posiada wiedzę z zakresu uwarunkowań prawnych i regulacyjnych wpływających na działania i obowiązki podmiotów zaangażowanych w zapewnianie cyberbezpieczeństwa. | P6S_WK_A |
| CBZ1A_W08 | Zna zasady funkcjonowania krajowego i międzynarodowego systemu cyberbezpieczeństwa. | P6S_WK_A |
| CBZ1A_W09 | Zna i rozumie zagrożenia i szanse wynikające z funkcjonowania w świecie cyfrowym wpływające na współczesne państwa, społeczeństwa, podmioty prywatne. | P6S_WK_A |
| CBZ1A_W10 | Zna normy i standardy określające wytyczne i wymagania w zakresie zapewniania bezpieczeństwa informacyjnego. | P6S_WK_A |

Umiejętności

| Symbol KEU | Kierunkowe efekty uczenia się | Symbol CEU |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| CBZ1A_U01 | Potrafi definiować oraz realizować zadania, w szczególności dotyczące bezpieczeństwa teleinformatycznego, dobierając odpowiednie źródła informacji oraz krytycznie je analizując i syntetyzując, a także wybierając stosowne narzędzia programistyczne, sprzętowe i sieciowe. | P6S_UW_A |
| CBZ1A_U02 | Potrafi opracować dokumentację, przedstawić prezentację i dyskutować na temat zadania, projektu czy zagadnień w szczególności związanych z bezpieczeństwem teleinformatycznym, również w języku obcym. | P6S_UK_A |
| CBZ1A_U03 | Potrafi pracować indywidualnie i w zespole, planować pracę, a także komunikować się przy użyciu technik właściwych dla branży IT w szczególności w sektorze cyberbezpieczeństwa. | P6S_UO_A |
| CBZ1A_U04 | Ma umiejętność samokształcenia się, potrafi planować swój dalszy rozwój zawodowy w branży IT, w szczególności w sektorze cyberbezpieczeństwa. | P6S_UU_A |

| Symbol KEU | Kierunkowe efekty uczenia się | Symbol CEU |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| CBZ1A_U05 | Potrafi planować i przeprowadzać testy, eksperymenty i badania z dziedziny telekomunikacji i informatyki, w szczególności związane z cyberbezpieczeństwem, oparte na obliczeniach, symulacjach komputerowych i pomiarach. | P6S_UW_A_Inz_01 |
| CBZ1A_U06 | Potrafi analizować i projektować protokoły, sieci i systemy teleinformatyczne, stosując właściwe metody, techniki i narzędzia, biorąc również pod uwagę aspekty systemowe i pozatechniczne a w szczególności związane z bezpieczeństwem ich użytkowania. | P6S_UW_A_Inz_02 |
| CBZ1A_U07 | Potrafi konfigurować urządzenia i protokoły oraz zarządzać i przede wszystkim dbać o bezpieczeństwo zasobów danych, sieci i systemów teleinformatycznych. | P6S_UW_A_Inz_02 |
| CBZ1A_U08 | Potrafi pisać algorytmy i aplikacje oraz wykonywać większe projekty programistyczne, w szczególności w sferze cyberbezpieczeństwa, w oparciu o języki programowania niskiego i wysokiego poziomu, aplikacje sieciowe i bazy danych. | P6S_UW_A_Inz_02 |
| CBZ1A_U09 | Potrafi analizować akty prawne kluczowe z punktu widzenia cyberbezpieczeństwa oraz implementować wynikające z nich obowiązki. | P6S_UK_A, P6S_UO_A |
| CBZ1A_U10 | Potrafi zaplanować i wdrożyć procedury i rozwiązania organizacyjne związane z bezpieczeństwem informacyjnym | P6S_UW_A |
| CBZ1A_U11 | Potrafi zarządzać ryzykiem związanym z wielowymiarowymi wyzwaniami płynącymi z cyberprzestrzeni | P6S_UW_A, P6S_UK_A |

Kompetencje społeczne

| Symbol KEU | Kierunkowe efekty uczenia się | Symbol CEU |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| CBZ1A_K01 | Rozumie potrzebę krytycznej oceny posiadanej wiedzy oraz ciągłego doskonalenia się i konsultacji z innymi ekspertami z branży IT, w szczególności związanej z cyberbezpieczeństwem. | P6S_KK_A |
| CBZ1A_K02 | Potrafi współpracować i działać na rzecz grupy współpracowników oraz szerzej na rzecz środowiska społecznego, potrafi też myśleć i działać w sposób przedsiębiorczy. | P6S_KO_A |
| CBZ1A_K03 | Ma świadomość roli zawodowej i społecznej absolwenta technicznych studiów wyższych i wagi przestrzegania zasad etyki zawodowej w branży IT, 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 cyberbezpieczeństwa | 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 | podstawowe procesy zachodzące w cyklu życia urządzeń, obiektów i systemów technicznych | CBZ1A_W02, CBZ1A_W03, CBZ1A_W04, CBZ1A_W05 |
| P6S_WK_A_Inz | 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 | 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 | 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

2021/2022/S/li/IEiT/CBZ/all

| Przedmiot | Kod | 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 |
|-----------------------------------------------------------------|----------------------------------------------------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| Wprowadzenie do prawa karnego i postępowania karnego | IEiTCBZS.li1P.9ba69f67daee654f93a77c1404132c7d.21 | | | | | | x | x | | | | | | | | | | | | x | | | | | | | | x |
| Wstęp do informatyki | IEiTCBZS.li1P.0dc4696e1d7fba8f3707d463a1b1389.21 | x | x | x | | | | | | | | | | x | x | | | | x | | | | x | | | | x | x |
| Wprowadzenie do sieci Internet | IEiTCBZS.li10.0fdc5bca0d6418dd2a5babfa2b3eb48d.21 | | | | x | | | | | | | | | x | | | | | | | | | | x | | | | |
| Analiza 1 | IEiTCBZS.li1P.8aae61ca6e57cf03260df9af3cd3661f.21 | x | | | | | | | | | | x | | | | | | | | | | | x | | | | | |
| Algebra | IEiTCBZS.li1P.5c7fd2ae7c5cff56692ac76a3173da65.21 | x | | | | | | | | | | | | | | x | x | | x | | | | x | | x | | | |
| Krajowy system cyberbezpieczeństwa | IEiTCBZS.li1K.2ba59fb5a942767566b38dcb24bad9fd.21 | | | | | | | x | x | x | | | | | x | | | | | x | | | x | x | x | x | x | x |
| Wstęp do administracji i bezpieczeństwa komputerowego | IEiTCBZS.li1P.f7bac7fdc4a53d57ac1f18c3042bfc7f.21 | | | | | x | | | | | x | | | | | | | x | | | | | x | | x | | | |
| Matematyka dyskretna | IEiTCBZS.li2P.e259c5b2344d0df764021f794fe479ed.21 | x | | | | | | | | | | x | x | x | | | | | x | | | | | x | | | | |
| Język rosyjski B-2 - kurs obowiązkowy 135 godzin - semestr 1/3 | IEiTCBZS.li2J0.9207a194b6d4f62b09f23e6556e6b2ed.21 | | | | | | | | | | | | | x | | | | | | | | | | | | | | |
| Język niemiecki B-2 - kurs obowiązkowy 135 godzin - semestr 1/3 | IEiTCBZS.li2J0.375d0ed08478ee775e900113312791c3.21 | | | | | | | | | | | | | x | | | | | | | | | | | | | | |

| Przedmiot | Kod | 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 angielski B-2 - kurs obowiązkowy 135 godzin - semestr 1/3 | IEiTCBZS.li2JO.df2639cc44c5e396cf0074ea122cab71.21 | | | | | | | | | | | | x | | | | | | | | | | | | | | | |
| Probabilistyka i statystyka | IEiTCBZS.li2P.feee334d1c1c525a280375e6f257c710.21 | x | | | | | | | | | x | x | | x | | | | | | | | | x | | | | | x |
| Język francuski B-2 - kurs obowiązkowy 135 godzin - semestr 1/3 | IEiTCBZS.li2JO.e553773bdd5bdb73e59798df5bf39847.21 | | | | | | | | | | | | | x | | | | | | | | | | | | | | |
| Język hiszpański B-2 - kurs obowiązkowy 135 godzin - semestr 1/3 | IEiTCBZS.li2JO.e2e9f855d3be1c6e44f1609c9b3733bf.21 | | | | | | | | | | | | | x | | | | | | | | | | | | | | |
| Analiza 2 | ICBZ00S.li2P.cf9d0d2f24d79245646ef2bf84c61c3a.21 | x | | | | | | | | | | x | | | | | | | | | | | x | | | | | |
| Fizyka 1 | IEiTCBZS.li2P.6b2156684a724e1f4e161620f5f9a455.21 | x | | | | | | | | | | x | x | x | x | | | | | | | | x | | | | | |
| Projektowanie i analiza algorytmów | IEiTCBZS.li2K.2bfef0a783c233910f0aa2fa2d404a0b.21 | x | | | | | | | | | | x | | | | | | | | | | | x | | | | | |
| Wykrywanie incydentów | IEiTCBZS.li2K.1b081a7391f5dda6ebff6036c654ee5.21 | | | | | | | | | x | | | | | | | | | x | | x | | | | | | | x |
| Podstawy programowania | IEiTCBZS.li2P.7983d546d9dbac88551ec2353f11ac91.21 | | | x | | | | | | | | | | | | | | | x | | | | | x | | | | |
| Bezpieczeństwo systemów i sieci teleinformatycznych | IEiTCBZS.li2K.562f5da974e694905149dc857b5bd6f0.21 | x | | | x | x | | | | | | x | | | | x | x | | | | | | x | | | x | | |
| Zarządzanie bezpieczeństwem informacji | IEiTCBZS.li2K.fdcfc9313515450c06885ebc603d9393.21 | | | | | | x | x | | x | x | x | x | x | | | | | | x | x | x | x | x | x | x | x | x |
| Inżynieria społeczna | IEiTCBZS.li40.1e7441ed12bb0a1d1ffcd4f7168b43c1.21 | | | | | | | | | x | | | | | x | | | | | x | x | | | x | x | | | |

| Przedmiot | Kod | 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 rosyjski B-2 - kurs obowiązkowy 135 godzin - semestr 2/3 | IEiTCBZS.li4JO.1b348d99edf04f5b24411f8925d672c5.21 | | | | | | | | | | | | x | | | | | | | | | | | | | | |
| Język angielski B-2 - kurs obowiązkowy 135 godzin - semestr 2/3 | IEiTCBZS.li4JO.53db5d5bb3888bb0d3df2be2aca157b1.21 | | | | | | | | | | | | x | | | | | | | | | | | | | | | | |
| Bezpieczeństwo lokalnych sieci komputerowych | IEiTCBZS.li4K.e2ed177ef976a3a5db0fc7724e66a8ff.21 | | | | x | x | | | | | | x | | | | | | x | | | | | x | | | | | | |
| Bezpieczeństwo aplikacji webowych i mobilnych | IEiTCBZS.li4K.660ac5e007871ac5c320b19e304249fb.21 | | | x | x | | | | | | x | x | x | x | x | x | | | x | | | | x | x | x | | x | x | |
| Informatyka śledcza | IEiTCBZS.li4K.d56ebf7ef7f60541174f4b8167c2ab27.21 | | | x | x | x | | | | | | | | | | | x | | | | | | | | | | x | | |
| Język francuski B-2 - kurs obowiązkowy 135 godzin - semestr 2/3 | IEiTCBZS.li4JO.022ccfa514f05e50192ce87a0bff56b7.21 | | | | | | | | | | | | x | | | | | | | | | | | | | | | | |
| Wstęp do zwalczania cyberprzestępczości | IEiTCBZS.li4K.527d27c22b4570da347f40b21f368905.21 | | | | | | | x | x | x | | | | | x | | | | | | | | | x | | | | | |
| Język hiszpański B-2 - kurs obowiązkowy 135 godzin - semestr 2/3 | IEiTCBZS.li4JO.a7a0e38e103236aa9b214adde0985c59.21 | | | | | | | | | | | | x | | | | | | | | | | | | | | | | |
| Fizyka 2 | IEiTCBZS.li4P.eeb96d41e6d57c930f93b913100c61dc.21 | x | | | | | | | | | | x | x | x | x | | | | | | | | x | | | | | | |
| Język niemiecki B-2 - kurs obowiązkowy 135 godzin - semestr 2/3 | IEiTCBZS.li4JO.194f7fd6b2f8791bf3f31dfd0a5d917d.21 | | | | | | | | | | | | x | | | | | | | | | | | | | | | | |
| Programowanie skryptowe | IEiTCBZS.li4K.6f48245ec79f893cb690ffea569d82f3.21 | | | | x | | | | | | | | | | | | | | x | | | | x | | | | | | |
| Kryptografia | IEiTCBZS.li4K.29ff2fb13c451eb0988217388bf253fc.21 | x | x | x | x | | | | | x | | x | | | | x | x | | x | | | | x | | | x | x | x | |

| Przedmiot | Kod | 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 |
|------------------------------------------------------------------|----------------------------------------------------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| Systemy operacyjne | IEiTCBZS.li4K.b9d40ab367cf3e4a432ef6e87fec8967.21 | | | | x | | | | | | | x | | | | | | | x | | | | | | x | | x | |
| Analiza powłamaniowa | IEiTCBZS.li8K.d48aff5ebadb6c2842f21deb55d5235.21 | | | | | x | | | | | x | | x | | | | | | | | | | x | | | | | |
| Język rosyjski B-2 - kurs obowiązkowy 135 godzin - semestr 3/3 | IEiTCBZS.li8JO.49d62cc9cd39f7fb09b10f8cfbeb7b06.21 | | | | | | | | | | | | | x | | | | | | | | | | | | | | |
| Bezpieczeństwo bezprzewodowych sieci komputerowych | IEiTCBZS.li8K.d27b6ca4174208b96219300dc8b66f33.21 | | x | | x | x | | | | | x | x | x | | | x | x | x | | | | | x | x | x | | | x |
| Wprowadzenie do białego wywiadu | ICBZ00S.li8O.0b5550071879f4043c469fdeb715348a.21 | | | | | | | | | x | | | | | x | | | | | | | | x | | | | x | |
| Język hiszpański B-2 - kurs obowiązkowy 135 godzin - semestr 3/3 | IEiTCBZS.li8JO.001aefb3b9af1096e2664b81b183c217.21 | | | | | | | | | | | | | x | | | | | | | | | | | | | | |
| Język francuski B-2 - kurs obowiązkowy 135 godzin - semestr 3/3 | IEiTCBZS.li8JO.6807c4d8cf5331d62a78d10b502b9ccb.21 | | | | | | | | | | | | | x | | | | | | | | | | | | | | |
| Organizacje międzynarodowe a cyberbezpieczeństwo | IEiTCBZS.li8O.f19c2a2929936e5be73df19bee31a1cc.21 | | | | | | | | x | x | x | | | | x | | | | | x | | | x | | | x | x | |
| Bezpieczeństwo oprogramowania | IEiTCBZS.li8K.c513d1c8b0d66bc21f36b0d66843aed6.21 | | x | x | | x | | | | | x | x | x | | | x | | | | | | x | | | | | | x |
| Wykrywanie anomalii sieciowych z użyciem uczenia maszynowego | IEiTCBZS.li8K.9bf8eec690e06ffe497a16136fe6ba54.21 | x | x | x | x | x | | | | | | x | x | x | x | | x | | | | | | x | | | | x | x |
| Język angielski B-2 - kurs obowiązkowy 135 godzin - semestr 3/3 | IEiTCBZS.li8JO.5e50e9a2d67b5162c856cf859a9b227f.21 | | | | | | | | | | | | | x | | | | | | | | | | | | | | |

| Przedmiot | Kod | 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 malware | ICBZ00S.li8K.9a735e2e4d9290349cc2d3c6e0645580.21 | | | x | x | x | | | | | | | | | | | x | | | | | | | | | | x | |
| Język niemiecki B-2 - kurs obowiązkowy 135 godzin - semestr 3/3 | IEiTCBZS.li8JO.e9248a9a134c74395721cf546e69ecdf.21 | | | | | | | | | | | | x | | | | | | | | | | | | | | | |
| Sprzętowe aspekty cyberbezpieczeństwa | IEiTCBZS.li8K.58c8910cc535d6f1d6bc4e5e93f181a9.21 | x | x | x | x | x | | x | | x | x | x | x | x | | x | x | x | x | | x | | | | | | | x |
| Ochrona danych osobowych i technologie wzmacniające prywatność | ICBZ00S.li8K.309676e6c264e6746facab38d407043d.21 | | | | | x | x | | | | x | x | | | | | | | x | | x | | | | | | | x |
| Bazy danych | IEiTCBZS.li8K.5eb52d767603909189082b3acc3bc79d.21 | | | x | | | | | | | | | | | x | | | | x | | | | | x | | | | x |
| Bezpieczeństwo systemów komórkowych i sieci 5G | ICBZ00S.li10K.07a1aae1f1265efb93f0898e8abc60d3.21 | x | x | | x | x | | | | | | x | x | x | | x | x | x | | | | | x | x | | | | |
| Cybersecurity and contemporary conflicts | IEiTCBZS.li10PJO.4bf2d4e680eb8d7947c02a56b2645766.21 | | | | | | | | x | x | | | | | x | | | | | | x | | x | x | | x | x | x |
| Biometria | IEiTCBZS.li10K.91429ab6404d946c7103b476884a319e.21 | x | | | | | | x | | x | x | x | x | x | x | x | x | | x | x | x | x | | x | x | | x | x |
| Ochrona informacji niejawnych | IEiTCBZS.li10K.5145750c05a1e0f5f4fee1331cc9b831.21 | | | | | | x | x | x | x | x | | | x | x | | x | | | x | x | x | x | x | x | x | x | x |
| Wprowadzenie do inżynierii oprogramowania | IEiTCBZS.li100.64d08ad26e8621a021be9d5c4d3bd749.21 | x | x | x | | | | x | x | x | x | x | x | x | x | | | | x | x | x | x | x | x | x | | | x |
| Szpiegostwo przemysłowe | IEiTCBZS.li10K.9c1e730c819991a3357a7bf4cba78a10.21 | | | | | | x | x | | | | | | | | | | | | x | | | | | | | | x |
| Zarządzanie incydentami - SOC oraz CERT | IEiTCBZS.li10K.227fe3ba93083a2110975d2e455ee3ee.21 | | | | | | | x | x | x | x | | | | | | | | | | x | | | | | | | |

| Przedmiot | Kod | 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 zwirtualizowanych środowisk IT | IEiTCBZS.li10K.ef382922cefd8ca87b9ae8529232839e.21 | | | | x | x | | | | | | | x | x | | | x | x | | | x | | x | | | |
| Testy penetracyjne | ICBZ00S.li10K.f479bb92e5cf7662bceb74ac6fa7a783.21 | | | | | | | | | | x | | | | | | x | | | | | | | | x | | | x |
| Bezpieczeństwo w sieciach rozległych | IEiTCBZS.li10K.979f76511b5d2580af8495b6b015c523.21 | | | | x | x | | | | | | | | | | | | x | | | | | x | | | | | |
| Koło naukowe | IEiTCBZS.li20K.6c2dd2a0521f52b7970d675b80f21b94.21 | | x | x | x | x | x | x | | x | x | x | x | x | x | | | | | x | x | | x | | | x | x | |
| Security of operating systems | IEiTCBZS.li20K.723aec15067ec466380d438e74eb4008.21 | | | x | x | | | | | | | x | | x | | | x | x | | | | | x | x | x | | | |
| Podstawy analizy informacji | IEiTCBZS.li20K.26e3f0d4a7d9b4f869835eb856059e3c.21 | | | | | | x | x | x | x | x | x | x | | | | | | | x | x | x | | | | x | x | x |
| Praktyczne wykorzystanie informacji z otwartych źródeł | IEiTCBZS.li20K.5358cd5c2cc151ff51e3f9795cf439a2.21 | | | | | | | | | x | | | | | x | | | | | | | | | x | | | | |
| Wprowadzenie do informatyki kwantowej | IEiTCBZS.li20K.323b3a8026a0248b9af0042d78982777.21 | x | | | | x | | | | | x | | | x | | x | | | | | | | x | x | x | | | |
| Cyberbezpieczeństwo i prawo międzynarodowe | IEiTCBZS.li20K.8404c0d97150c18d899908a607671be4.21 | | | | | | | x | x | x | x | | | x | x | | | | | x | | | x | x | | | x | x |
| Krajowe zasoby informacyjne | IEiTCBZS.li20K.9f7b37ca8a4f07c2e1b5c11370ee5655.21 | | | | | | | x | | x | x | | | | | | | | | x | | | | | | | | x |
| Bezpieczeństwo infrastruktury krytycznej i systemów sterowania przemysłowego | IEiTCBZS.li20K.849876180bf9bf13ceb476ebd9121a85.21 | | | | | | | | | | x | | | | | | | | | | x | x | x | x | | | | |
| Pracownia projektowa 1 | IEiTCBZS.li20K.c9b12ced59d14cdda72665b694ada6b5.21 | | | | | | | | | | | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x |
| Praktyki zawodowe | IEiTCBZS.li20K.1eddd722812cb22a6375443a406368c2.21 | | | | | | | | | | | x | x | x | x | x | | | x | | | | | x | x | x | x | x |

| Przedmiot | Kod | 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 |
|---------------------------------------------------------|----------------------------------------------------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| Programowanie sieciowe wspierające aplikacje bezpieczne | IEiTCBZS.li20K.08d2f2e7b20c22e7544995348e6e43b0.21 | | | x | x | x | | | | | | | | | | x | x | x | x | | | | x | x | | | | |
| Przedmiot obieralny z UBPIO | IEiTCBZS.li400.35a1dd1261eebe67f76be03858741abf.21 | | | | x | x | x | x | x | | | | x | x | x | | | | | | | | x | | | x | x | |
| Pracownia projektowa 2 | IEiTCBZS.li40K.7bf6e013d20aa0cde672e1d35ac09881.21 | | | | | | | | | | | x | x | x | x | x | | | | | x | | | | x | x | x | x |
| Cyfrowe znaki wodne i steganografia | IEiTCBZS.li40K.0af9b507fbbcea58aab82f6595b336bf.21 | x | x | | | | | | | | | x | x | x | x | | x | | x | | | | x | | | | x | x |
| Bezpieczeństwo IoT | IEiTCBZS.li40K.9293145073460f5412cf3e1129984344.21 | | | | x | | | | | | | | x | x | x | | | x | | | | | | x | | | | |
| Projekt inżynierski | IEiTCBZS.li40K.f29d56545dbb5e5f3d4cafcbf5a1cbdb.21 | | | | | | | | | | | x | x | x | x | x | x | x | x | | x | x | x | | | x | x | x |
| Blockchain | IEiTCBZS.li40K.d2deb71ea8bc391df097d4e423ff2c9e.21 | x | x | | | x | x | x | x | x | x | x | x | x | x | x | | x | x | x | x | x | x | | | x | x | |
| Kryptoanaliza | IEiTCBZS.li40K.750cac3b33cf095aa56e575c7e7864c9.21 | x | | x | x | x | | | x | | | x | | | | x | x | | x | | | | x | | | x | | x |
| Koło naukowe | IEiTCBZS.li40K.6c2dd2a0521f52b7970d675b80f21b94.21 | | x | x | x | x | x | x | | x | x | x | x | x | x | | | | | x | x | | | | | x | x | |
| Cyberbezpieczeństwo a przetwarzanie danych w chmurze | IEiTCBZS.li40K.edaf0021ad67b2a5077d0da76f439fa1.21 | | | x | | x | | | | | x | | | x | x | | | | | | | | | | | | x | |
| Suma: | | 20 | 10 | 19 | 22 | 23 | 9 | 18 | 12 | 23 | 22 | 31 | 40 | 33 | 24 | 17 | 20 | 16 | 21 | 16 | 19 | 10 | 41 | 23 | 20 | 17 | 28 | 23 |

Matryca charakterystyk efektów uczenia się w odniesieniu do modułów zajęć

Kierunek: Cyberbezpieczeństwo

2021/2022/S/li/IEiT/CBZ/all

| Przedmiot | Kod | P6S_WG_A | P6S_WG_A_Inz | P6S_WK_A_Inz | P6S_WK_A | 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 |
|-----------------------------------------------------------------|----------------------------------------------------|----------|--------------|--------------|----------|----------|----------|----------|----------|-----------------|-----------------|----------|----------|----------|
| | | | | | | | | | | | | | | |
| Wprowadzenie do prawa karnego i postępowania karnego | IEiTCBZS.li1P.9ba69f67daee654f93a77c1404132c7d.21 | | | x | x | | x | x | | | | | | x |
| Wstęp do informatyki | IEiTCBZS.li1P.0dc4696e1d7fba8f3707d463a1b1389.21 | x | x | | | | | x | x | | x | x | x | x |
| Wprowadzenie do sieci Internet | IEiTCBZS.li1O.0fdc5bca0d6418dd2a5babfa2b3eb48d.21 | | x | | | | | x | | | | | x | |
| Analiza 1 | IEiTCBZS.li1P.8aae61ca6e57cf03260df9af3cd3661f.21 | x | | | | x | | | | | | x | | |
| Algebra | IEiTCBZS.li1P.5c7fd2ae7c5cff56692ac76a3173da65.21 | x | | | | | | | | x | x | x | | x |
| Krajowy system cyberbezpieczeństwa | IEiTCBZS.li1K.2ba59fb5a942767566b38dcb24bad9fd.21 | | | | x | | x | x | x | | | x | x | x |
| Wstęp do administracji i bezpieczeństwa komputerowego | IEiTCBZS.li1P.f7bac7fdc4a53d57ac1f18c3042bfc7f.21 | | x | x | | | | | | | x | x | | x |
| Matematyka dyskretna | IEiTCBZS.li2P.e259c5b2344d0df764021f794fe479ed.21 | x | | | | x | x | x | | | x | | x | |
| Język rosyjski B-2 - kurs obowiązkowy 135 godzin - semestr 1/3 | IEiTCBZS.li2JO.9207a194b6d4f62b09f23e6556e6b2ed.21 | | | | | | x | | | | | | | |
| Język niemiecki B-2 - kurs obowiązkowy 135 godzin - semestr 1/3 | IEiTCBZS.li2JO.375d0ed08478ee775e900113312791c3.21 | | | | | | x | | | | | | | |
| Język angielski B-2 - kurs obowiązkowy 135 godzin - semestr 1/3 | IEiTCBZS.li2JO.df2639cc44c5e396cf0074ea122cab71.21 | | | | | | x | | | | | | | |
| Probabilistyka i statystyka | IEiTCBZS.li2P.feee334d1c1c525a280375e6f257c710.21 | x | | | x | x | | x | | | | x | x | |

| Przedmiot | Kod | P6S_WG_A | P6S_WG_A_Inz | P6S_WK_A_Inz | P6S_WK_A | 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 |
|------------------------------------------------------------------|----------------------------------------------------|----------|--------------|--------------|----------|----------|----------|----------|----------|-----------------|-----------------|----------|----------|----------|
| | | | | | | | | | | | | | | |
| Język francuski B-2 - kurs obowiązkowy 135 godzin - semestr 1/3 | IEiTCBZS.li2JO.e553773bdd5bdb73e59798df5bf39847.21 | | | | | | x | | | | | | | |
| Język hiszpański B-2 - kurs obowiązkowy 135 godzin - semestr 1/3 | IEiTCBZS.li2JO.e2e9f855d3be1c6e44f1609c9b3733bf.21 | | | | | | x | | | | | | | |
| Analiza 2 | ICBZ00S.li2P.cf9d0d2f24d79245646ef2bf84c61c3a.21 | x | | | | x | | | | | | x | | |
| Fizyka 1 | IEiTCBZS.li2P.6b2156684a724e1f4e161620f5f9a455.21 | x | | | | x | x | x | x | | | x | | |
| Projektowanie i analiza algorytmów | IEiTCBZS.li2K.2bfeb0a783c233910f0aa2fa2d404a0b.21 | x | | | | x | | | | | | x | | |
| Wykrywanie incydentów | IEiTCBZS.li2K.1b081a7391f5dda6ebef6036c654ee5.21 | | | | x | x | | | | | x | | x | |
| Podstawy programowania | IEiTCBZS.li2P.7983d546d9dbac88551ec2353f11ac91.21 | x | x | | | | | | | | x | | x | |
| Bezpieczeństwo systemów i sieci teleinformatycznych | IEiTCBZS.li2K.562f5da974e694905149dc857b5bd6f0.21 | x | x | | | x | | | | | x | x | x | |
| Zarządzanie bezpieczeństwem informacji | IEiTCBZS.li2K.fdcfc9313515450c06885ebc603d9393.21 | | | x | x | x | x | x | | | | x | x | x |
| Inżynieria społeczna | IEiTCBZS.li4O.1e7441ed12bb0a1d1ffcd4f7168b43c1.21 | | | | x | x | x | x | | | | | x | x |
| Język rosyjski B-2 - kurs obowiązkowy 135 godzin - semestr 2/3 | IEiTCBZS.li4JO.1b348d99edf04f5b24411f8925d672c5.21 | | | | | | x | | | | | | | |
| Język angielski B-2 - kurs obowiązkowy 135 godzin - semestr 2/3 | IEiTCBZS.li4JO.53db5d5bb3888bb0d3df2be2aca157b1.21 | | | | | | x | | | | | | | |
| Bezpieczeństwo lokalnych sieci komputerowych | IEiTCBZS.li4K.e2ed177ef976a3a5db0fc7724e66a8ff.21 | | x | | | x | | | | | | x | x | |
| Bezpieczeństwo aplikacji webowych i mobilnych | IEiTCBZS.li4K.660ac5e007871ac5c320b19e304249fb.21 | x | x | | x | x | x | x | x | x | x | x | x | x |
| Informatyka śledcza | IEiTCBZS.li4K.d56ebf7ef7f60541174f4b8167c2ab27.21 | x | x | | | | | | | | | x | | x |

| Przedmiot | Kod | | | | | | | | | | | | | |
|------------------------------------------------------------------|----------------------------------------------------|----------|--------------|--------------|----------|----------|----------|----------|----------|-----------------|-----------------|----------|----------|----------|
| | | P6S_WG_A | P6S_WG_A_Inz | P6S_WK_A_Inz | P6S_WK_A | 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 |
| Język francuski B-2 - kurs obowiązkowy 135 godzin - semestr 2/3 | IEiTCBZS.li4JO.022ccfa514f05e50192ce87a0bff56b7.21 | | | | | | x | | | | | | | |
| Wstęp do zwalczania cyberprzestępczości | IEiTCBZS.li4K.527d27c22b4570da347f40b21f368905.21 | | | | x | | | x | | | | | x | |
| Język hiszpański B-2 - kurs obowiązkowy 135 godzin - semestr 2/3 | IEiTCBZS.li4JO.a7a0e38e103236aa9b214adde0985c59.21 | | | | | | x | | | | | | | |
| Fizyka 2 | IEiTCBZS.li4P.eeb96d41e6d57c930f93b913100c61dc.21 | x | | | | x | x | x | x | | | | x | |
| Język niemiecki B-2 - kurs obowiązkowy 135 godzin - semestr 2/3 | IEiTCBZS.li4JO.194f7fd6b2f8791bf3f31dfd0a5d917d.21 | | | | | | x | | | | | | | |
| Programowanie skryptowe | IEiTCBZS.li4K.6f48245ec79f893cb690ffea569d82f3.21 | x | x | | | | | | | | | x | x | |
| Kryptografia | IEiTCBZS.li4K.29ff2fb13c451eb0988217388bf253fc.21 | x | x | | x | x | | | | | x | x | x | x |
| Systemy operacyjne | IEiTCBZS.li4K.b9d40ab367cf3e4a432ef6e87fec8967.21 | | x | | | x | | | | | | x | | x |
| Analiza powłamaniowa | IEiTCBZS.li8K.d48aff5ebadb6c2842f21debf55d5235.21 | | x | | x | | x | | | | | | x | |
| Język rosyjski B-2 - kurs obowiązkowy 135 godzin - semestr 3/3 | IEiTCBZS.li8JO.49d62cc9cd39f7fb09b10f8cfbeb7b06.21 | | | | | | x | | | | | | | |
| Bezpieczeństwo bezprzewodowych sieci komputerowych | IEiTCBZS.li8K.d27b6ca4174208b96219300dc8b66f33.21 | x | x | | x | x | x | | | | x | x | x | x |
| Wprowadzenie do białego wywiadu | ICBZ00S.li8O.0b5550071879f4043c469fdeb715348a.21 | | | | x | | | | x | | | | x | x |
| Język hiszpański B-2 - kurs obowiązkowy 135 godzin - semestr 3/3 | IEiTCBZS.li8JO.001aefb3b9af1096e2664b81b183c217.21 | | | | | | x | | | | | | | |
| Język francuski B-2 - kurs obowiązkowy 135 godzin - semestr 3/3 | IEiTCBZS.li8JO.6807c4d8cf5331d62a78d10b502b9ccb.21 | | | | | | x | | | | | | | |
| Organizacje międzynarodowe a cyberbezpieczeństwo | IEiTCBZS.li8O.f19c2a2929936e5be73df19bee31a1cc.21 | | | | x | | x | x | x | | | | x | x |

| Przedmiot | Kod | | | | | | | | | | | | | |
|-----------------------------------------------------------------|------------------------------------------------------|----------|--------------|--------------|----------|----------|----------|----------|----------|-----------------|-----------------|----------|----------|----------|
| | | P6S_WG_A | P6S_WG_A_Inz | P6S_WK_A_Inz | P6S_WK_A | 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 |
| Bezpieczeństwo oprogramowania | IEiTCBZS.li8K.c513d1c8b0d66bc21f36b0d66843aed6.21 | x | x | x | x | x | | | x | | | | x | |
| Wykrywanie anomalii sieciowych z użyciem uczenia maszynowego | IEiTCBZS.li8K.9bf8eec690e06ffe497a16136fe6ba54.21 | x | x | | | x | x | x | x | | | x | x | x |
| Język angielski B-2 - kurs obowiązkowy 135 godzin - semestr 3/3 | IEiTCBZS.li8JO.5e50e9a2d67b5162c856cf859a9b227f.21 | | | | | | x | | | | | | | |
| Analiza malware | ICBZ00S.li8K.9a735e2e4d9290349cc2d3c6e0645580.21 | x | x | | | | | | | | | x | | x |
| Język niemiecki B-2 - kurs obowiązkowy 135 godzin - semestr 3/3 | IEiTCBZS.li8JO.e9248a9a134c74395721cf546e69ecdf.21 | | | | | | | x | | | | | | |
| Sprzętowe aspekty cyberbezpieczeństwa | IEiTCBZS.li8K.58c8910cc535d6f1d6bc4e5e93f181a9.21 | x | x | x | x | x | x | | x | x | | | | x |
| Ochrona danych osobowych i technologie wzmacniające prywatność | ICBZ00S.li8K.309676e6c264e6746facab38d407043d.21 | | x | x | x | | | | | | | x | | x |
| Bazy danych | IEiTCBZS.li8K.5eb52d767603909189082b3acc3bc79d.21 | x | x | | | | | x | | | | x | | x |
| Bezpieczeństwo systemów komórkowych i sieci 5G | ICBZ00S.li10K.07a1aae1f1265efb93f0898e8abc60d3.21 | x | x | | | x | x | x | | x | x | x | x | x |
| Cybersecurity and contemporary conflicts | IEiTCBZS.li10PJO.4bf2d4e680eb8d7947c02a56b2645766.21 | | | | x | x | | | x | | | x | x | x |
| Biometria | IEiTCBZS.li10K.91429ab6404d946c7103b476884a319e.21 | x | | | x | x | x | x | x | x | x | | x | x |
| Ochrona informacji niejawnych | IEiTCBZS.li10K.5145750c05a1e0f5f4fee1331cc9b831.21 | | | x | x | x | x | x | x | | | x | x | x |
| Wprowadzenie do inżynierii oprogramowania | IEiTCBZS.li100.64d08ad26e8621a021be9d5c4d3bd749.21 | x | x | | x | x | x | x | x | x | x | x | x | x |
| Szpiegostwo przemysłowe | IEiTCBZS.li10K.9c1e730c819991a3357a7bf4cba78a10.21 | | | x | x | | x | x | | | | | | x |
| Zarządzanie incydentami - SOC oraz CERT | IEiTCBZS.li10K.227fe3ba93083a2110975d2e455ee3ee.21 | | | | x | x | | | | | | | | |
| Bezpieczeństwo zwirtualizowanych środowisk IT | IEiTCBZS.li10K.ef382922cefd8ca87b9ae8529232839e.21 | | x | | | x | x | x | | | | x | x | |

| Przedmiot | Kod | | | | | | | | | | | | | | | |
|------------------------------------------------------------------------------|----------------------------------------------------|----------|--------------|--------------|----------|----------|----------|----------|----------|-----------------|-----------------|----------|----------|----------|---|---|
| | | P6S_WG_A | P6S_WG_A_Inz | P6S_WK_A_Inz | P6S_WK_A | 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 | | |
| Testy penetracyjne | ICBZ00S.li10K.f479bb92e5cf7662bceb74ac6fa7a783.21 | | | | x | | | | | | | | x | | x | x |
| Bezpieczeństwo w sieciach rozległych | IEiTCBZS.li10K.979f76511b5d2580af8495b6b015c523.21 | | x | | | | | | | | | | x | x | | |
| Koło naukowe | IEiTCBZS.li20K.6c2dd2a0521f52b7970d675b80f21b94.21 | x | x | x | x | x | x | x | x | | | | x | x | x | |
| Security of operating systems | IEiTCBZS.li20K.723aec15067ec466380d438e74eb4008.21 | x | x | | | x | | x | | | | | x | x | x | x |
| Podstawy analizy informacji | IEiTCBZS.li20K.26e3f0d4a7d9b4f869835eb856059e3c.21 | | | x | x | x | x | x | | | | | | | x | x |
| Praktyczne wykorzystanie informacji z otwartych źródeł | IEiTCBZS.li20K.5358cd5c2cc151ff51e3f9795cf439a2.21 | | | | x | | | | | x | | | | x | | |
| Wprowadzenie do informatyki kwantowej | IEiTCBZS.li20K.323b3a8026a0248b9af0042d78982777.21 | x | x | | x | | | | x | | x | | x | x | x | |
| Cyberbezpieczeństwo i prawo międzynarodowe | IEiTCBZS.li20K.8404c0d97150c18d899908a607671be4.21 | | | | x | | x | x | x | | | | x | x | x | |
| Krajowe zasoby informacyjne | IEiTCBZS.li20K.9f7b37ca8a4f07c2e1b5c11370ee5655.21 | | | | x | | x | x | | | | | | | x | |
| Bezpieczeństwo infrastruktury krytycznej i systemów sterowania przemysłowego | IEiTCBZS.li20K.849876180bf9bf13ceb476ebd9121a85.21 | | | | x | x | x | | | | | | | x | x | |
| Pracownia projektowa 1 | IEiTCBZS.li20K.c9b12ced59d14cdda72665b694ada6b5.21 | | | | | x | x | x | x | x | x | x | x | x | x | x |
| Praktyki zawodowe | IEiTCBZS.li20K.1eddd722812cb22a6375443a406368c2.21 | | | | | x | x | x | x | x | x | | | | x | x |
| Programowanie sieciowe wspierające aplikacje bezpieczne | IEiTCBZS.li20K.08d2f2e7b20c22e7544995348e6e43b0.21 | x | x | | | | | | | | | x | x | x | x | |
| Przedmiot obieralny z UBPJO | IEiTCBZS.li400.35a1dd1261eebe67f76be03858741abf.21 | | x | x | x | | x | x | x | | | | x | x | x | |
| Pracownia projektowa 2 | IEiTCBZS.li40K.7bf6e013d20aa0cde672e1d35ac09881.21 | | | | | x | x | x | x | x | | | | | x | x |
| Cyfrowe znaki wodne i steganografia | IEiTCBZS.li40K.0af9b507fbbcea58aab82f6595b336bf.21 | x | x | | | x | x | x | x | | | | x | x | x | x |
| Bezpieczeństwo IoT | IEiTCBZS.li40K.9293145073460f5412cf3e1129984344.21 | | x | | | | | x | x | x | | | x | | x | |

| Przedmiot | Kod | | | | | | | | | | | | | |
|------------------------------------------------------|----------------------------------------------------|----------|--------------|--------------|----------|----------|----------|----------|----------|-----------------|-----------------|----------|----------|----------|
| | | P6S_WG_A | P6S_WG_A_Inz | P6S_WK_A_Inz | P6S_WK_A | 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 |
| Projekt inżynierski | IEiTCBZS.li40K.f29d56545dbb5e5f3d4cafcbf5a1cbdb.21 | | | | | x | x | x | x | x | x | x | x | x |
| Blockchain | IEiTCBZS.li40K.d2deb71ea8bc391df097d4e423ff2c9e.21 | x | x | x | x | x | x | x | x | x | x | x | x | x |
| Kryptoanaliza | IEiTCBZS.li40K.750cac3b33cf095aa56e575c7e7864c9.21 | x | x | | x | x | | | | x | x | x | | x |
| Koło naukowe | IEiTCBZS.li40K.6c2dd2a0521f52b7970d675b80f21b94.21 | x | x | x | x | x | x | x | x | | | x | x | x |
| Cyberbezpieczeństwo a przetwarzanie danych w chmurze | IEiTCBZS.li40K.edaf0021ad67b2a5077d0da76f439fa1.21 | x | x | | x | | | x | x | | x | | x | |
| Suma: | | 33 | 34 | 9 | 36 | 39 | 49 | 39 | 24 | 17 | 36 | 41 | 43 | 37 |

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

Kierunek: Cyberbezpieczeństwo

2021/2022/S/li/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 |
|-------------------------------------------------------|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Wprowadzenie do prawa karnego i postępowania karnego | Wykład, Ćwiczenia audytoryjne | Odpowiedź ustna, Udział w dyskusji | CBZ1A_W06, CBZ1A_W07, CBZ1A_U09, CBZ1A_K06 |
| Wstęp do informatyki | Wykład, Ćwiczenia laboratoryjne | Aktywność na zajęciach, Kolokwium | CBZ1A_W01, CBZ1A_W03, CBZ1A_W02, CBZ1A_U03, CBZ1A_U04, CBZ1A_U08, CBZ1A_K01, CBZ1A_K05, CBZ1A_K06 |
| Wprowadzenie do sieci Internet | Wykład, Ćwiczenia laboratoryjne | Wykonanie ćwiczeń laboratoryjnych, Kolokwium, Zaliczenie laboratorium | CBZ1A_W04, CBZ1A_U03, CBZ1A_K02 |
| Analiza 1 | Wykład, Ćwiczenia audytoryjne | Aktywność na zajęciach, Kolokwium, Egzamin, Odpowiedź ustna | CBZ1A_W01, CBZ1A_U01, CBZ1A_K01 |
| Algebra | Wykład, Ćwiczenia audytoryjne | Egzamin, Aktywność na zajęciach | CBZ1A_W01, CBZ1A_U05, CBZ1A_U06, CBZ1A_U08, CBZ1A_K01, CBZ1A_K03 |
| Krajowy system cyberbezpieczeństwa | Wykład | Aktywność na zajęciach, Udział w dyskusji, Egzamin, Odpowiedź ustna | CBZ1A_W07, CBZ1A_W08, CBZ1A_W09, CBZ1A_U04, CBZ1A_U09, CBZ1A_K01, CBZ1A_K02, CBZ1A_K03, CBZ1A_K04, CBZ1A_K05, CBZ1A_K06 |
| Wstęp do administracji i bezpieczeństwa komputerowego | Wykład, Ćwiczenia laboratoryjne | Udział w dyskusji, Kolokwium, Wykonanie ćwiczeń laboratoryjnych, Zaliczenie laboratorium | CBZ1A_W10, CBZ1A_W05, CBZ1A_U07, CBZ1A_K01, CBZ1A_K03 |
| Matematyka dyskretna | Wykład, Ćwiczenia audytoryjne | Aktywność na zajęciach, Kolokwium, Egzamin, Odpowiedź ustna | CBZ1A_W01, CBZ1A_U02, CBZ1A_U03, CBZ1A_U01, CBZ1A_U08, CBZ1A_K02 |

| Nazwa modułu zajęć | Forma zajęć dydaktycznych | Sposób weryfikacji i oceny efektów uczenia się osiągniętych przez studenta w ramach poszczególnych form zajęć i dla całego modułu zajęć | Odniesienia do KEU |
|-------------------------------------------------------------------|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| 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 | CBZ1A_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 | CBZ1A_U02 |
| 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 | CBZ1A_U02 |
| Probabilistyka i statystyka | Wykład, Ćwiczenia audytorjne | Aktywność na zajęciach, Kolokwium, Egzamin, Udział w dyskusji | CBZ1A_W01, CBZ1A_W10, CBZ1A_U01, CBZ1A_U03, CBZ1A_K01, CBZ1A_K06 |
| 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 | CBZ1A_U02 |
| 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 | CBZ1A_U02 |
| Analiza 2 | Wykład, Ćwiczenia audytorjne | Aktywność na zajęciach, Kolokwium, Egzamin, Odpowiedź ustna | CBZ1A_W01, CBZ1A_U01, CBZ1A_K01 |
| Fizyka 1 | Wykład, Ćwiczenia audytorjne | 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 |
| Projektowanie i analiza algorytmów | Wykład, Ćwiczenia laboratoryjne | Aktywność na zajęciach, Kolokwium, Egzamin | CBZ1A_W01, CBZ1A_U01, 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 |
|-----------------------------------------------------------------|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Wykrywanie incydentów | Wykład, Ćwiczenia laboratoryjne | Wykonanie ćwiczeń laboratoryjnych, Kolokwium | CBZ1A_W09, CBZ1A_U10, CBZ1A_U07, CBZ1A_K06 |
| Podstawy programowania | Wykład, Ćwiczenia laboratoryjne | Wykonanie ćwiczeń laboratoryjnych | CBZ1A_W03, CBZ1A_U08, CBZ1A_K02 |
| Bezpieczeństwo systemów i sieci teleinformatycznych | Wykład, Ćwiczenia laboratoryjne | Wykonanie ćwiczeń laboratoryjnych, Kolokwium, Sprawozdanie, Zaliczenie laboratorium | CBZ1A_W01, CBZ1A_W04, CBZ1A_W05, CBZ1A_U01, CBZ1A_U06, CBZ1A_U07, CBZ1A_K01, CBZ1A_K04 |
| Zarządzanie bezpieczeństwem informacji | Wykład, Ćwiczenia laboratoryjne | Aktywność na zajęciach, Udział w dyskusji, Wykonanie projektu, Wykonanie ćwiczeń laboratoryjnych, Projekt, Zaangażowanie w pracę zespołu, Prezentacja, Odpowiedź ustna, Zaliczenie laboratorium | CBZ1A_W06, CBZ1A_W07, CBZ1A_W09, CBZ1A_W10, CBZ1A_U01, CBZ1A_U02, CBZ1A_U03, CBZ1A_U10, CBZ1A_U11, CBZ1A_U09, CBZ1A_K01, CBZ1A_K02, CBZ1A_K03, CBZ1A_K04, CBZ1A_K05, CBZ1A_K06 |
| Inżynieria społeczna | Wykład, Ćwiczenia laboratoryjne | Aktywność na zajęciach, Kolokwium, Prezentacja | CBZ1A_W09, CBZ1A_U03, CBZ1A_U10, CBZ1A_U09, CBZ1A_K02, CBZ1A_K03 |
| Język rosyjski B-2 - kurs obowiązkowy 135 godzin - semestr 2/3 | Lektorat | Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wynik testu zaliczeniowego, Wypracowania pisane na zajęciach, Prezentacja | CBZ1A_U02 |
| Język angielski B-2 - kurs obowiązkowy 135 godzin - semestr 2/3 | Lektorat | Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wynik testu zaliczeniowego, Wypracowania pisane na zajęciach, Prezentacja | CBZ1A_U02 |
| Bezpieczeństwo lokalnych sieci komputerowych | Wykład, Ćwiczenia laboratoryjne | Aktywność na zajęciach | CBZ1A_W04, CBZ1A_W05, CBZ1A_U01, CBZ1A_U07, CBZ1A_K01 |
| Bezpieczeństwo aplikacji webowych i mobilnych | Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe | Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych, Zaliczenie laboratorium, Wykonanie projektu, Projekt, Zaangażowanie w pracę zespołu, Prezentacja | CBZ1A_W03, CBZ1A_W04, CBZ1A_W10, CBZ1A_U01, CBZ1A_U03, CBZ1A_U05, CBZ1A_U02, CBZ1A_U04, CBZ1A_U08, CBZ1A_K01, CBZ1A_K02, CBZ1A_K05, CBZ1A_K06, CBZ1A_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 |
|------------------------------------------------------------------|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Informatyka śledcza | Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe | Wykonanie projektu, Wykonanie ćwiczeń laboratoryjnych | CBZ1A_W05, CBZ1A_W03, CBZ1A_W04, CBZ1A_U06, CBZ1A_K05 |
| Język francuski B-2 - kurs obowiązkowy 135 godzin - semestr 2/3 | Lektorat | Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wynik testu zaliczeniowego, Wypracowania pisane na zajęciach, Prezentacja | CBZ1A_U02 |
| Wstęp do zwalczania cyberprzestępczości | Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe | Aktywność na zajęciach, Udział w dyskusji, Koordynacja, realizacja projektu badawczego, przygotowanie referatu/publikacji, organizacja konferencji, obozów i wycieczek naukowych | CBZ1A_W09, CBZ1A_W07, CBZ1A_W08, CBZ1A_U03, CBZ1A_K02 |
| Język hiszpański B-2 - kurs obowiązkowy 135 godzin - semestr 2/3 | Lektorat | Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Esej, Wynik testu zaliczeniowego, Wypracowania pisane na zajęciach, Prezentacja | CBZ1A_U02 |
| Fizyka 2 | Wykład, Ćwiczenia audytorjne, 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 |
| Język niemiecki B-2 - kurs obowiązkowy 135 godzin - semestr 2/3 | Lektorat | Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wynik testu zaliczeniowego, Wypracowania pisane na zajęciach, Prezentacja | CBZ1A_U02 |
| Programowanie skryptowe | Wykład, Ćwiczenia laboratoryjne | Zaliczenie laboratorium | CBZ1A_W03, CBZ1A_U08, CBZ1A_K01 |
| Kryptografia | Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe | Egzamin, Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych | 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 |
| Systemy operacyjne | Wykład, Ćwiczenia laboratoryjne | Aktywność na zajęciach, Kolokwium, Udział w dyskusji, Wykonanie ćwiczeń laboratoryjnych | CBZ1A_W04, CBZ1A_U01, CBZ1A_U08, CBZ1A_K05, CBZ1A_K03 |

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

| Nazwa modułu zajęć | Forma zajęć dydaktycznych | Sposób weryfikacji i oceny efektów uczenia się osiągniętych przez studenta w ramach poszczególnych form zajęć i dla całego modułu zajęć | Odniesienia do KEU |
|------------------------------------------------------------------|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Analiza powłamaniowa | Wykład, Ćwiczenia projektowe | Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń | CBZ1A_W05, CBZ1A_W10, CBZ1A_U02, CBZ1A_K01 |
| Język rosyjski B-2 - kurs obowiązkowy 135 godzin - semestr 3/3 | Lektorat | Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wynik testu zaliczeniowego, Wypracowania pisane na zajęciach, Prezentacja | CBZ1A_U02 |
| Bezpieczeństwo bezprzewodowych sieci komputerowych | Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe | Kolokwium, Egzamin, Wykonanie ćwiczeń laboratoryjnych, Projekt | CBZ1A_W02, CBZ1A_W04, CBZ1A_W05, CBZ1A_W10, CBZ1A_U06, CBZ1A_U07, CBZ1A_U05, CBZ1A_U01, CBZ1A_U02, CBZ1A_K01, CBZ1A_K02, CBZ1A_K03, CBZ1A_K06 |
| Wprowadzenie do białego wywiadu | Wykład, Ćwiczenia projektowe | Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych, Projekt | CBZ1A_W09, CBZ1A_U03, CBZ1A_K01, CBZ1A_K05 |
| Język hiszpański B-2 - kurs obowiązkowy 135 godzin - semestr 3/3 | Lektorat | Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wynik testu zaliczeniowego, Wypracowania pisane na zajęciach, Prezentacja | CBZ1A_U02 |
| Język francuski B-2 - kurs obowiązkowy 135 godzin - semestr 3/3 | Lektorat | Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wynik testu zaliczeniowego, Wypracowania pisane na zajęciach, Prezentacja | CBZ1A_U02 |
| 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 |
| 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 |

| 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 |
|-----------------------------------------------------------------|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Wykrywanie anomalii sieciowych z użyciem uczenia maszynowego | Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe | Kolokwium, Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych, Odpowiedź ustna, Zaliczenie laboratorium, Udział w dyskusji, Projekt, Sprawozdanie, Studium przypadków, Prezentacja, Przygotowanie i przeprowadzenie badań | CBZ1A_W01, CBZ1A_W02, CBZ1A_W03, CBZ1A_W04, CBZ1A_W05, CBZ1A_U02, CBZ1A_U03, CBZ1A_U04, CBZ1A_U08, CBZ1A_U01, CBZ1A_U06, CBZ1A_K01, CBZ1A_K05, CBZ1A_K06 |
| Język angielski B-2 - kurs obowiązkowy 135 godzin - semestr 3/3 | Lektorat | Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wynik testu zaliczeniowego, Wypracowania pisane na zajęciach, Prezentacja | CBZ1A_U02 |
| Analiza malware | Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe | Wykonanie projektu, Wykonanie ćwiczeń laboratoryjnych | CBZ1A_W03, CBZ1A_W04, CBZ1A_W05, CBZ1A_U06, CBZ1A_K05 |
| Język niemiecki B-2 - kurs obowiązkowy 135 godzin - semestr 3/3 | Lektorat | Aktywność na zajęciach, Udział w dyskusji, Wykonanie ćwiczeń, Kolokwium, Egzamin, Wynik testu zaliczeniowego, Wypracowania pisane na zajęciach, Prezentacja | CBZ1A_U02 |
| Sprzętowe aspekty cyberbezpieczeństwa | Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe | Aktywność na zajęciach, Udział w dyskusji, Wykonanie projektu, Wykonanie ćwiczeń laboratoryjnych, Kolokwium, Projekt, Sprawozdanie, Prezentacja, Odpowiedź ustna, Zaliczenie laboratorium | CBZ1A_W02, CBZ1A_W07, CBZ1A_W01, CBZ1A_W09, CBZ1A_W10, CBZ1A_W03, CBZ1A_W05, CBZ1A_W04, CBZ1A_U05, CBZ1A_U07, CBZ1A_U08, CBZ1A_U10, CBZ1A_U06, CBZ1A_U01, CBZ1A_U02, CBZ1A_U03, CBZ1A_K05 |
| Ochrona danych osobowych i technologie wzmacniające prywatność | Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe | Wykonanie projektu, Wykonanie ćwiczeń laboratoryjnych | CBZ1A_W09, CBZ1A_W10, CBZ1A_W04, CBZ1A_W05, CBZ1A_U08, CBZ1A_U10, CBZ1A_K05 |
| Bazy danych | Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe | Kolokwium, Projekt, Prezentacja | CBZ1A_W03, CBZ1A_U08, CBZ1A_U03, CBZ1A_K02, 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 systemów komórkowych i sieci 5G | 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_U02, CBZ1A_U06, CBZ1A_U07, CBZ1A_K01, CBZ1A_K02 |
| Cybersecurity and contemporary conflicts | Wykład, Ćwiczenia audytoryjne, Ćwiczenia projektowe | Aktywność na zajęciach, Udział w dyskusji, Projekt, Studium przypadków, Odpowiedź ustna, Zaangażowanie w pracę zespołu, Prezentacja, Wykonanie projektu | CBZ1A_W08, CBZ1A_W09, CBZ1A_U04, CBZ1A_U10, CBZ1A_K01, CBZ1A_K02, CBZ1A_K04, CBZ1A_K05, CBZ1A_K06 |
| 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_U02, CBZ1A_U04, CBZ1A_U09, CBZ1A_U01, CBZ1A_U05, CBZ1A_U08, CBZ1A_U06, CBZ1A_U03, CBZ1A_U10, CBZ1A_U11, CBZ1A_K02, CBZ1A_K06, CBZ1A_K03, 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_K01, CBZ1A_K02, CBZ1A_K03, CBZ1A_K04, CBZ1A_K05, CBZ1A_K06 |
| Wprowadzenie do inżynierii oprogramowania | Wykład, Ćwiczenia projektowe | Egzamin | CBZ1A_W01, CBZ1A_W02, CBZ1A_W03, CBZ1A_W07, CBZ1A_W08, CBZ1A_W09, CBZ1A_W10, CBZ1A_U01, CBZ1A_U02, CBZ1A_U03, CBZ1A_U04, CBZ1A_U05, CBZ1A_U08, CBZ1A_U09, CBZ1A_U10, CBZ1A_U11, CBZ1A_K01, CBZ1A_K02, CBZ1A_K03, CBZ1A_K06 |
| Szpiegostwo przemysłowe | Wykład, Ćwiczenia projektowe, Zajęcia seminaryjne | Odpowiedź ustna, Udział w dyskusji | CBZ1A_W06, CBZ1A_W07, CBZ1A_U09, 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 |
|--------------------------------------------------------|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Zarządzanie incydentami - SOC oraz CERT | Wykład, Ćwiczenia projektowe | Aktywność na zajęciach, Projekt, Egzamin | CBZ1A_W07, CBZ1A_W08, CBZ1A_W10, CBZ1A_W09, CBZ1A_U10 |
| 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 |
| Testy penetracyjne | Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe | Wykonanie projektu, Wykonanie ćwiczeń laboratoryjnych | CBZ1A_W10, CBZ1A_U06, CBZ1A_K03, CBZ1A_K06 |
| Bezpieczeństwo w sieciach rozległych | Ćwiczenia laboratoryjne | Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych, Egzamin, Studium przypadków | CBZ1A_W04, CBZ1A_W05, CBZ1A_U07, CBZ1A_K01 |
| Koło naukowe | Praca w kole naukowym | Koordinacja, 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 |
| Security of operating systems | Wykład, Ćwiczenia laboratoryjne | Aktywność na zajęciach, Udział w dyskusji, Kolokwium, Studium przypadków, Zaangażowanie w pracę zespołu, Zaliczenie laboratorium | CBZ1A_W04, CBZ1A_W03, CBZ1A_U06, CBZ1A_U07, CBZ1A_U01, CBZ1A_U03, CBZ1A_K01, CBZ1A_K02, CBZ1A_K03 |
| Podstawy analizy informacji | Wykład, Ćwiczenia laboratoryjne | Aktywność na zajęciach, Udział w dyskusji, Odpowiedź ustna | CBZ1A_W08, CBZ1A_W09, CBZ1A_W10, CBZ1A_W07, CBZ1A_W06, CBZ1A_U01, CBZ1A_U02, CBZ1A_U09, CBZ1A_U10, CBZ1A_U11, CBZ1A_K04, CBZ1A_K05, CBZ1A_K06 |
| Praktyczne wykorzystanie informacji z otwartych źródeł | Wykład, Ćwiczenia laboratoryjne | Aktywność na zajęciach | CBZ1A_W09, CBZ1A_U04, CBZ1A_K01 |
| 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 |

| 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 |
|------------------------------------------------------------------------------|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 |
| Krajowe zasoby informacyjne | Wykład, Ćwiczenia laboratoryjne | Odpowiedź ustna, Udział w dyskusji | CBZ1A_W10, CBZ1A_W09, CBZ1A_W07, CBZ1A_U09, CBZ1A_K06 |
| Bezpieczeństwo infrastruktury krytycznej i systemów sterowania przemysłowego | Wykład, Ćwiczenia laboratoryjne | Egzamin | CBZ1A_W08, CBZ1A_U11, CBZ1A_U10, CBZ1A_K01, CBZ1A_K02 |
| Pracownia projektowa 1 | Ćwiczenia laboratoryjne | Udział w dyskusji, Zaangażowanie w pracę zespołu, Zaliczenie laboratorium | CBZ1A_U01, CBZ1A_U02, CBZ1A_U03, CBZ1A_U04, CBZ1A_U05, CBZ1A_U08, CBZ1A_U09, CBZ1A_U06, CBZ1A_U07, CBZ1A_U10, CBZ1A_U11, CBZ1A_K01, CBZ1A_K02, CBZ1A_K03, CBZ1A_K04, CBZ1A_K05 |
| Praktyki zawodowe | Ćwiczenia projektowe, Zajęcia praktyczne | Prezentacja, Udział w pracach badawczych, konferencjach, dodatkowych stażach i szkoleniach, Przygotowanie i przeprowadzenie badań, Praca wykonana w ramach praktyki | CBZ1A_U01, CBZ1A_U02, CBZ1A_U05, CBZ1A_U08, CBZ1A_U03, CBZ1A_U04, CBZ1A_K02, CBZ1A_K03, CBZ1A_K05, CBZ1A_K06, CBZ1A_K04 |
| Programowanie sieciowe wspierające aplikacje bezpieczne | Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe | Aktywność na zajęciach, Wykonanie ćwiczeń laboratoryjnych, Kolokwium | CBZ1A_W04, CBZ1A_W05, CBZ1A_W03, CBZ1A_U06, CBZ1A_U08, CBZ1A_U07, CBZ1A_U05, CBZ1A_K01, CBZ1A_K02 |
| Przedmiot obieralny z UBPJO | Wykład, Ćwiczenia laboratoryjne | Aktywność na zajęciach | CBZ1A_W04, CBZ1A_W07, CBZ1A_W08, CBZ1A_W05, CBZ1A_W06, CBZ1A_U02, CBZ1A_U03, CBZ1A_U04, CBZ1A_K01, CBZ1A_K04, CBZ1A_K05 |
| Pracownia projektowa 2 | Ćwiczenia projektowe | Prezentacja, Udział w pracach badawczych, konferencjach, dodatkowych stażach i szkoleniach, Koordynacja, realizacja projektu badawczego, przygotowanie referatu/publikacji, organizacja konferencji, obozów i wycieczek naukowych | CBZ1A_U01, CBZ1A_U02, CBZ1A_U03, CBZ1A_U05, CBZ1A_U04, CBZ1A_U10, CBZ1A_K03, CBZ1A_K04, CBZ1A_K05, 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 |
|------------------------------------------------------|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cyfrowe znaki wodne i steganografia | Wykład, Ćwiczenia laboratoryjne, Ćwiczenia projektowe | Kolokwium, Projekt, Prezentacja | CBZ1A_W01, CBZ1A_W02, CBZ1A_U02, CBZ1A_U03, CBZ1A_U04, CBZ1A_U08, CBZ1A_U01, CBZ1A_U06, CBZ1A_K01, CBZ1A_K05, CBZ1A_K06 |
| Bezpieczeństwo IoT | Wykład, Ćwiczenia projektowe | Wykonanie projektu, Projekt | CBZ1A_W04, CBZ1A_U02, CBZ1A_U03, CBZ1A_U04, CBZ1A_U07, CBZ1A_K02 |
| Projekt inżynierski | 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 |
| Blockchain | Wykład, Ćwiczenia projektowe | Wykonanie projektu, Projekt | CBZ1A_W01, CBZ1A_W03, CBZ1A_W05, CBZ1A_W06, CBZ1A_W07, CBZ1A_W08, CBZ1A_W09, CBZ1A_W10, CBZ1A_U01, CBZ1A_U02, CBZ1A_U03, CBZ1A_U04, CBZ1A_U05, CBZ1A_U07, CBZ1A_U08, CBZ1A_U09, CBZ1A_U10, CBZ1A_U11, CBZ1A_K01, CBZ1A_K03, CBZ1A_K04 |
| Kryptoanaliza | Wykład, Ćwiczenia laboratoryjne | Aktywność na zajęciach, Egzamin, Wynik testu zaliczeniowego, Wykonanie ćwiczeń laboratoryjnych | CBZ1A_W01, CBZ1A_W03, CBZ1A_W05, CBZ1A_W04, CBZ1A_W09, CBZ1A_K05, CBZ1A_U01, CBZ1A_U08, CBZ1A_U05, CBZ1A_U06, CBZ1A_K01, CBZ1A_K03 |
| Koło naukowe | Praca w kole naukowym | Koordinacja, 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 |
| 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 |

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 | 105 |
| zajęć z zakresu nauk podstawowych właściwych dla danego kierunku studiów | 35 |
| 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) | 75 |
| 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 | 13 |
| zajęć z języka obcego | 5 |
| 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

Par. 17 Regulaminu Studiów AGH dokładnie określa zasady wpisu na kolejny semestr:

https://samorzad.agh.edu.pl/wp-content/uploads/2017/12/regulamin_studiow_pierwszego_i_drugiego_stopnia_w_agh_pazdzienik_2017.pdf

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

Par. 17 Regulaminu Studiów AGH dokładnie określa zasady wpisu na kolejny semestr w ramach tzw. dopuszczalnego deficytu punktów ECTS:

https://samorzad.agh.edu.pl/wp-content/uploads/2017/12/regulamin_studiow_pierwszego_i_drugiego_stopnia_w_agh_pazdzienik_2017.pdf

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

5, 7

Zasady odbywania studiów według indywidualnej organizacji studiów

Par. 9 Regulaminu Studiów AGH dokładnie określa zasady indywidualizacji procesu kształcenia:

https://samorzad.agh.edu.pl/wp-content/uploads/2017/12/regulamin_studiow_pierwszego_i_drugiego_stopnia_w_agh_pazdzienik_2017.pdf

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. Organizacja praktyk jest koordynowana przez Opiekuna Praktyk Studenckich dla kierunku Informatyka. Na Wydziale dostępna jest procedura obsługi praktyk dostępna na stronie: <http://www.iet.agh.edu.pl/pl/studenci/procedury/praktyka/>.

Zasady obieralności modułów zajęć

Praktycznie każdy semestr posiada pewną liczbę przedmiotów obieralnych. Na pierwszych semestrach jest to język obcy czy też przedmiot humanistyczny a rozpoczynając od trzeciego semestru są to przedmioty kierunkowe. Przed rozpoczęciem semestru zostają zebrane preferencje studentów co do zapisów na przedmioty kierunkowe, następnie studenci przypisywani są do konkretnych zajęć przez Pełnomocnika Dziekana ds. Studenckich kierunku. Priorytet wyboru konkretnych przedmiotów mają osoby które osiągają lepsze rezultaty na przedmiotach w poprzednim semestrze wybranych przez Pełnomocnika.

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

Par. 25 i 26 Regulaminu Studiów AGH dokładnie określają zasady przygotowania projektów dyplomowych oraz dyplomowania:

https://samorzad.agh.edu.pl/wp-content/uploads/2017/12/regulamin_studiow_pierwszego_i_drugiego_stopnia_w_agh_pazdzienik_2017.pdf

Student przygotowuje pracę w ramach Pracowni Projektowej realizowanej na 6 i 7 semestrze oraz Projektu Inżynierskiego realizowanego na 7 semestrze. Projekt Inżynierski prowadzony jest przez promotora pracy, natomiast Pracownia Projektowa jest prowadzona przez doświadczonych pracowników naukowych, którzy dbają o sam proces tworzenia projektu dyplomowego.

Zasady ustalania ogólnego wyniku ukończenia studiów

Par. 27 Regulaminu Studiów AGH dokładnie określa zasady ustalania ogólnego wyniku ukończenia studiów:

https://samorzad.agh.edu.pl/wp-content/uploads/2017/12/regulamin_studiow_pierwszego_i_drugiego_stopnia_w_agh_pazdzienik_2017.pdf

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

Brak