

### Program studiów

Kierunek studiów:	automatyka i informatyka przemysłowa
Poziom studiów:	studia drugiego stopnia
Profil studiów:	ogólnoakademicki
Formy studiów:	studia stacjonarne studia niestacjonarne
Liczba semestrów:	3
Liczba punktów ECTS konieczna do ukończenia studiów:	90 ECTS
Tytuł zawodowy nadawany absolwentom:	magister inżynier
Kierunek studiów jest przyporządkowany do dyscyplin:	automatyka, elektronika, elektrotechnika i technologie kosmiczne 75% – dyscyplina wiodąca; informatyka techniczna i telekomunikacja 25%
Łączna liczba godzin zajęć:	studia stacjonarne: 1000 studia niestacjonarne: 638
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia:	studia stacjonarne: 45 ECTS studia niestacjonarne: 36 ECTS
Liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć z dziedziny nauk humanistycznych lub nauk społecznych – w przypadku kierunków studiów przyporządkowanych do dyscyplin w ramach dziedzin innych niż odpowiednio nauki humanistyczne lub nauki społeczne:	5 ECTS
Wymiar oraz liczba punktów ECTS, jaką student musi uzyskać w ramach praktyk zawodowych:	program nie przewiduje praktyki
Zasady i forma odbywania praktyk zawodowych:	program nie przewiduje praktyki

### Efekty uczenia się

Symbol	Zakładane efekty uczenia się	Odniesienie do charakterystyk drugiego stopnia efektów uczenia się Polskiej Ramy Kwalifikacji
<b>Wiedza: zna i rozumie</b>		
K2A_W1	W pogłębionym stopniu – zagadnienia stanowiące zaawansowaną wiedzę ogólną z zakresu dyscyplin naukowych, do których przyporządkowano studiowany kierunek, przydatne do formułowania i rozwiązywania złożonych zadań inżynierskich charakterystycznych dla automatyki i informatyki przemysłowej	P7S_WG
K2A_W2	Wybrane zagadnienia z zakresu zaawansowanej wiedzy szczegółowej związanej z automatyką i informatyką przemysłową, a także podstaw cyberbezpieczeństwa, modelowania zagrożeń.	P7S_WG
K2A_W3	Główne tendencje rozwojowe dyscyplin naukowych, do których przyporządkowany jest kierunek studiów automatyka i informatyka przemysłowa	P7S_WG
K2A_W4	Podstawowe procesy zachodzące w cyklu życia urządzeń, obiektów i systemów technicznych oraz metody, techniki, narzędzia i materiały stosowane przy rozwiązywaniu złożonych zadań inżynierskich związanych z automatyką i informatyką przemysłową.	P7S_WG inż. P7S_WK inż.
K2A_W5	Podstawowe zasady tworzenia i rozwoju różnych form indywidualnej przedsiębiorczości.	P7S_WK
K2A_W6	Społeczne, ekonomiczne, prawne, etyczne i inne pozatechniczne uwarunkowania działalności inżynierskiej, w tym zasady ochrony własności przemysłowej i prawa autorskiego, a także zagadnienia związane z Europejskim i krajowym systemem cyberbezpieczeństwa oraz standaryzacją i certyfikacją cyberbezpieczeństwa	P7S_WK
K2A_W7	Podstawowe problemy i dylematy współczesnej cywilizacji właściwe dla programu studiów kierunku automatyka i informatyka przemysłowa, w tym związane z wykorzystywaniem sztucznej inteligencji.	P7S_WK
K2A_W8	Metody i techniki projektowania systemów automatyki oraz informatyki przemysłowej z uwzględnieniem cyberbezpieczeństwa, w tym bezpieczeństwa: aplikacji webowych, chmury obliczeniowej, infrastruktury sieciowej i systemów przemysłowych	P7S_WG

<b>Umiejętności: potrafi</b>		
K2A_U1	Wykorzystywać posiadaną wiedzę do identyfikacji, formułowania i rozwiązywania złożonych i nietypowych problemów inżynierskich związanych z automatyką i informatyką przemysłową, z uwzględnieniem zagadnień bezpieczeństwa (w tym bezpieczeństwa aplikacji webowych, chmury obliczeniowej, infrastruktury sieciowej i systemów przemysłowych) poprzez właściwy dobór źródeł i informacji z nich pochodzących oraz dobór i przystosowanie właściwych metod i narzędzi (istniejących lub samodzielnie opracowanych), w tym zaawansowanych technik informacyjno-komunikacyjnych	P7S_UW
K2A_U2	Formułować i testować hipotezy związane z prostymi problemami badawczymi z zakresu automatyki i informatyki przemysłowej.	P7S_UW
K2A_U3	Planować i przeprowadzać eksperymenty, w tym pomiary i symulacje komputerowe, interpretować uzyskane wyniki i wyciągać wnioski.	P7S_UW nż..
K2A_U4	Przy identyfikacji i formułowaniu specyfikacji zadań inżynierskich z zakresu automatyki i informatyki przemysłowej 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;	P7S_UW inż.
K2A_U5	Dokonywać krytycznej analizy sposobu funkcjonowania istniejących rozwiązań technicznych i oceniać te rozwiązania.	P7S_UW inż.
K2A_U6	Zaprojektować - zgodnie z zadaną specyfikacją - oraz wykonać typowe dla automatyki i informatyki przemysłowej złożone urządzenie, obiekt, system lub zrealizować proces, używając właściwych metod, technik, narzędzi i materiałów.	P7S_UW inż.
K2A_U7	Pracować indywidualnie i w zespole, przyjmując w nim różne role, w tym rolę wiodącą; potrafi kierować pracą zespołu	P7S_U0
K2A_U8	Komunikować się na tematy specjalistyczne ze zróżnicowanymi kręgami odbiorców i prowadzić debatę z użyciem specjalistycznej terminologii i nowoczesnych technologii informacyjno-komunikacyjnych, potrafi prowadzić debatę	P7S_UK
K2A_U9	Posługiwać się językiem obcym na poziomie B2+ oraz specjalistyczną terminologią charakterystyczną dla dyscyplin do których przyporządkowany jest kierunek studiów automatyka i informatyka przemysłowa	P7S_UW P7S_UW nż..
K2A_U10	Samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie.	P7S_UU
K2A_U11	Stosować zaawansowane metody i techniki obliczeniowe oraz zintegrowane systemy do modelowania i optymalizacji układów automatyki przemysłowej.	P7S_UW P7S_nż.inż.
K2A_U12	Wybrać i używać zaawansowane narzędzia informatyczne wspomagające automatyzację i informatyzację oraz robotyzację procesów technologicznych w tym ich cyberbezpieczeństwo	P7S_UW
<b>Kompetencje społeczne: jest gotów do</b>		
K2A_K1	Krytycznej oceny posiadanej wiedzy i odbieranych treści, uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięgnięcia opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu.	P7S_KK
K2A_K2	Wypełniania zobowiązań społecznych, inspirowania i organizowania działalności na rzecz środowiska społecznego, inicjowania działań na rzecz interesu publicznego, myślenia i działania w sposób kreatywny i przedsiębiorczy.	P7S_K0
K2A_K3	Odpowiedzialnego pełnienia ról zawodowych, z uwzględnieniem zmieniających się potrzeb społecznych, rozwijania dorobku zawodu, podtrzymywania etosu zawodu, przestrzegania i rozwijania etyki zawodowej oraz działania na rzecz przestrzegania tych zasad; ma świadomość ważności i zrozumienie pozatechnicznych aspektów i skutków działalności inżynierskiej.	P7S_KR

## Learning outcomes

<b>_Symbol</b>	<b>Assumed learning outcomes</b>	<b>Reference to the characteristics of the second cycle of learning outcomes of the Polish Qualifications Framework</b>
<b>Knowledge: knows and understands</b>		
K2A_W1	At an in-depth level - issues constituting advanced general knowledge in the field of scientific disciplines to which the studied field is assigned, useful for formulating and solving complex engineering tasks characteristic of automation and industrial IT	P7S_WG
K2A_W2	Selected topics in advanced detailed knowledge related to automation and industrial computing, as well as basics of cybersecurity and threat modelling.	P7S_WG
K2A_W3	The main development trends of the scientific disciplines to which the field of study - automation and industrial informatics - is assigned	P7S_WG
K2A_W4	Basic processes occurring in the life cycle of technical equipment, objects and systems and the methods, techniques, tools and materials used in solving complex engineering tasks related to automation and industrial informatics	P7S_WG inż. P7S_WK inż.
K2A_W5	Basic principles for the creation and development of various forms of individual business.	P7S_WK
K2A_W6	Social, economic, legal, ethical and other non-technical determinants of engineering activities, including the principles of industrial property protection and protection of	P7S_WK

	copyright, as well as issues related to the European and national cyber-security framework and cyber-security standardisation and certification	
K2A_W7	Fundamental problems and dilemmas of modern civilisation relevant to the study programme of industrial automation and informatics, including issues related to the use of artificial intelligence.	P7S_WK
K2A_W8	Methods and techniques for the design of automation systems and industrial information technology with a focus on cybersecurity, including the security of: web applications, cloud computing, network infrastructure and industrial systems	P7S_WG
<b>Skills: is able to</b>		
K2A_U1	Apply acquired knowledge to identify, formulate and solve complex and non-standard engineering problems related to automation and industrial informatics, taking into account security issues (including security of web applications, cloud computing, network infrastructures and industrial systems) through the appropriate selection of sources and information from them and the selection and adaptation of appropriate methods and tools (existing or independently developed), including advanced information and communication techniques	P7S_UW
K2A_U2	Formulate and test hypotheses related to simple research problems in automation and industrial informatics,	P7S_UW
K2A_U3	Plan and perform experiments, including measurements and computer simulations, evaluate the results obtained and draw conclusions	P7S_UW inż.
K2A_U4	In identifying and formulating specifications of engineering tasks in the field of automation and industrial computing and their solution: - use analytical, simulation and experimental methods, - recognise their system and non-technical aspects, including ethical aspects, - make a preliminary economic assessment of proposed solutions and engineering actions taken	P7S_UW inż.
K2A_U5	Critically analyze how existing technical solutions work and evaluate these solutions	P7S_UW inż.
K2A_U6	Design - according to a given specification - and manufacture a complex device, object, system or process typical of automation and industrial informatics, using appropriate methods, techniques, tools and materials.	P7S_UW inż.
K2A_U7	Work individually and as part of a team, taking on a variety of roles within the team, including leadership; can lead the work of the team	P7S_UO
K2A_U8	Communicate on specialized topics with a diverse audience and conduct debate using specialized terminology and modern information and communication technologies, is able to debate	P7S_UK
K2A_U9	Use a foreign language at B2+ level and the specialized terminology specific to the disciplines to which the field of study automation and industrial informatics is assigned	P7S_UW P7S_UW inż.
K2A_U10	Independently plan and implement their own lifelong learning and guide others in this area	P7S_UU
K2A_U11	Apply advanced computational methods and techniques and integrated systems to the modelling and optimization of industrial automation systems.	P7S_UW P7S_UW inż.
K2A_U12	Select and use advanced IT tools to support automation, computerisation and robotisation of technological processes including their cybersecurity	P7S_UW
<b>Social competences: is ready to</b>		
K2A_K1	Critically evaluate the knowledge they have and the content they receive, recognise the importance of knowledge in solving cognitive and practical problems, and seek expert advice when they have difficulty solving a problem themselves.	P7S_KK
K2A_K2	Fulfil social responsibilities, inspire and organize activities for the social environment, initiate actions in the public interest, think and act creatively and entrepreneurially	P7S_KO
K2A_K3	Perform professional roles responsibly, taking into account the changing needs of society, develop the achievements of the profession, uphold the ethos of the profession, observe and develop professional ethics and act to uphold these principles; is aware of the importance and understanding of the non-technical aspects and impacts of engineering activities.	P7S_KR

## Zajęcia i grupy zajęć

nazwa zajęć lub grupy zajęć	Liczba punktów ECTS	Efekty uczenia się (symbol) przypisane do zajęć lub grupy zajęć	Treści programowe zapewniające uzyskanie efektów uczenia się
Język obcy Foreign language	4	K2A_U8 K2A_U9	Tematyka/słownictwo, funkcje komunikacyjne i struktury gramatyczne na wybranym poziomie biegłości językowej.
HES	5	K2A_W5 K2A_W6 K2A_U4 K2A_K2 K2A_K3	Zarządzanie kadrami – jego elementy i uwarunkowania. Zaawansowane procedury, metody i instrumenty zarządzania kadrami. Definicja i klasyfikacja własności intelektualnej. Prawo autorskie i prawa pokrewne. Prawo własności przemysłowej.

Zajęcia kierunkowe obowiązkowe Obligatory core courses	11	K2A_W1 K2A_W3 K2A_U4 K2A_U11	<p>Repetitorium z podstaw automatyki (układy liniowe). Układy regulacji z opóźnieniem. Układy kaskadowe. Układy zamknięto-otwarte. Sterowanie układami nieliniowymi. Charakterystyki układów nieliniowych. Metoda płaszczyzny fazowej. Metoda funkcji opisującej. Stabilność układów nieliniowych – druga i pierwsza metoda Lapunowa. Układy regulacji przekąźnikowej. Nieliniowe układy dyskretne. Repetitorium techniki cyfrowej, cyfrowe bloki funkcjonalne, kody detekcyjne i korekcyjne, metoda tablic kolejności łączeń. Systemy sterowania związane z bezpieczeństwem, funkcje bezpieczeństwa, poziomy nienaruszalności bezpieczeństwa – SIL i poziomy zapewnienia bezpieczeństwa – Performance Level. Sprzęt i oprogramowanie implementujące funkcje bezpieczeństwa.</p> <p>Określanie modelu matematycznego rozpatrywanego obiektu/procesu, zmiennych decyzyjnych i ograniczeń oraz funkcji celu. Klasyfikacja zadań optymalizacji, Metody numeryczne programowania liniowego i nieliniowego. Optymalizacja wielokryterialna. Optymalizacja w hierarchicznej strukturze sterowania i zarządzania.</p>
Zajęcia kierunkowe – zwiastuny ścieżek dyplomowania Core courses – preview of graduation tracks	12	K2A_W4 K2A_W6 K2A_W8 K2A_U1 K2A_U7 K2A_U12 K2A_K1	<p>Systemy SCADA: sprzęt, oprogramowanie, technologie komunikacyjne, przykładowe systemy.</p> <p>Charakterystyka bezpieczeństwa informacji, rozumienie pojęcia cyberbezpieczeństwa, charakterystyka cyberzagrożeń, zarządzanie cyberbezpieczeństwem w organizacjach, wykorzystanie matryc MITRE ATT&amp;CK, prowadzenie audytów bezpieczeństwa informacji, narzędzia wykorzystywane w celu monitorowania cyberbezpieczeństwa oraz prowadzeniu audytów.</p> <p>Magistrale i protokoły komunikacyjne stosowane w rozproszonych systemach sterowania: RS-485, Modbus, Profibus, DeviceNet, różne odmiany Ethernetu przemysłowego (p. EtherCAT, Profinet), AS-i, HART, komunikacja bezprzewodowa. Stochastyczne modele kolejkowe protokołów transmisyjnych. Przemysłowy internet rzeczy (IIoT) i jego zastosowania w logistyce i produkcji.</p>
Ścieżka dyplomowania: automatyka i informatyka przemysłowa/The graduation track: Automatic control and industrial informatics – moduł zgodny z 12 celem Zrównoważonego Rozwoju: Zrównoważona konsumpcja i produkcja	58	K2A_W1 K2A_W2 K2A_W3 K2A_W6 K2A_W7 K2A_U1 K2A_U2 K2A_U3 K2A_U4 K2A_U5 K2A_U6 K2A_U7 K2A_U8 K2A_U10 K2A_U12 K2A_K1 K2A_K3	<p>Akwizycja obrazów cyfrowych, czujniki obrazów, rozpoznawanie obrazów: struktura ciągu przetwarzania informacji wizyjnej, zasady przetwarzania obrazów cyfrowych, przekształcenia skali szarości i korekta geometrii obrazów; rozpoznawanie obiektów na obrazach, optyczne przyrządy pomiarowe, przemysłowe i kontrolne; odtwarzanie obrazów, uwydatnianie treści obrazów; przyrządy i systemy laserowe. Termowizja i jej zastosowania. Techniki pomiarowe wielkości nieelektrycznych, pomiary: temperatury, sił i momentów, ciśnienia, poziomu, drgań i wstrząsów, hałasu, prędkości i przepływu płynów, wilgotności.</p> <p>Modele obiektów. Klasyfikacja metod identyfikacji. Identyfikacja charakterystyk statycznych. Podstawowe metody identyfikacji obiektów dynamicznych. Identyfikacja obiektów z opóźnieniem. Wsadowe i rekursywne metody estymacji. Identyfikacja w układzie zamkniętym. Identyfikacja obiektów niestacjonarnych.</p> <p>Modelowanie procesów sekwencyjnych z wykorzystaniem sieci Petriego i języka SFC/GRAFSET. Specyfika i działanie elementów bibliotecznych zgodnych z normą IEC61131. Wykorzystanie elementów dwustanowych, detektorów zbocza sygnału, czasomierzy, liczników. Praktyczne realizacje regulatorów w sterownikach programowalnych: regulator PID, regulator dwupołożeniowy/trójpołożeniowy, przykłady realizacji. Przykłady wykorzystania PLC do sterowania wybranymi procesami dyskretnymi i ciągłymi. Sterowniki PLC w napędzie elektrycznym. Panele HMI i ich programowanie.</p> <p>Regulacja adaptacyjna. Regulacja predykcyjna. Układy regulacji z modelem obiektu. Układy regulacji ekstremalnej. Sterowanie optymalne. Regulatory rozmyte. Dynamiczna linearyzacja układów nieliniowych. Odtwarzanie zmiennych stanu. Filtr Kalmana. Przebiegi stochastyczne w liniowych i nieliniowych układach regulacji. Złożone, wielowymiarowe układy sterowania ze sprzężeniami skrośnymi – metody odsprężania.</p> <p>Algorytmy sztucznej inteligencji: głębokie uczenie, uczenie maszynowe, uczenie ze wzmocnieniem. Systemy autonomiczne, samodzielnie podejmujące decyzje i sterujące procesami bez interwencji człowieka. Analiza danych i Big Data. Rozmywanie i wyostrzenie wielkości wejściowych i wyjściowych. Rozmyte bazy reguł i podstawy wnioskowania rozmytego. Logika rozmyta w podejmowaniu decyzji. Konfiguracje i algorytmy uczenia sztucznych sieci neuronowych. Sztuczne sieci neuronowe w analizie i klasyfikacji danych. Algorytmy ewolucyjne w rozwiązywaniu zadań optymalizacyjnych. Wykorzystanie sztucznej inteligencji w monitorowaniu i sterowaniu przebiegiem procesów produkcyjnych. Diagnostyka maszyn i urządzeń oraz wsparcie utrzymania ruchu. Prognozowanie popytu i optymalizacja zapasów. Generatywna sztuczna inteligencja. Modele lingwistyczne i ich zastosowanie.</p> <p>Realizacja projektu PBL w wybranym obszarze tematycznym zgodnym z kierunkiem studiów/wybraną ścieżką dyplomowania.</p> <p>W ramach zajęć realizowanych w j. angielskim posługiwanie się specjalistyczną terminologią związaną obranym kierunkiem studiów na</p>

			<p>poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego. Wstęp do rozproszonych systemów sterowania-- architektura, cechy, trendy rozwojowe (np. przemysł 4.0) Wybrane elementy rozproszonego sterowania-- sterowniki, moduły we/wy, moduły komunikacyjne i konwertery protokołów, elementy interfejsu użytkownika (panele HMI), moduły specjalistyczne (np. wagowe, pomiarowe, do stref zagrożonych wybuchem itp.). Opóźnienia w rozproszonych układach sterowania i ich wpływ na pracę układu. Zalety i wady rozproszonych układów sterowania. Bezpieczeństwo funkcjonalne w rozproszonych układach sterowania-- znaczenie bezpieczeństwa funkcjonalnego, podstawowe normy. Przykłady zastosowań rozproszonych układów sterowania.</p> <p>Budowa manipulatora 6-osiowego, funkcje kontrolera robota, kalibrowanie czujników przegubów robota, rodzaje pracy robota: ręczny i automatyczny, ręczne sterowanie robota za pomocą przenośnego sterowniczego (teach-pendant), prędkości ruchów zapewniające bezpieczeństwo podczas ręcznego sterowania, funkcje bezpieczeństwa celi zrobotyzowanej, programowanie robota w języku RAPID, instrukcje (ruchu, sterujące, warunkowe, przerwań) projektowanie wirtualnych celi zrobotyzowanych w programie RobotStudio, programowanie zadanych trajektorii wirtualnych i rzeczywistych robotów.</p> <p>Seminarium dyplomowe. Praca dyplomowa.</p>
<p>Ścieżka dyplomowania: Cyberbezpieczeństwo systemów przemysłowych/ The graduation track: Cybersecurity of industrial systems – moduł zgodny z 12 celem Zrównoważonego Rozwoju: Zrównoważona konsumpcja i produkcja</p>	58	<p>K2A_W1 K2A_W2 K2A_W3 K2A_W6 K2A_W7 K2A_U1 K2A_U2 K2A_U3 K2A_U4 K2A_U5 K2A_U6 K2A_U7 K2A_U8 K2A_U10 K2A_U12 K2A_K1 K2A_K3</p>	<p>Środki legislacyjne w standaryzacji i certyfikacji cyberbezpieczeństwa (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 wraz z aktualizacjami, Ustawa o Krajowym Systemie Cyberbezpieczeństwa, Narodowe Standardy Cyberbezpieczeństwa, Common Criteria – norma PN-ISO/IEC 15408); krajowy system cyberbezpieczeństwa, obowiązki dostawcy usług cyfrowych, obowiązki operatora usługi kluczowej</p> <p>Podstawy informacji wykorzystywanych do tworzenia aplikacji webowych, podstawy protokołu HTTP. Autentykacja, autoryzacja i zarządzanie sesją w aplikacjach webowych. Powstawanie i wykorzystywanie podatności, charakterystyka najważniejszych podatności.</p> <p>Modele chmury obliczeniowej, jej zalety i wady. Chmura prywatna, publiczna i hybrydowa. Modele bezpieczeństwa dla usług chmurowych. Standardy: Norma ISO 27017: Praktyczne zasady zabezpieczenia informacji na podstawie ISO/IEC 27002 dla usług w chmurze, NSC 800-210: Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej. Zagrożenia występujące w rozwiązaniach chmurowych, aspekty bezpieczeństwa w chmurze oraz typy narzędzi zabezpieczających w chmurze.</p> <p>Koncepcja procesu digital forensics &amp; incident response (DFIR). Definicja dowodu cyfrowego, podstawy prawne. Klasyfikacja incydentów, zgłaszanie i postępowanie z incydentami; dokumentacja zarządzania incydentami, zasady zarządzania incydentami: koncepcje oraz fazy zarządzania bezpieczeństwem informacji; wytyczne dotyczące reagowania na zdarzenia. Dobre praktyki związane z gromadzeniem materiału dowodowego. Narzędzia wykorzystywane do zabezpieczania i analizy materiału dowodowego.</p> <p>Wpływ sztucznej inteligencji na cyberbezpieczeństwo. Narzędzia wykorzystujące sztuczną inteligencję do zwalczania cyberataków, ulepszenie narzędzi bezpieczeństwa z wykorzystaniem AI</p> <p>Realizacja projektu PBL w wybranym obszarze tematycznym zgodnym z kierunkiem studiów/wybraną ścieżką dyplomowania.</p> <p>W ramach zajęć realizowanych w j. angielskim posługiwanie się specjalistyczną terminologią związaną obranym kierunkiem studiów na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego.</p> <p>Podstawowe sposoby projektowania i konfigurowania systemów bezpieczeństwa w infrastrukturze sieciowej. Mechanizmy zabezpieczające infrastrukturę teleinformatyczną przed atakami. Typowe ataki w sieciach komputerowych. Zabezpieczenia i segmentacja sieci. Wykrywanie anomalii w ruchu sieciowym. Wykorzystanie VPN. Bezpieczeństwo poczty elektronicznej oraz systemów DNS. Zarządzanie politykami bezpieczeństwa w elementach infrastruktury sieciowej.</p> <p>Model referencyjny Purdue w systemach przemysłowych Podstawowe pojęcia i założenia związane z budową infrastruktury zabezpieczeń dla przemysłowych systemów sieciowych. Zarządzanie siecią OT. Bezpieczeństwo sieci OT. Protokoły w sieci przemysłowej. Systemy monitorowania w zależności od topologii sieci. Segmentacja sieci przemysłowej. Detekcja ataków na sieci przemysłowe i narzędzia rejestrowania zdarzeń. Współpraca działów IT i OT.</p> <p>Seminarium dyplomowe. Praca dyplomowa.</p>



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

Nazwa sposobu weryfikacji i oceny efektów uczenia się	Opis sposobu weryfikacji i oceny efektów uczenia się
Egzamin pisemny	Egzamin pisemny obejmuje opisowe odpowiedzi na pytania dotyczące zagadnień obejmujących treści programowe danego przedmiotu. Czas trwania egzaminu jest ograniczony i jest podawany przez egzaminatora przed rozpoczęciem egzaminu.
Egzamin ustny	Egzamin ustny obejmuje ustne odpowiedzi na pytania dotyczące zagadnień obejmujących treści programowe danego przedmiotu. Student ma prawo do ograniczonego czasowo przygotowania się do odpowiedzi oraz sporządzania notatek.
Egzamin dyplomowy	Egzamin ustny obejmuje ustne odpowiedzi na pytania dotyczące zagadnień obejmujących treści programowe danego kierunku i ścieżki dyplomowania.
Sprawdzian pisemny	Sprawdzian pisemny obejmuje fragment treści programowych przedmiotu, np. jedno ćwiczenie laboratoryjne, określony typ zadań itp.
Test	Test polega na wyborze jednej lub kilku podanych odpowiedzi na postawione pytanie.
Kolokwium pisemne	Kolokwium pisemne obejmuje opisowe odpowiedzi na pytania dotyczące zagadnień obejmujących treści programowe danego przedmiotu. Czas trwania kolokwium jest ograniczony i jest podawany przez egzaminatora przed jego rozpoczęciem. Ta forma weryfikacji może być stosowana w przypadku przedmiotów niekończących się egzaminem.
Kolokwium ustne	Kolokwium ustne obejmuje ustne odpowiedzi na pytania dotyczące zagadnień obejmujących treści programowe danego przedmiotu. Student ma prawo do ograniczonego czasowo przygotowania się do odpowiedzi oraz sporządzania notatek. Ta forma weryfikacji może być stosowana w przypadku przedmiotów niekończących się egzaminem.
Elaborat	Student przygotowuje obszerne opracowanie pisemne wybranego zagadnienia dotyczącego treści kształcenia danego przedmiotu.
Ocena pracy dyplomowej	Student przygotowuje pisemne opracowanie, liczące od kilkunastu do kilkuset stron, będące sprawozdaniem z przeprowadzonych przez studenta działań. Praca dyplomowa może mieć charakter teoretyczny, praktyczny lub może zawierać opis wykonanych eksperymentów i obserwacji. Na studiach II stopnia praca dyplomowa może mieć charakter projektu.
Ocena sprawozdania	Sprawozdanie zawiera opis pomiarów, badań, obserwacji itp. przeprowadzonych w ramach ćwiczenia laboratoryjnego, wyjazdu terenowego itp. Sprawozdanie może podlegać zaliczeniu bez wystawiania oceny.
Ocena projektu	Projekt stanowi potwierdzenie realizacji konkretnego zadania (najczęściej inżynierskiego) wykonanego po przyjęciu narzuconych przez prowadzącego założeń wstępnych. Dopuszcza się m.in. następujące formy projektów: opracowanie pisemne, program komputerowy, rysunek, model matematyczny itp.
Ocena prezentacji	Student przygotowuje prezentację, najczęściej multimedialną, w której prezentuje opis wybranego zagadnienia, efekty badań itp. Prezentacja powinna być wygłoszona w ramach zajęć.
Obserwacja i ocena aktywności i umiejętności studenta	Prowadzący na podstawie obserwacji zachowania studenta, jego aktywności i umiejętności wykazanych w trakcie zajęć, może uznać osiągnięcie zakładanych efektów uczenia się.