Załącznik nr 2
do uchwały Senatu WAT nr 80/WAT/2025
z dnia 25 września 2025 r.

Wojskowa Akademia Techniczna

WOJSKOWA AKADEMIA TECHNICZNA
Wydział Cybernetyki

PROGRAM STUDIÓW
DLA KANDYDATÓW NA OFICERÓW

Kierunek studiów: „kryptologia i cyberbezpieczeństwo”
Poziom studiów: jednolite studia magisterskie
Profil studiów: ogólnoakademicki

Specjalność wojskowa:

systemy kryptograficzne (SW 29A), bezpieczeństwo informacyjne (SW 29B), bezpieczeństwo systemów informatycznych (SW 29B), cyberobrona (SW 29B)

Program studiów ustalony uchwałą *Senatu Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego* ***nr*** *80/WAT/2025* ***z dnia*** *25 września 2025 r.*

Obowiązuje kandydatów rozpoczynających kształcenie od roku akademickiego 2025/2026

Warszawa

2025

Strona celowo pozostawiona pusta

Spis treści

1. PROGRAM STUDIÓW - ZAŁOŻENIA ORGANIZACYJNE

Kierunek studiów: „kryptologia i cyberbezpieczeństwo”

Poziom studiów: jednolite studia magisterskie

Profil studiów: ogólnoakademicki

Forma studiów: stacjonarna

Tytuł zawodowy nadawany absolwentom: magister inżynier

Poziom Polskiej Ramy Kwalifikacji: siódmy (7)

Przyporządkowanie kierunku do dziedziny i dyscyplin naukowych, do których odnoszą się zakładane efekty uczenia się:
Dziedzina nauki: nauki inżynieryjno-techniczne

Dyscyplina (wiodąca): informatyka techniczna i telekomunikacja

Liczba semestrów dziesięć (10)

Łączna liczba godzin w specjalnościach:

W programie specjalności profilowanej przedmiotami wybieralnymi	*Łączna liczba godzin*
Systemy kryptograficzne	**5096**
Bezpieczeństwo informacyjne	**5070**
Bezpieczeństwo systemów informatycznych	**5096**
Cyberobrona	**5118**

Liczba punktów ECTS konieczna do ukończenia studiów: 300

Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć:

- **prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia**

W programie specjalności profilowanej przedmiotami wybieralnymi	*Liczba punktów ECTS*
Systemy kryptograficzne	**151**
Bezpieczeństwo informacyjne	**150,2**
Bezpieczeństwo systemów informatycznych	**151**
Cyberobrona	**152**

- **kształcących umiejętności praktyczne lub o charakterze naukowym**

W programie specjalności profilowanej przedmiotami wybieralnymi	*Liczba punktów ECTS*
Systemy kryptograficzne	**151,5**

Bezpieczeństwo informacyjne	**144**
Bezpieczeństwo systemów informatycznych	**143,5**
Cyberobrona	**143**

– **z dziedziny nauk humanistycznych lub nauk społecznych - 2,5**

Wymiar, liczba punktów ECTS, zasady i forma odbywania praktyk zawodowych-: 16

Łączna liczba punktów ECTS, którą kandydat na oficera kierunku „kryptologia i cyberbezpieczeństwo" musi uzyskać w ramach praktyki zawodowej w formie praktyk dowódczych, realizowanych w wymiarze 8 tygodni - 8:

- po IV semestrze studiów: 4-tygodniowa praktyka dowódcy drużyny;
- w X semestrze studiów: 4-tygodniowa praktyka dowódcy plutonu.

Łączna liczba punktów ECTS, którą kandydat na oficera kierunku „kryptologia i cyberbezpieczeństwo" musi uzyskać w ramach praktyki zawodowej w formie praktyk i szkoleń specjalistycznych, realizowanych w wymiarze 8 tygodni - 8:

- po VI semestrze studiów: 4-tygodniowa praktyka zawodowa specjalistyczna;
- w VIII semestrze studiów: 4-tygodniowe szkolenie specjalistyczne.

2. INFORMACJE OGÓLNE

2.1. Ogólna charakterystyka uczelni

Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego, powołana ustawą z 1951 roku, jest publiczną uczelnią akademicką nadzorowaną przez Ministra Obrony Narodowej. Jako uczelnia akademicka służy: Siłom Zbrojnym RP, nauce, gospodarce i społeczeństwu, poprzez kształcenie podchorążych i studentów, rozwój kadry badawczej i dydaktycznej oraz prowadzenie badań naukowych i prac rozwojowych w dziedzinach nauk inżynieryjno-technicznych, ścisłych i przyrodniczych oraz społecznych, a w szczególności w zakresie techniki wojskowej i technologii bezpieczeństwa. Współpracuje z uczelniami akademickimi w kraju i za granicą. Przygotowuje przyszłe kadry inżynierskie, przekazuje wiedzę, kształtuje umiejętności i doskonali kompetencje na najwyższym poziomie, ucząc jednocześnie patriotyzmu i odpowiedzialności za Ojczyznę.

Jej kształt i funkcjonowanie determinowane są potrzebami zapewnienia Siłom Zbrojnym RP wysokokwalifikowanej i wyspecjalizowanej kadry oficerskiej. W obszarze działalności dydaktycznej, realizuje kształcenie na poziomie jednolitych studiów magisterskich dla kandydatów na żołnierzy zawodowych oraz na rzecz osób cywilnych: stacjonarne dwustopniowe studia cywilne (licencjackie, inżynierskie i magisterskie), jednolite studia magisterskie. Ponadto na rzecz zarówno osób cywilnych jak i wojskowych: studia niestacjonarne dwustopniowe, studia podyplomowe (w tym MBA), kształcenie w Szkole Doktorskiej i szereg form szkolenia kursowego.

Wojskowa Akademia Techniczna jest uczelnią, która poprzez rozwój podnosi swoją jakość w obszarze badań i kształcenia w zgłoszonych do Ministerstwa Nauki i Szkolnictwa Wyższego w trzech dziedzinach nauk (nauk inżynieryjno-technicznych, nauk ścisłych

i przyrodniczych, nauk społecznych) oraz siedmiu dyscyplinach naukowych (automatyka, elektronika, elektrotechnika i technologie kosmiczne; informatyka techniczna i telekomunikacja; inżynieria lądowa, geodezja i transport; inżynieria materiałowa, inżynieria mechaniczna, nauki chemiczne, nauki o bezpieczeństwie), dążąc przy tym do rozszerzenia obszaru kształcenia w innych dziedzinach i dyscyplinach naukowych.

Ambicją Akademii jest umacnianie pozycji uczelni, jako kreatywnej, nowoczesnej i na bieżąco dostosowującej się do oczekiwań rynku odbiorców jej absolwentów. W obszarze kształcenia kadr wojskowych umacniana jest pozycja lidera w procesie zapewnienia zdolności Sił Zbrojnych RP do utrzymywania zasobów wysoko wykwalifikowanej kadry technicznej.

Akademia w dalszym ciągu spełniać będzie rolę zaplecza eksperckiego i badawczego Ministra Obrony Narodowej oraz podległego temu Ministrowi działu administracji rządowej "obrona narodowa". Uczelnia zmierzać będzie do wzmocnienia współpracy badawczej z ośrodkami naukowymi o wysokiej renomie w skali międzynarodowej, w szczególności w priorytetowych obszarach badawczych, techniki oraz technologii obronnych i podwójnego zastosowania, co zwiększy jej rozpoznawalność, zwłaszcza w Unii Europejskiej oraz w NATO.

Wypełniając misję społeczną uczelni akademickiej, wspieranym jest rozwój przedsiębiorczości studentów i doktorantów, kultury studenckiej i sportu akademickiego. W wyniku realizacji prestiżowych projektów i programów międzynarodowych oraz podejmowanych wspólnie z innymi renomowanymi ośrodkami akademickimi, zarówno publicznymi jak i niepublicznymi, inicjatyw związanych z szeroko rozumianym rozwojem, stale rozbudowywana i unowocześniana jest infrastruktura badawcza uczelni, niezbędna do prowadzenia badań naukowych i zajęć dydaktycznych. Rozwijana jest nowoczesna infrastruktura informatyczna, pozwalająca na zmianę jakości kształcenia i zarządzania uczelnią.

Kierując się koniecznością sprostania wyzwaniom stojącym przed uczelnią akademicką XXI w., zapewnienia wysokiego standardu procesu kształcenia, rozwoju kompetencji naukowych i prowadzenia projektów badawczych oraz rozwojowych, jakości "know-how" i utrzymywania zdolności do współpracy międzynarodowej, zgodnie z przyjętą strategią WAT, uwzględnianymi są między innymi następujące cele w rozwoju Wojskowej Akademii Technicznej w obszarze kształcenia:

1. Realizacja polityki naukowej państwa poprzez udział w programach i przedsięwzięciach Ministerstwa Nauki i Szkolnictwa Wyższego;

2. Intensyfikacja pozyskiwania środków finansowych przyznanych w trybie konkursowym na realizację inwestycji związanych z działalnością naukową oraz kształceniem, z uwzględnieniem potrzeb Sił Zbrojnych RP wynikających z Programów Rozwoju Sił Zbrojnych;

3. Rozszerzanie oferty studiów stacjonarnych, niestacjonarnych, podyplomowych, kursów kwalifikacyjnych i doskonalących oraz innych form kształcenia i szkolenia wynikających

z Programu Rozwoju Sił Zbrojnych, a także zapewnienie odpowiedniej bazy dydaktycznej i socjalnej wynikającej z potrzeb resoru obrony narodowej;

4. Przygotowanie kompleksowych rozwiązań służących rozwojowi zawodowemu pracowników uczelni, efektem czego staje się podniesienie jakości kształcenia studentów i doktorantów, w szczególności na kierunkach i w dyscyplinach naukowych związanych z priorytetowymi obszarami badawczymi;

Podnoszenie międzynarodowej rozpoznawalności działalności dydaktycznej i naukowej uczelni oraz jej międzynarodowego znaczenia poprzez optymalizację jakości zarządzania uczelnią i wzmocnienie współpracy badawczej z ośrodkami naukowymi i dydaktycznymi o wysokiej renomie w skali międzynarodowej.

2.2. Charakterystyka kierunku studiów

Wydział Cybernetyki prowadzi studia dla kandydatów na oficerów na kierunku:

- INFORMATYKA (od 1968r.)
- **KRYPTOLOGIA I CYBERBEZPIECZEŃSTWO** (od 2015r.)

Studia w charakterze kandydata na oficera realizowane są jako jednolite studia magisterskie; trwają 10 semestrów i kończą się uzyskaniem tytułu zawodowego magistra inżyniera oraz stopnia wojskowego podporucznika. W ramach kształcenia na kierunku studiów „Kryptologia i Cyberbezpieczeństwo" oferuje się możliwość uzyskania jednej z czterech specjalizacji, dających unikatową wiedzę i umiejętności.

Specjalność „Systemy kryptograficzne"

Specjalność wiąże się ze zdobyciem zaawansowanej wiedzy z zakresu informatyki, a także ogólnej wiedzy z zakresu nauk matematycznych oraz inżynierii bezpieczeństwa, w tym z obszaru bezpieczeństwa systemów technicznych. Zdobywa wiedzę i umiejętności z zakresu inżynierii systemów bezpieczeństwa, zarządzania bezpieczeństwem informacji, budowy systemów ochrony informacji, bezpieczeństwa systemów informatycznych wykorzystywania algorytmów kryptograficznych. Jest przygotowywany do pracy w strukturach odpowiedzialnych za bezpieczeństwo państwa, w szczególności w zakresie efektywnego uczestniczenia w projektowaniu systemów bezpieczeństwa informacji oraz analizach i ocenach bezpieczeństwa i ryzyka.

Specjalność „Bezpieczeństwo informacyjne"

Specjalność z zakresu inżynierii oprogramowania i projektowania systemów informatycznych ze szczególnym uwzględnieniem metodyk i technologii zapewnienia bezpieczeństwa systemów informacji. Zdobywa ogólną wiedzę z zakresu nauk matematycznych oraz inżynierii bezpieczeństwa, w tym z obszaru bezpieczeństwa systemów technicznych tworzących krytyczną infrastrukturę państwa. Zdobywa umiejętność wykorzystania metod ilościowych do oceny ryzyka w bezpieczeństwie informacji. Zdobywa wiedzę i umiejętności z zakresu budowy systemów zarządzania bezpieczeństwem informacji, systemów ochrony informacji, zagrożeń w cyberprzestrzeni oraz metod skutecznego przeciwdziałania tym zagrożeniom. Poznaje również kierunki rozwoju technologii komputerowych, w tym technologii mobilnych i Internetu Rzeczy.

Specjalność „Bezpieczeństwo systemów informatycznych”

Specjalność wiąże się ze zdobyciem zaawansowanej wiedzy i umiejętności z zakresu informatyki, szczególnie analizy, projektowania i zarządzania systemami teleinformatycznymi, a także wiedzy i umiejętności w zakresie szeroko rozumianego bezpieczeństwa systemów teleinformatycznych. Zdobywa wiedzę i umiejętności w zakresie diagnostyki i tolerowania uszkodzeń, projektowania i utrzymywania systemów zabezpieczeń i systemów zarządzania bezpieczeństwem informacji, stosowania technik dochodzeniowych i śledczych, typowych technik ataków oraz rozpoznawania podatności systemów informatycznych.

Specjalność „Cyberobrona”

Specjalność wiąże się ze zdobyciem zaawansowanej wiedzy z zakresu informatyki, szczególnie sieci komputerowych, a także inżynierii bezpieczeństwa, w tym zwłaszcza z obszaru bezpieczeństwa systemów technicznych. Student uzyskuje wiedzę i umiejętności w zakresie eksploracji sieci rozumianej jako wyszukiwanie i korelacja informacji o systemach teleinformatycznych oraz rozpoznawanie, badanie i identyfikacja zasobów sieci. Ponadto poznaje charakterystykę i narzędzia ataków sieciowych oraz uzyskuje wiedzę i umiejętności w zakresie wykorzystywania różnorodnych zabezpieczeń teleinformatycznych. Zdobywa wiedzę i umiejętności w zakresie obsługi urządzeń sieciowych, administrowania systemami operacyjnymi Windows i Linux, projektowania i zarządzania bezpieczeństwem w sieciach bezprzewodowych. Nabywa również umiejętności w zakresie projektowania i implementacji oprogramowania systemów rozproszonych, z zastosowaniem współcześnie stosowanych technologii oraz organizowania obrony w cyberprzestrzeni.

2.3. Opis sylwetki absolwenta

Absolwent studiów w charakterze kandydata na oficera będzie posiadać wiedzę, umiejętności i kompetencje społeczne niezbędne do dowodzenia i kierowania zespołami ludzi oraz techniczne przygotowanie specjalistyczne, umożliwiające zarządzanie eksploatacją sprzętu wojskowego, adekwatnie do zajmowanego stanowiska służbowego w Siłach Zbrojnych RP.

Studia na kierunku „kryptologia i cyberbezpieczeństwo” przygotowują specjalistów w zakresie bezpieczeństwa informacji, przygotowanych do samodzielnego rozwiązywania problemów z zakresu projektowania, organizacji i eksploatacji systemów bezpieczeństwa informacji oraz bezpieczeństwa systemów informatycznych, działających w różnych środowiskach. Przygotowują do pracy w zespołach interdyscyplinarnych rozwiązujących zagadnienia związane z zarządzaniem ryzykiem, identyfikacją i prognozowaniem zagrożeń bezpieczeństwa informacji.

Absolwent kierunku będzie posługiwał się językiem angielskim na poziomie biegłości 3232, zgodnie z porozumieniem standaryzacyjnym NATO STANAG 6001, zarówno w tematyce ogólnej, wojskowej, jak i tematyce specjalistycznej z zakresu kierunku kształcenia. W trakcie studiów wobec kandydata na oficera przeprowadza się postępowanie sprawdzające zgodnie z zapisami ustawy o ochronie informacji niejawnych, umożliwiające uzyskanie poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych. Kandydat zobowiązany jest do wyrażenia pisemnej zgody na przeprowadzenie postępowania sprawdzającego.

2.4. Warunki ukończenia studiów

Studia wojskowe kończą się egzaminem dyplomowym i egzaminem na oficera. Absolwenci otrzymują dyplom ukończenia studiów magisterskich, patent oficerski i mianowanie na stopień podporucznika.

Warunkiem mianowania kandydata na żołnierza zawodowego na pierwszy stopień oficerski jest uzyskanie przez niego wykształcenia wyższego na poziomie określonym w programie studiów (tytuł magistra, magistra inżyniera) oraz zdanie egzaminu na oficera. Warunkiem dopuszczenia kandydata na żołnierza zawodowego do egzaminu na oficera jest: uzyskanie pozytywnych ocen z egzaminów lub zaliczeń ze wszystkich zajęć z kształcenia wojskowego i specjalistycznego oraz posiadanie świadectwa znajomości języka angielskiego na poziomie określonym przez Ministra Obrony Narodowej.

3. MODUŁ WOJSKOWY

3.1. Realizacja standardu kształcenia wojskowego

3.1.1. OPIS ZAKŁADANYCH EFEKTÓW UCZENIA SIĘ WYNIKAJĄCYCH ZE STANDARDU KSZTAŁCENIA WOJSKOWEGO

Zakładane efekty kształcenia wojskowego określono w załączniku do Decyzji Nr 211/DSW Ministra Obrony Narodowej z dnia 27 maja 2024 r. w sprawie Standardu Kształcenia Wojskowego dla kandydatów na oficerów – minimalne wymagania programowe.

Standard kształcenia wojskowego określa minimalne wymagania w zakresie treści kształcenia oraz efektów uczenia się, niezbędne do osiągnięcia odpowiednich kompetencji przez przyszłego oficera Sił Zbrojnych Rzeczypospolitej Polskiej. Określa minimalny zakres wiedzy niezbędnej do wykonywania obowiązków na stanowiskach służbowych przeznaczonych dla oficerów młodszych. Treści kształcenia są wspólne dla wszystkich korpusów osobowych (grup osobowych) i specjalności wojskowych.

W wyniku realizacji standardu kształcenia wojskowego absolwent powinien w trakcie studiów osiągnąć poniżej określone kwalifikacje.

Symbol	*Efekty uczenia się*
Kategoria efektów: *WIEDZA*	
W_SW_1	posiada interdyscyplinarną wiedzę z dziedziny nauk humanistycznych i społecznych, dotyczącą istoty, prawidłowości i problemów funkcjonowania oficera w jednostce wojskowej w warunkach pokoju, kryzysu i wojny;
W_SW_2	posiada wiedzę z zakresu systemu dowodzenia i realizacji procesu dowodzenia;
W_SW_3	zna zasady organizowania i utrzymania gotowości bojowej w pododdziale;
W_SW_4	posiada wiedzę o organizacji, strukturach, rodzajach i podstawowym wyposażeniu pododdziałów rodzajów SZ RP oraz armii innych państw;
W_SW_5	posiada wiedzę na temat prowadzenia działań taktycznych na współczesnym polu walki na szczeblu plutonu i kompanii (równorzędnym) oraz charakterystykę i zasady wykorzystania różnego rodzaju wsparcia tych działań;
W_SW_6	posiada wiedzę niezbędną oficerowi młodszemu do dowodzenia, organizowania i prowadzenia działalności szkoleniowej, metodycznej i wychowawczej w pododdziale;
W_SW_7	zna budowę i zasady bezpiecznej eksploatacji w szkoleniu powierzonego sprzętu wojskowego (SpW) oraz zasady prowadzenia nadzoru nad powierzonym mieniem i SpW;
W_SW_8	zna misję i wizję SZ RP, zadania realizowane w ramach działań niekinetycznych i współpracy międzynarodowej oraz zasady ich komunikowania społeczeństwu;
W_SW_9	posiada wiedzę z zakresu prawnych uwarunkowań związanych ze służbą wojskową i funkcjonowaniem pododdziału oraz Międzynarodowego Prawa Humanitarnego Konfliktów Zbrojnych (MPHKZ);
W_SW_10	zna zagrożenia występujące w cyberprzestrzeni oraz zasady bezpiecznego korzystania z przestrzeni informatycznej;
W_SW_11	zna podstawowe środki wsparcia dowodzenia;

W_SW_12	zna zasady i sposoby unikania zagrożeń oraz postępowania w sytuacji walki o przetrwanie w różnych warunkach;
W_SW_13	posiada wiedzę na temat zabezpieczenia medycznego działań bojowych do szczebla batalionu oraz zna zasady udzielania pomocy medycznej poszkodowanym, w tym założenia taktyczno-medyczne i standardy TCCC (Tactical Combat Casualty Care);
W_SW_14	zna regulacje prawne i procedury postępowania dotyczące bezpieczeństwa i higieny pracy oraz zagrożenia środowiska naturalnego oraz zasady ochrony oraz postępowania z zanieczyszczeniami;
W_SW_15	zna zasady bezpiecznego posługiwania się bronią strzelecką, amunicją oraz granatami ręcznymi, podstawowe pojęcia balistyki i teorii strzału, przeznaczenie, charakterystykę oraz ogólną budowę broni strzeleckiej, amunicji i granatów ręcznych, ogólne zasady działania części i mechanizmów broni etatowej i granatów ręcznych, przeznaczenie, ogólną budowę i zasady wykorzystania celowników optoelektronicznych, stosowanych do etatowej broni strzeleckiej oraz podstawowych przyrządów obserwacyjnych, zasady strzelania z etatowej broni strzeleckiej oraz jej możliwości ogniowe, zasady przygotowania i obsługi broni do/po strzelaniu oraz konfiguracji oporządzenia.
Kategoria efektów: *UMIEJĘTNOŚCI*	
U_SW_1	rozpoznaje, diagnozuje i rozwiązuje problemy związane z dowodzonym pododdziałem wykorzystując elementy przywództwa;
U_SW_2	posiada umiejętności do kierowania i dowodzenia podległym pododdziałem;
U_SW_3	stosuje formy, metody, techniki i narzędzia niezbędne do planowania i prowadzenia szkolenia ogólnowojskowego i bojowego w pododdziale;
U_SW_4	planuje, organizuje i prowadzi działalność szkoleniową, metodyczną oraz wychowawczą w pododdziale;
U_SW_5	potrafi posługiwać się ogólnowojskowym SpW będącym na wyposażeniu pododdziału;
U_SW_6	wykorzystuje w szkoleniu możliwości bojowe powierzonego SpW z zachowaniem procedur bezpieczeństwa i higieny pracy oraz umiejętność przestrzegania zasad ochrony środowiska podczas realizacji zadań;
U_SW_7	prowadzi właściwą gospodarkę mieniem wojskowym oraz zasobami ludzkimi;
U_SW_8	skutecznie przewodzi zasobami ludzkimi, komunikuje się oraz negocjuje i przekonuje w zwartej grupie;
U_SW_9	dostosowuje się do częstych zmian otoczenia wynikających ze specyfiki służby wojskowej;
U_SW_10	stosuje przepisy prawne oraz procedury regulujące zagadnienia związane ze służbą wojskową oraz Międzynarodowym Prawem Humanitarnym Konfliktów Zbrojnych (MPHKZ);
U_SW_11	potrafi bezpiecznie korzystać z systemów informacyjnych w zakresie niezbędnym do pełnienia służby wojskowej;
U_SW_12	posiada umiejętność obiektywnego oceniania i opiniowania podwładnych;
U_SW_13	posiada umiejętności planowania i organizacji zabezpieczenia medycznego działań bojowych do szczebla batalionu oraz potrafi właściwie (tj. zgodnie ze standardem TCCC) wdrożyć czynności udzielania pomocy na polu walki oraz zarządzać personelem medycznym w toku zabezpieczenia działań pododdziału do szczebla batalionu;

U_SW_14	posiada zdolność funkcjonowania w środowisku narażonym na korupcję, w tym rozpoznaje ryzyka korupcyjne i skutecznie je eliminuje;
U_SW_15	posługuje się językiem angielskim na poziomie jego znajomości określonym zgodnie z obowiązującymi w resorcie obrony narodowej aktami normatywnymi dotyczącymi kształcenia i egzaminowania ze znajomości języków obcych w resorcie obrony narodowej;
U_SW_16	posiada sprawność fizyczną zgodnie z obowiązującymi w resorcie obrony narodowej aktami normatywnymi dotyczącymi wychowania fizycznego;
U_SW_17	posiada zdolność do funkcjonowania we współczesnym środowisku informacyjnym oraz potrafi skutecznie komunikować w czasie pokoju, kryzysu i wojny;
U_SW_18	potrafi skonfigurować swoje oporządzenie w zależności od zadania, rozkładać i składać etatowe uzbrojenie, czyścić i konserwować etatowe uzbrojenie i sprzęt wojskowy, wykonać przegląd i obsługę etatowego uzbrojenia i sprzętu wojskowego przed i po strzelaniu, bezpiecznie posługiwać się bronią, amunicją i granatami ręcznymi, prowadzić obserwację terenu oraz wykrywać, rozpoznawać i wskazywać cele, określać odległość do celów i przedmiotów terenowych różnymi sposobami, składać meldunki o wykrytych celach, posługiwać się optoelektronicznymi przyrządami celowniczymi do etatowej broni strzeleckiej oraz przyrządami obserwacyjnymi, przyjmować prawidłowo postawy strzeleckie: stojąc, klęcząc, leżąc z mocnej i słabej strony, prowadzić celny i powtarzalny ogień z etatowej broni zza, spod i znad przesłony (z mocnej i słabej strony) do celów stałych, ukazujących się i ruchomych w postawie strzeleckiej stojąc, klęcząc i leżąc, w dzień i w nocy; wykonywać wymianę magazynka sposobem awaryjnym i taktycznym, wykonywać zwroty w miejscu z bronią w postawie strzeleckiej stojąc, klęcząc i leżąc, usuwać zacięcia i drobne niesprawności broni, obserwować wyniki prowadzonego ognia oraz nanosić poprawki, wykonywać strzelania sprawdzające/sytuacyjne z etatowej broni strzeleckiej.
Kategoria efektów: *KOMPETENCJE SPOŁECZNE*	
K_SW_1	rozumie idee uczenia się przez całe życie oraz wykazuje gotowość do pogłębiania wiedzy, umiejętności i kompetencji niezbędnych do wykonywania zadań na zajmowanym stanowisku;
K_SW_2	jest świadomy posiadania wysokiej sprawności fizycznej oraz odporności psychicznej, pozwalającej na niezakłóconą realizację zadań w warunkach stresu i wzmożonego ryzyka;
K_SW_3	ma poczucie bycia obywatelem Rzeczypospolitej Polskiej (RP) oraz Unii Europejskiej (UE) o ugruntowanej świadomości patriotyczno – historyczno – obronnej, rozumie relacje funkcji społecznych i zawodowych oraz zachodzące procesy społeczne i ekonomiczne;
K_SW_4	zna, rozumie i stosuje zasady *Kodeksu Honorowego Żołnierza Zawodowego Wojska Polskiego*, rozumie znaczenie komunikacji w procesie kształtowania pozytywnego wizerunku żołnierza SZ RP;
K_SW_5	rozumie rolę dowódcy w pododdziale, jest świadomy znaczenia przywództwa, samodoskonalenia oraz doskonalenia zawodowego podwładnych, odpowiedzialności za dowodzenie i szkolenie podwładnych, powierzony SpW,

	utrzymanie wysokiej dyscypliny i gotowości bojowej oraz terminową realizację zadań;
K_SW_6	jest świadomy zagrożeń dla zdrowia podwładnych i własnego w przypadku nieprzestrzegania warunków bezpieczeństwa i higieny pracy w służbie wojskowej;
K_SW_7	jest świadom zagrożeń występujących w obszarze cyberbezpieczeństwa;
K_SW_8	rozumie pojęcia z obszaru komunikacji strategicznej oraz zasady funkcjonowania środowiska informacyjnego, poprawnie komunikuje się w języku polskim oraz zna zasady nowoczesnego kształtowania wizerunku Wojska Polskiego.

3.1.2. OPIS PROCESU KSZTAŁCENIA WYNIKAJĄCEGO ZE STANDARDU KSZTAŁCENIA WOJSKOWEGO

Zasadniczym celem kształcenia jest przygotowanie kandydatów na oficerów do dowodzenia (zarządzania) i realizacji zadań na stanowiskach oficerów młodszych w warunkach pokojowego funkcjonowania a także kryzysu i wojny.

Kształcenie wojskowe realizowane jest z żołnierzami dobrowolnej zasadniczej służby wojskowej – w trakcie pierwszego roku studiów oraz żołnierzami zawodowymi wszystkich kierunków studiów, korpusów i grup osobowych – w trakcie kolejnych lat studiów. Obejmuje moduł szkolenia podstawowego, moduł szkolenia w ramach 11-miesięcznej dobrowolnej zasadniczej służby wojskowej oraz moduł oficerski.

Pierwszym etapem kształcenia realizowanym częściowo jeszcze przed rozpoczęciem I roku studiów jest Szkolenie Podstawowe kończące się egzaminem a następnie złożeniem przysięgi wojskowej. Szkolenie podstawowe realizowane jest w oparciu o „*Program szkolenia podstawowego SZ RP*" ze szczególnym uwzględnieniem treści w obszarze: podstaw regulaminów SZ RP, taktyki, szkolenia strzeleckiego, inżynieryjno–saperskiego, OPBMR, OPL, łączności, terenoznawstwa i szkolenia medycznego.

W trakcie pierwszego roku studiów realizowane jest szkolenie w ramach 11-miesięcznej dobrowolnej zasadniczej służby wojskowej. Treści kształcenia realizowane w tym etapie szkolenia są częścią modułu oficerskiego w zakresie przygotowującym kandydatów do egzaminu na podoficera. Egzamin na podoficera przeprowadzany jest po pierwszym roku studiów zgodnie z zasadami określonymi w standardzie kształcenia wojskowego.

Pozostałe treści przedmiotów wchodzące w zakres modułu oficerskiego kształcone są w Wojskowej Akademii Technicznej w trakcie kolejnych ośmiu semestrów studiów (semestry od II do X).

Jednym z etapów kształcenia są zajęcia realizowane w ramach obozu językowego, w trakcie którego podnoszone są umiejętności językowe podchorążych.

Kandydaci na żołnierzy zawodowych, a od drugiego roku studiów – żołnierze zawodowi podlegają w trakcie studiów ciągłemu procesowi kształtowania sylwetki osobowej przyszłego oficera. Ma na to wpływ przestrzeganie dyscypliny szkoleniowej w trakcie zajęć, oddziaływanie przełożonych – dowódców pododdziałów oraz kadry dydaktycznej biorącej udział w zajęciach. Wszelkie kontakty kadry z kandydatami na żołnierzy zawodowych oraz żołnierzami zawodowymi mają na celu przygotowanie ich do funkcjonowania na pierwszych stanowiskach służbowych.

Ponadto część zajęć, wynikająca ze standardu wojskowego, w ramach przedmiotu Obrona przed bronią masowego rażenia realizowana jest jako szkolenie przygotowujące do realizacji zadań w warunkach rzeczywistych skażeń. W trakcie szkolenia realizowane są zajęcia z użyciem ćwiczebno-bojowych środków trujących i substancji promieniotwórczych w „Rejonie skażeń" w Poligonowym Ośrodku Szkolenia z OPBMR w SZ RP, zlokalizowanym w Centrum Szkolenia Wojsk Lądowych Drawsko. W zakresie treści i efektów uczenia się przedmiotowe szkolenie realizowane w jednym bloku szkoleniowym dla wszystkich zajęć praktycznych OPBMR przewidzianych dla Modułu Oficerskiego obywać się będzie na III roku studiów.

3.1.3. SPOSÓB WERYFIKACJI ZAKŁADANYCH EFEKTÓW UCZENIA SIĘ ZE STANDARDU KSZTAŁCENIA WOJSKOWEGO

Weryfikacja zakładanych efektów uczenia się i szkolenia wojskowego prowadzona jest systematycznie przez cały okres studiów. Warunkiem zaliczenia każdego z przedmiotów kształcenia jest uzyskanie pozytywnej oceny z obowiązującego rygoru dydaktycznego: egzaminu, zaliczenia na ocenę lub zaliczenia bez oceny. Warunkiem przeniesienia studenta na kolejne semestry kształcenia wojskowego jest zaliczenie wszystkich przedmiotów z tego obszaru. Ponadto w trakcie semestrów przeprowadzane są kolokwia pisemne, ćwiczenia audytoryjne, oceniany jest też udział w dyskusji, czy też aktywność w zajęciach.

Zajęcia praktyczne, strzelania szkolne, zajęcia instruktorsko-metodyczne zaliczane są na podstawie wyników uzyskanych z poszczególnych strzelań szkolnych i bojowych, praktycznego prowadzenia szkolenia w roli instruktora i kierownika zajęć oraz ocenę umiejętności posługiwania się uzbrojeniem i sprzętem wojskowym.

Przedmiot język angielski zaliczany jest na podstawie: aktywnego udziału w zajęciach (wypowiedzi ustne, udział w dyskusji), prac kontrolnych ze znajomości słownictwa oraz bieżących zagadnień gramatycznych, prac domowych, ćwiczeń leksykalnych i gramatycznych oraz dłuższych wypowiedzi pisemnych, zaliczenia egzaminu STANAG 6001 na poziom 2 2 2 2, egzaminu na poziomie B2 wg Europejskiego Systemu Opisu Kształcenia Językowego; testów zaliczeniowych na ocenę, egzaminu STANAG 6001 na SPJ 3 2 3 2 w przedostatnim lub ostatnim semestrze studiów.

Weryfikacja efektów uczenia się z przedmiotu wychowanie fizyczne realizowana jest poprzez wypracowany system ćwiczeń i testów do zaliczenia, obowiązujących kandydatów na żołnierzy zawodowych na zakończenie określonego etapu szkolenia (np. szkolenie podstawowe), a także okresu kształcenia (semestr). Ocenę semestralną z wychowania fizycznego kandydata na żołnierza zawodowego stanowi ocena poziomu sprawności fizycznej i umiejętności utylitarnych. Sprawność fizyczna i poziom umiejętności utylitarnych studentów wojskowych diagnozuje się próbami utylitarnymi zawartymi w „Rygorach dydaktycznych z wychowania fizycznego dla studentów WAT".

Weryfikacja efektów uczenia się w zakresie kształtowania sylwetki osobowej przyszłego oficera realizowana jest także na bieżąco w toku służby wojskowej pełnionej w charakterze kandydata na żołnierza zawodowego lub żołnierza zawodowego. Oceny w tym zakresie dokonują przełożeni – dowódcy pododdziałów w trakcie odbywania szkoleń i praktyk realizowanych w centrach szkolenia i jednostkach wojskowych oraz kadra dydaktyczna.

Szczegółowe informacje dotyczące weryfikacji zakładanych efektów uczenia się z poszczególnych przedmiotów i modułów kształcenia określone są w kartach

informacyjnych przedmiotów i przedstawiane studentom wojskowym w początkowym etapie zajęć.

Po zakończeniu 11-miesięcznej dobrowolnej zasadniczej służby wojskowej kandydaci na żołnierzy zawodowych mają możliwość przystąpienia do egzaminu na podoficera. Egzamin przygotowywany i prowadzony jest zgodnie z aktualnymi Wytycznymi Dyrektora Departamentu Szkolnictwa Wojskowego w sprawie przygotowania i prowadzenia egzaminu na podoficera w uczelniach wojskowych.

Ostateczną formą weryfikacji nabytej wiedzy i umiejętności jest Egzamin na oficera, w trakcie którego sprawdzeniu podlega: wyszkolenie i umiejętności strzeleckie, teoretyczna i praktyczna znajomość regulaminów i przepisów wojskowych, wyszkolenie z musztry, umiejętność dowodzenia pododdziałem oraz prowadzenia nauczania w roli instruktora i kierownika zajęć. Weryfikowana jest także wiedza z zakresu prowadzenia działań taktycznych przez pododdział, zagadnień zabezpieczenia bojowego i zabezpieczenia logistycznego. Sprawdzana jest także wiedza z zakresu Historii Polski i Historii sztuki wojennej. Warunkiem przystąpienia do egzaminu na oficera jest uzyskanie pozytywnych wyników z kształcenia wojskowego, kształcenia specjalistycznego, praktyk oraz wychowania fizycznego a także uzyskanie wymaganego poziomu umiejętności językowych.

KSZTAŁCENIE WOJSKOWE

Jednostka organizacyjna odpowiedzialna za przedmiot	Nazwa przedmiotu	Symbol efektu kształcenia wojskowego
	Grupa treści kształcenia ogólnego	
WLO - IOZ	Działalność wychowawcza i profilaktyka dyscyplinarna	W_SW_1,W_SW_6, U_SW_1, U_SW_4, U_SW_12, K_SW_1, K_SW_3, K_SW_4, K_SW_5,
WLO - IOZ	Podstawy komunikacji strategicznej – teoria i praktyka	W_SW_1, W_SW_8, U_SW_2, U_SW_8, U_SW_17; K_SW_4, K_SW_8,
WLO - IOZ	Przywództwo w dowodzeniu	W_SW_1, W_SW_2, W_SW_6, U_SW_1, U_SW_2, U_SW_8, U_SW_12, K_SW_5,
WLO - IOZ	Historia sztuki wojennej	W_SW_1, W_SW_5, K_SW_1, K_SW_3,
WLO - IOZ	Historia Polski	W_SW_1, W_SW_8, K_SW_1, K_SW_3, K_SW_4,
SSW	Ochrona informacji niejawnych	W_SW_9, W_SW_10, U_SW_1, U_SW_11, U_SW_17, K_SW_5, K_SW_7
WLO - IOZ	Profilaktyka antykorupcyjna	W_SW_1, U_SW_14, K_SW_4,

WCY	Bezpieczeństwo w cyberprzestrzeni	W_SW_1 W_SW_10, U_SW_11, U_SW_17, K_SW_7, K_SW_8
Sekcja BHP	Bezpieczeństwo i higiena pracy (BHP)	W_SW_7, W_SW_14, U_SW_6, K_SW_6,
	Grupa treści kształcenia kierunkowego	
SSW	Podstawy dowodzenia	W_SW_2, W_SW_3, W_SW_4, W_SW_5, W_SW_6, U_SW_2, U_SW_3, K_SW_1, K_SW_5
SSW	Taktyka	W_SW_2, W_SW_4, W_SW_5, W_SW_6, U_SW_2, U_SW_3, U_SW_5, U_SW_9, K_SW_1, K_SW_5
SSW	Podstawy survivalu	W_SW_5, W_SW_12, U_SW_5, U_SW_9, U_SW_16, K_SW_2, , K_SW_6,
SSW	Gotowość mobilizacyjna i bojowa	W_SW_1 W_SW_2, W_SW_3, U_SW_2, U_SW_9, K_SW_5,
SSW	Rozpoznanie i armie innych państw	W_SW_2, W_SW_4, W_SW_5, U_SW_2, U_SW_3, K_SW_5,
WIG	Topografia wojskowa	W_SW_1, W_SW_2, U_SW_3, U_SW_5, U_SW_11, K_SW_1,
WLO	Zabezpieczenie logistyczne działań taktycznych	W_SW_1,W_SW_5, W_SW_7, W_SW-8, U_SW_5, U_SW_6, U_SW_7, K_SW_3, K_SW_5,
SSW	Szkolenie strzeleckie	W_SW_6, W_SW_7, W_SW_14, W_SW_15; U_SW_3, U_SW_4, U_SW_5, U_SW_6, U_SW_18; K_SW_5, K_SW_6
WEL	System łączności i środki dowodzenia	W_SW_2, W_SW_4, W_SW_11, U_SW_5, U_SW_11, K_SW_7,
WLO - IOZ/ /SSW	Działalność szkoleniowa i szkoleniowo - metodyczna	W_SW_1, W_SW_6, U_SW_3, U_SW_4, U_SW_6, K_SW_1, K_SW_5,
WLO - IOZ	Międzynarodowe prawo humanitarne konfliktów zbrojnych (MPHKZ)	W_SW_1, W_SW_8, W_SW_9, U_SW_10, K_SW_5,
WLO - IBO	Wybrane zagadnienia bezpieczeństwa narodowego i międzynarodowego	W_SW_1, W_SW_5, W_SW_8, U_SW_9, U_SW_9, U_SW_10, K_SW_3, K_SW_5

WML	Podstawy eksploatacji sprzętu wojskowego (SpW)	W_SW_6, W_SW_7, W_SW_14, U_SW_5, U_SW_6, U_SW_7, K_SW_5, K_SW_6,
WLO	Działania niekinetyczne	W_SW_1, W_SW_8, W_SW_9, U_SW_10, U_SW_17, K_SW_1, K_SW_3, K_SW_8
WIG	Ochrona środowiska	W_SW_1, W_SW_14, U_SW_6, K_SW_6
SSW	Obrona powietrzna	W_SW_2, W_SW_4, W_SW_5, U_SW_5, U_SW_6, K_SW_5,
WTC	Obrona przed bronią masowego rażenia (OPBMR)	W_SW_1, W_SW_4, W_SW_5, W_SW_14, U_SW_4, U_SW_5, U_SW_6, K_SW_5, K_SW_6
WML	Połączone wsparcie ogniowe	W_SW_4, W_SW_5, U_SW_5, U_SW_6, K_SW_5, K_SW_6
SSW	Zabezpieczenie inżynieryjne	W_SW_3, W_SW_4, W_SW_5, W_SW_7, W_SW_14, U_SW_5, U_SW_6, K_SW_2, K_SW_5, K_SW_6,
SSW	Zabezpieczenie medyczne	W_SW_1, W_SW_13, U_SW_13, K_SW_6,
SSW	Regulaminy SZRP	W_SW_1, W_SW_6, U_SW_4, U_SW_9, K_SW_5,
	Grupa treści kształcenia sportowo - językowego	
SJO	Język angielski	U_SW_15, K_SW_1
SWF	Wychowanie fizyczne	W_SW_14, U_SW_16, K_SW_2, K_SW_6

3.1.4. MACIERZ POKRYCIA EFEKTÓW UCZENIA SIĘ WYNIKAJĄCYCH ZE STANDARDU WOJSKOWEGO

	Działalność wychowawcza i profilaktyka dyscyplinarna	Podstawy komunikacji strategicznej – teoria i praktyka	Przywództwo w dowodzeniu	Historia sztuki wojennej	Historia Polski	Ochrona informacji niejawnych	Profilaktyka antykorupcyjna	Bezpieczeństwo w cyberprzestrzeni	Bezpieczeństwo i higiena pracy (BHP)	Podstawy dowodzenia	Taktyka	Podstawy survivalu	Gotowość mobilizacyjna i bojowa	Rozpoznanie i armie innych państw	Topografia wojskowa	Zabezpieczenie logistyczne działań taktycznych	Szkolenie strzeleckie	System łączności i środki dowodzenia	Działalność szkoleniowa i szkoleniowo metodyczna	Międzynarodowe Prawo Humanitarne Konfliktów Zbrojnych (MPHKZ)	Wybrane zagadnienia bezpieczeństwa narodowego i międzynarodowego	Podstawy eksploatacji sprzętu wojskowego (SpW)	Działania niekinetyczne	Ochrona środowiska	Obrona powietrzna	Obrona przed bronią masowego rażenia (OPBMR)	Połączone wsparcie ogniowe	Zabezpieczenie inżynieryjne	Zabezpieczenie medyczne	Regulaminy SZRP	Język angielski	Wychowanie fizyczne
W_SW_1	X	X	X	X	X		X	X					X		X	X			X	X	X		X	X		X			X	X		
W_SW_2			X							X	X		X	X	X			X							X							
W_SW_3										X			X																X			
W_SW_4										X	X			X				X							X	X	X	X				
W_SW_5				X						X	X	X		X		X					X				X	X	X	X				
W_SW_6	X		X							X	X						X		X			X								X		
W_SW_7									X							X	X					X							X			
W_SW_8		X			X											X			X	X			X									
W_SW_9						X													X	X			X									
W_SW_10						X		X																								
W_SW_11																		X														
W_SW_12												X																				
W_SW_13																													X			
W_SW_14									X								X					X		X		X		X				X
W_SW_15																	X															
U_SW_1	X		X			X																										
U_SW_2		X	X							X	X		X	X																		
U_SW_3										X	X			X	X		X		X													
U_SW_4	X																X		X						X					X		
U_SW_5											X	X			X	X	X	X				X			X	X	X	X				
U_SW_6									X							X	X		X			X		X	X	X	X	X				
U_SW_7																X						X										
U_SW_8		X	X																													
U_SW_9											X	X	X								X									X		
U_SW_10																				X	X		X									
U_SW_11						X		X							X			X														
U_SW_12	X		X																													
U_SW_13																													X			
U_SW_14							X																									
U_SW_15																															X	
U_SW_16												X																				X
U_SW_17		X				X		X															X									
U_SW_18																	X															
K_SW_1	X			X	X					X	X				X				X				X								X	
K_SW_2												X																				X
K_SW_3	X			X	X											X					X		X									
K_SW_4	X	X			X		X																									
K_SW_5	X		X			X				X	X		X	X		X	X		X	X	X	X			X	X	X	X		X		
K_SW_6									X			X					X					X		X		X	X	X	X			X
K_SW_7						X		X										X														
K_SW_8		X						X															X									

4. MODUŁ KIERUNKOWY

4.1. Opis zakładanych efektów uczenia się

Opis zakładanych efektów uczenia się uwzględnia:

- uniwersalne charakterystyki pierwszego stopnia określone w załączniku do ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji
- charakterystyki drugiego stopnia określone w załączniku do rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 14 listopada 2018 r. w sprawie charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 Polskiej Ramy Kwalifikacji, w tym również umożliwiających uzyskanie kompetencji inżynierskich[1]

i jest ujęty w trzech kategoriach:

- kategoria **wiedzy (W)**, która określa:
  - zakres i głębię (**G**) - kompletność perspektywy poznawczej i zależności,
  - kontekst (**K**) - uwarunkowania, skutki.
- kategoria **umiejętności (U)**, która określa:
  - w zakresie wykorzystania wiedzy (**W**) - rozwiązywane problemy i wykonywane zadania,
  - w zakresie komunikowania się (**K**) - odbieranie i tworzenie wypowiedzi, upowszechnianie wiedzy w środowisku naukowym i posługiwanie się językiem obcym,
  - w zakresie organizacji pracy (**O**) - planowanie i pracę zespołową,
  - w zakresie uczenia się (**U**) - planowanie własnego rozwoju i rozwoju innych osób.
- kategoria **kompetencji społecznych (K)** - która określa:
  - w zakresie ocen (**K**) - krytyczne podejście,
  - w zakresie odpowiedzialności (**O**) - wypełnianie zobowiązań społecznych i działanie na rzecz interesu publicznego,
  - w odniesieniu do roli zawodowej (**R**) - niezależność i rozwój etosu.

Objaśnienie oznaczeń:

- w kolumnie ***symbol i numer efektu***:
  - K - kierunkowe efekty uczenia się;
  - W, U, K (po podkreślniku) - kategoria - odpowiednio: wiedzy, umiejętności, kompetencji społecznych;
  - 01, 02, 03, …. - numer efektu uczenia się.
- w kolumnie ***kod składnika opisu*** - Inż[2]_P7S_WG - kod składnika opisu charakterystyk drugiego stopnia dla kwalifikacji na poziome 7 Polskiej Ramy Kwalifikacji.

[1] *dotyczy kierunków studiów, absolwentom których nadawany jest tytuł zawodowy: inż., mgr inż.*
[2] *w przypadku kompetencji inżynierskich;*

Symbol i numer efektu	opis zakładanych efektów uczenia się	kod składnika opisu
WIEDZA	**Absolwent:**	
K_W01	zna i rozumie w pogłębionym stopniu charakter, miejsce i znaczenie nauk społecznych i humanistycznych oraz ich relacje do innych nauk	P7S_WG
K_W02	zna i rozumie w pogłębionym stopniu problematykę wybranych działów matematyki, niezbędną do rozumienia i studiowania przedmiotów kierunkowych oraz analizowania, modelowania, konstruowania i eksploatacji systemów informatycznych, w tym: symbole, podstawowe pojęcia, określenia i twierdzenia logiki, teorii mnogości, algebry z geometrią, analizy matematycznej, matematyki dyskretnej, optymalizacji, probabilistyki i matematycznych podstaw kryptologii	P7S_WG
K_W03	posiada pogłębioną wiedzę o ogólnych zasadach fizyki, wielkościach fizycznych i oddziaływaniach fundamentalnych w zakresie fizyki klasycznej, fizyki relatywistycznej oraz fizyki kwantowej i jądrowej oraz zna i rozumie zasady przeprowadzania i opracowywania wyników pomiarów fizycznych, rodzajów niepewności pomiarowych i sposobów ich wyznaczania	P7S_WG
K_W04	zna i rozumie w pogłębionym stopniu pojęcia i zasady działania elementów elektronicznych i układów cyfrowych	P7S_WG
K_W05	zna i rozumie podstawowe pojęcia z zakresu podstaw informatyki, teorii algorytmów i struktur danych, zarządzania danymi oraz zna paradygmaty i techniki programowania niskopoziomowego i wysokopoziomowego	P7S_WG Inż_P7S_WG
K_W06	rozróżnia klasy i rodzaje systemów informatycznych, zna narzędzia i metody projektowania takich systemów oraz wytwarzania oprogramowania pracującego pod ich kontrolą	P7S_WG Inż_P7S_WG
K_W07	zna i rozumie procesy zarządzania oraz w pogłębionym stopniu informatyczne metody, narzędzia oraz środowiska służące do modelowania i wspomagania procesów zarządzania organizacją i zasobami oraz ogólne zasady tworzenia i rozwoju różnych form przedsiębiorczości	P7S_WK Inż_P7S_WK
K_W08	zna i rozumie w pogłębionym stopniu modele, metody, metodyki oraz narzędzia do wytwarzania (analizy, projektowania, implementacji i testowania) systemów informatycznych (początkowe etapy cyklu życia systemów)	P7S_WG Inż_P7S_WG
K_W09	zna i rozumie w pogłębionym stopniu metody, dobre praktyki i metodyki wdrażania, utrzymywania, doskonalenia i wycofywania systemów informatycznych (końcowe etapy cyklu życia systemów)	P7S_WG Inż_P7S_WG
K_W10	zna i rozumie w pogłębionym stopniu metody i narzędzia wykorzystywane do modelowania oraz symulacji obiektów i systemów, pozwalających na wyznaczanie ich charakterystyk wydajnościowych, niezawodnościowych i bezpieczeństwa	P7S_WG
K_W11	zna i rozumie w pogłębionym stopniu modele, metody i narzędzia wykorzystywane do formułowania i rozwiązywania problemów: decyzyjnych, z zakresu inteligencji obliczeniowej oraz przetwarzania i analizy danych	P7S_WG

K_W12	zna i rozumie w pogłębionym stopniu pojęcia, opisy i zasady budowy, funkcjonowania i eksploatacji współczesnych systemów operacyjnych	P7S_WG
K_W13	ma pogłębioną wiedzę w zakresie zasad funkcjonowania sieci teleinformatycznych, usług sieciowych, projektowania i zarządzania sieciami teleinformatycznymi, w tym administrowania sieciowymi systemami operacyjnymi	P7S_WG
K_W14	ma pogłębioną wiedzę w zakresie metod i technik zapewniania bezpieczeństwa systemów informatycznych; zna i rozumie pojęcia, opisy, wybrane fakty i zjawiska w zakresie bezpieczeństwa informacyjnego oraz metody badań i przykłady implementacji w obszarze bezpieczeństwa systemów teleinformatycznych	P7S_WG
K_W15	zna i rozumie pojęcia, metody i techniki z zakresu bezpieczeństwa pracy i ergonomii oraz komunikacji człowiek – komputer	P7S_WG
K_W16	zna i rozumie pojęcia z zakresu konstruowania, opisu, działania i przeznaczenia układów cyfrowych, interfejsów oraz podzespołów komputerów	P7S_WG
K_W17	zna i rozumie pojęcia z zakresu architektury i organizacji systemów komputerowych oraz zasad projektowania, wytwarzania oprogramowania i eksploatacji systemów komputerowych (etapy cyklu życia systemu); zna podstawowe techniki testowania podzespołów sprzętowych i oprogramowania, zasady projektowania struktur diagnostycznych i techniki tolerowania błędów	P7S_WG
K_W18	zna i rozumie pojęcia z zakresu cyfrowego przetwarzania sygnałów w tym obrazów, kodowania i kompresji danych oraz grafiki komputerowej	P7S_WG
K_W19	zna i rozumie pojęcia z zakresu sterowania, programowania sterowników logicznych, mikrokontrolerów oraz modelowania układów regulacji i sterowania	P7S_WG
K_W20	zna i rozumie fundamentalne dylematy współczesnej cywilizacji, ze szczególnym uwzględnieniem dylematów związanych z informatyką; zna najnowsze tendencje rozwojowe, innowacyjne rozwiązania, nowoczesne metody i narzędzia z zakresu projektowania, wytwarzania, zabezpieczania, wdrażania, utrzymywania i doskonalenia systemów informatycznych, w tym w środowiskach sieciowych narażonych na ataki cybernetyczne oraz zawierających elementy informatyki kwantowej	P7S_WK P7S_WG Inż_P7S_WG
K_W21	zna i rozumie w pogłębionym stopniu ekonomiczne, prawne i inne uwarunkowania różnych rodzajów działań związanych z wykorzystywaniem metod i środków informatyki, w tym podstawowe pojęcia i zasady z zakresu ochrony własności przemysłowej i prawa autorskiego	P7S_WK
K_W22	zna i rozumie pojęcia, zasady i metody z zakresu teorii liczb i matematycznych podstaw i koncepcji kryptologii	P7S_WG
K_W23	zna i rozumie pojęcia oraz zasady i metody konstrukcji i analizy poprawności protokołów i algorytmów kryptograficznych i kryptoanalitycznych	P7S_WK
K_W24	zna i rozumie pojęcia z zakresu analizy dużych zbiorów danych oraz sztucznej inteligencji, w tym: uczenia maszynowego, przetwarzania języka naturalnego, głębokich sieci neuronowych oraz dużych modeli językowych	P7S_WG

UMIEJĘTNOŚCI	Absolwent:	
K_U01	potrafi w pogłębionym stopniu identyfikować i interpretować podstawowe zjawiska i procesy społeczne, humanistyczne i prawne w zakresie informatyki i dyscyplin pokrewnych	P7S_UW Inż_P7S_UW
K_U02	potrafi posługiwać się językiem angielskim na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego lub SPJ 3232 według STANAG 6001, w stopniu pozwalającym na porozumiewanie się w mowie i w piśmie w zakresie ogólnym oraz w zakresie terminologii informatycznej i wojskowej	P7S_UK
K_U03	umie posługiwać się językiem matematyki wykorzystując właściwe symbole, określenia i twierdzenia oraz umie formułować i rozwiązywać problemy metodami matematycznymi	P7S_UW Inż_P7S_UW
K_U04	potrafi wykorzystać poznane zasady i metody fizyki, stosując odpowiednie narzędzia matematyczne, do opisu właściwości fizycznych i związanych z nimi efektów przyczynowo- skutkowych oraz umie przeprowadzić pomiary wybranych wielkości fizycznych, opracować i zinterpretować wyniki	P7S_UW
K_U05	potrafi realizować zadanie projektowe z zastosowaniem zasad inżynierii oprogramowania, uwzględniając krytyczną ocenę funkcjonowania istniejących rozwiązań oraz odpowiednie metody i narzędzia analizy, projektowania, programowania i dokumentowania; umie zastosować wiedzę z zakresu języków programowania oraz zaawansowanych technik algorytmicznych do implementacji złożonych systemów teleinformatycznych zgodnie z ustaloną metodyką postępowania	P7S_UW Inż_P7S_UW
K_U06	potrafi wykorzystać wiedzę z zakresu procesów zarządzania organizacją oraz wykorzystywać informatyczne metody, narzędzia i środowiska do modelowania i wspomagania tych procesów	P7S_UW Inż_P7S_UW
K_U07	potrafi uczestniczyć w zespołowym projektowaniu, implementacji i testowaniu oraz stosować w praktyce zasady wdrażania, utrzymywania, doskonalenia i wycofywania systemów informatycznych, jak również dokonać wstępnej analizy ekonomicznej skutków tych działań; umie pracować w zespole, kierować zespołem projektowym, dokonać krytycznej analizy istniejących rozwiązań technicznych, wstępnej oceny ekonomicznej oraz zarządzać procesami, wdrażania, utrzymywania, doskonalenia i wycofywania systemów informatycznych, a także komunikować się z odbiorcami tych systemów; potrafi zarządzać procesami analizy oraz dokumentowania zadania projektowego i badawczego z zastosowaniem inżynierii oprogramowania oraz wybranych metod i narzędzi wytwarzania oprogramowania	P7S_UW P7S_UO P7S_UK Inż_P7S_UW
K_U08	potrafi wykorzystać znane, modyfikować istniejące lub budować nowe metody i narzędzia do modelowania, konstruowania symulatorów obiektów i systemów, formułowania i rozwiązywania problemów decyzyjnych oraz problemów z zakresu inteligencji obliczeniowej, jak również systemów przetwarzania i analizy danych, w tym rozproszonych i równoległych; potrafi zaplanować i przeprowadzić eksperymenty obliczeniowe i symulacyjne oraz dokonać przetworzenia i interpretacji ich wyników	P7S_UW Inż_P7S_UW

K_U09	umie użytkować wybrane systemy operacyjne i administrować tymi systemami	P7S_UW
K_U10	umie wykorzystać rozszerzoną i pogłębioną wiedzę w zakresie zasad funkcjonowania sieci teleinformatycznych, usług sieciowych, projektowania i zarządzania sieciami teleinformatycznymi, w tym administrowania sieciowymi systemami operacyjnymi; umie użytkować i projektować sieci teleinformatyczne i zarządzać takimi sieciami	P7S_UW
K_U11	w obszarze bezpieczeństwa systemów teleinformatycznych umie formułować i analizować problemy, znajdować ich rozwiązania oraz przeprowadzać eksperymenty, interpretować ich wyniki i wyciągać wnioski; potrafi stosować metody i techniki oceniania oraz zapewniania bezpieczeństwa systemów informatycznych	P7S_UW Inż_P7S_UW
K_U12	umie stosować zasady ergonomii, bezpieczeństwa i higieny pracy oraz analizować i projektować interfejsy człowiek-komputer	P7S_UW
K_U13	umie posłużyć się wybranymi metodami prototypowania, programowania i konfigurowania wybranych układów cyfrowych, podzespołów komputerów oraz systemów komputerowych; potrafi stosować podstawowe techniki testowania podzespołów sprzętowych i oprogramowania, zasady projektowania struktur diagnostycznych i techniki tolerowania błędów oraz konstruować testy funkcjonalne	P7S_UW Inż_P7S_UW
K_U14	umie wykorzystywać metody cyfrowego przetwarzania sygnałów tym obrazów, metody kodowania i kompresji oraz wskazać ich zastosowania	P7S_UW
K_U15	umie tworzyć programy sterowników oraz modelować procesy regulacji i sterowania	P7S_UW
K_U16	umie stosować innowacyjne technologie, realizować wybrane techniki wirtualizacji systemów, rozwiązywać wybrane zadania z zakresu telematyki i robotyki oraz sieci mobilnych, bezprzewodowych sieci sensorycznych i Internetu Rzeczy	P7S_UW Inż_P7S_UW
K_U17	umie wykorzystać metody klasyfikacji oraz analizy sygnałów do tworzenia systemów rozpoznawania (w tym systemów biometrycznych), projektować aplikacje internetowe oraz serwisy multimedialne z wykorzystaniem technologii strumieniowania multimediów oraz implementować podstawowe rodzaje dialogów w interfejsie człowiek – komputer	P7S_UW Inż_P7S_UW
K_U18	potrafi samodzielnie planować i realizować własne permanentne uczenie się i ukierunkowywać innych w tym zakresie, pozyskiwać informacje z literatury, baz danych i innych źródeł, dokonywać syntezy i analizy tych informacji	P7S_UU
K_U19	umie konstruować algorytmy kryptograficzne oraz analizować i oceniać bezpieczeństwo systemów kryptograficznych	P7S_UW
K_U20	umie wykorzystywać wybrane algorytmy kryptograficzne	P7S_UW Inż_P7S_UW
K_U21	umie wykorzystać metody sztucznej inteligencji do rozwiązywania zadań identyfikacji, klasyfikacji, predykcji w oparciu o duże zbiory danych z wykorzystaniem zaawansowanych metod uczenia maszynowego oraz dużych modeli językowych	P7S_UW

KOMPETENCJE SPOŁECZNE	Absolwent:	
K_K01	jest gotów do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz do krytycznej oceny odbieranych treści i posiadanej wiedzy	P7S_KK
K_K02	jest gotów do wypełniania zobowiązań społecznych oraz do inspirowania i organizowania działalności na rzecz środowiska społecznego	P7S_KO
K_K03	jest gotów do inicjowania działania na rzecz interesu publicznego	P7S_KO
K_K04	jest gotów do myślenia i działania w sposób przedsiębiorczy	P7S_KO
K_K05	jest gotów do odpowiedzialnego pełnienia ról zawodowych, w tym: − przestrzegania zasad etyki zawodowej i wymagania tego od innych, − dbałości o dorobek i tradycje zawodu, − krytycznej oceny siebie oraz zespołów i organizacji, w których uczestniczy	P7S_KO
K_K06	jest gotów do odpowiedzialnego pełnienia ról zawodowych z uwzględnieniem zmieniających się potrzeb społecznych, w tym: - rozwijania dorobku zawodu, - podtrzymywania etosu zawodu, - przestrzegania i rozwijania zasad etyki zawodowej oraz działania na rzecz przestrzegania tych zasad, - przewodniczenia grupie i ponoszenia odpowiedzialności za nią	P7S_KR

4.2. Opis procesu kształcenia

Proces kształcenia jest ściśle powiązany z misją uczelni, określoną w statucie WAT, jak i strategią Uczelni oraz strategią Wydziału Cybernetyki a kierunek studiów jest przyporządkowany do dyscypliny naukowej Informatyka Techniczna i Telekomunikacja. To tworzy zasadnicze wyznaczniki dla realizowanego procesu kształcenia. W procedurze kształtowania procesu kształcenia uczestniczą przedstawiciele otoczenia społeczno-gospodarczego, w tym pracodawcy, zatrudniający absolwentów lub przyjmujący studentów na praktyki zawodowe. Istotną cechą koncepcji kształcenia jest ciągła konfrontacja i modyfikowanie treści kształcenia z potrzebami pracodawców. Szczególnym pracodawcą jest Ministerstwo Obrony Narodowej, reprezentowane przez Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC). Praktycznie w cyklu rocznym dokonywany jest przez specjalistów z DKWOC przegląd aktualnych treści kształcenia i zgłaszane są uwagi. Ponadto, znaczącą rolę odgrywa Rada ds. Kwalifikacji Absolwentów Wydziału Cybernetyki, będąca ciałem doradczym dziekana Wydziału Cybernetyki WAT, a wśród przedstawicieli Rady są dowódca i zastępca DKWOC

W module kształcenia kierunkowego (profil politechniczny) realizowane jest kształcenie w zakresie wymaganym dla kierunku studiów. Jest ono kontynuowane także w module kształcenia specjalistycznego, gdzie odbywa się zaawansowane kształcenie specjalistyczne (wojskowo-cywilne) określone specjalnościami kształcenia. Proces kształcenia w tej części jest realizowany w uczelni oraz w wybranych centrach szkolenia i jednostkach wojskowych w formie szkoleń specjalistycznych i praktyk zawodowych.
W planie studiów przewidziane są dwie formy praktycznego szkolenia specjalistycznego w dziedzinie IT/CYBER/CRYPTO – praktyki zawodowe specjalistyczne oraz szkolenia specjalistyczne po VI i po VIII semestrze studiów, o programie szczegółowym określonym specjalnością kształcenia.

4.3. Sposób weryfikacji kierunkowych efektów uczenia się

Weryfikacja zakładanych efektów uczenia się kierunkowego prowadzona jest systematycznie przez cały okres trwania szkolenia. Warunkiem zaliczenia każdego przedmiotu jest uzyskanie pozytywnej oceny z obowiązującego rygoru dydaktycznego: zaliczenia na ocenę.

Szczegółowe informacje dotyczące weryfikacji zakładanych efektów uczenia się z poszczególnych przedmiotów i modułów kształcenia określone są w sylabusach przedmiotów i przedstawiane studentom wojskowym w początkowym etapie zajęć. Wszystkie sylabusy przedmiotów uzgadniane są z Wydziałem Cybernetyki WAT, który reprezentuje Dziekan. Praktyki zalicza kierownik praktyk z Wydziału Cybernetyki WAT na podstawie opinii /oceny/ opiekuna praktyki z ramienia instytucji.

Wdrożenie koncepcji prowadzenia zajęć w oparciu o efekty uczenia się przekłada się na różnorodne formy i kryteria ewaluacji. Istotnym aspektem weryfikacji jest klarowne określenie kryteriów oceny w odniesieniu do poszczególnych efektów uczenia się. Na początku zajęć należy wyjaśnić, jakich efektów prowadzący oczekuje oraz jak są definiowane poszczególne poziomy osiągnięcia tych efektów. Same sposoby weryfikacji zakładanych efektów uczenia się zależą przede wszystkim od rodzaju zajęć. Szczegółowe zasady znajdują się w sylabusach do poszczególnych modułów kształcenia. Uogólniając, można jednakże wskazać wiele powtarzalnych zasad oceniania i weryfikacji.

Każdy przedmiot kształcenia kierunkowego zaliczany jest na podstawie egzaminu lub zaliczenia na ocenę. Egzamin może mieć formę pytań pisemną lub ustną w postaci: zadań, pytań otwartych lub testu (zwykłego albo komputerowego). Warunkiem dopuszczenia do zaliczenia/egzaminu jest zaliczenie pozytywne wszystkich innych rygorów, tj. ćwiczeń rachunkowych/konwersatoryjnych, ćwiczeń laboratoryjnych oraz seminarium i projektu.

Ćwiczenia laboratoryjne są prowadzone w salach komputerowych. Mogą być poprzedzane sprawdzeniem wiedzy studentów w zakresie zagadnień związanych z danym tematem. Po wykonaniu ćwiczenia studenci mogą wykonywać sprawozdania, w których muszą się wykazać umiejętnością podsumowania wykonanej pracy, analizy otrzymanych wyników i formułowania wniosków w oparciu o pozyskane umiejętności i doświadczenie.

Projekty zespołowe, jak również zadania laboratoryjne grupowe, dają podstawę do weryfikacji umiejętności działania w zespole, podziału, harmonogramowania i organizowania pracy a także odpowiedzialności za wspólne wyniki.

Ćwiczenia rachunkowe/konwersatoryjne są prowadzone w formie interaktywnej. Kolejne zajęcia realizowane są wg schematu: utrwalenie wiedzy teoretycznej z wykładów, zapoznanie studentów ze schematami rozwiązywania problemów na przykładach, samodzielna praca studentów nadzorowana przez prowadzącego, praca własna.

Karty informacyjne przedmiotów zawierają trójstronne powiązania pomiędzy poszczególnymi tematami zajęć a sposobami weryfikacji i wszystkimi wskazanymi dla modułu efektami.

Umiejętności samodzielnego rozwiązywania problemów i prezentowania ich w logicznie usystematyzowanej postaci (w tym pisemnej) weryfikowane są poprzez realizację projektów oraz pracy dyplomowej. Jest to poprzedzone lub uzupełnione prezentowaniem multimedialnym w trakcie seminariów dyplomowych.

4.4. Macierz pokrycia kierunkowych efektów uczenia się

Grupy zajęć/ przedmiotów i przypisane do nich punkty ECTS i efekty uczenia (odniesienie do efektów kierunkowych)

L.p.	Nazwa przedmiotu	Punkty ECTS	Kod dysc.	Symbol efektów uczenia się
I. Grupa treści kształcenia ogólnego				
1	Wprowadzenie do studiowania	0,5	NS	K_U18, K_K01
2	Ochrona własności intelektualnych	1	NP.	K_W01, K_W20, K_W21, K_K01, K_K02, K_K03, K_K05, K_K06
3	Wprowadzenie do informatyki	3	ITT	K_W05, K_W20, K_W21
4	Podstawy zarządzania i przedsiębiorczości	2,5	NZJ	K_W01, K_W20, K_W21, K_U01, K_K03, K_K04
II. Grupa treści kształcenia podstawowego				
1	Wprowadzenie do metrologii	3	AEE	K_W03, K_U04
2	Podstawy grafiki inżynierskiej	3	IM	K_W02, K_U03, K_U18
3	Matematyka 1	6	M	K_W02, K_U03, K_U18
4	Matematyka 2	6	M	K_W02, K_U03, K_U18
5	Matematyka dyskretna 1	2,5	M	K_W02, K_U03, K_U18
6	Analiza matematyczna	4	M	K_W02, K_U03, K_U18
7	Fizyka 1	6	NF	K_W02, K_U03, K_U18
8	Matematyka dyskretna 2	3	M	K_W02, K_U03, K_U18
9	Rachunek prawdopodobieństwa	3	M	K_W02, K_U03, K_U18
10	Teoretyczne podstawy informatyki	3	ITT	K_W02, K_U03, K_U18
11	Fizyka 2	4	NF	K_W05, K_U03, K_U18
12	Teoria grafów i sieci	2	ITT	K_W02, K_W07, K_W10, K_U03, K_U18
13	Podstawy optymalizacji	3	ITT	K_W02, K_U03, K_U18
14	Statystyka matematyczna	2	M	K_W02, K_U03, K_U18
15	Modelowanie matematyczne	3	ITT	K_W02, K_W11, K_U03, K_U18
16	Bezpieczeństwo pracy i ergonomia	1	ITT	K_W15, K_U12
17	Podstawy bezpieczeństwa informacji	2	ITT	K_W14, K_U11

III. Grupa treści kształcenia kierunkowego				
1	Wprowadzenie do programowania	3	ITT	K_W05, K_W06, K_W08, K_W09, K_U05, K_U07, K_U13, K_U15, K_U18
2	Podstawy techniki komputerów	5	ITT	K_W04, K_W16, K_U13
3	Architektura i organizacja komputerów	5	ITT	K_W17, K_U13
4	Podstawy podzespołów komputerów	2	ITT	K_W04, K_W16, K_W19, K_U13
5	Algorytmy i struktury danych	4	ITT	K_W05, K_U05, K_U07, K_U16
6	Teoria informacji i kodowania	3	ITT	K_W05, K_W18, K_W19, K_U05, K_U14
7	Programowanie niskopoziomowe i analiza kodu	2	ITT	K_W05, K_U05
8	Programowanie obiektowe	3	ITT	K_W05, K_W08, K_W09, K_U05, K_U07, K_U18
9	Bazy danych	3	ITT	K_W05, K_W08, K_U05, K_U06, K_U07, K_U18
10	Zastosowanie kryptografii w systemach teleinformatycznych	3	ITT	K_W23, K_U12, K_U18
11	Systemy operacyjne	5	ITT	K_W12, K_U09
12	Elementy teorii liczb	3	ITT	K_W02 , K_W22, K_U03
13	Wybrane elementy kryptologii	4	M	K_W02, K_U03, K_U17
14	Interfejsy komputerów	3	ITT	K_W16, K_U13
15	Zastosowania kryptografii w Internecie	3	ITT	K_W23, K_U19, K_U20
16	Inżynieria oprogramowania	4	ITT	K_W05, K_W06, K_W08, K_W09, K_W20, K_U05, K_U07, K_U18
17	Sieci komputerowe	5,5	ITT	K_W13, K_U10
18	Protokoły kryptograficzne	3	ITT	K_W23, K_U19, K_U20
19	Niezawodność systemów komputerowych	2	ITT	K_W10, K_W11, K_W17, K_U07, K_U11, K_U13, K_U18
20	Bezpieczeństwo baz danych	4	ITT	K_W06, K_W08, K_U05, K_U06, K_U07, K_U11
21	Procesy stochastyczne	2	M	K_W02, K_W11, K_U03

22	Metody symulacji komputerowej	4	ITT	K_W02, K_W11, K_U05, K_U08, K_K01
23	Steganografia	3	ITT	K_W02, K_W22, K_W23, K_U11, K_U19, K_U20, K_K01
24	Diagnostyka i tolerowanie uszkodzeń	6	ITT	K_W17, K_U13, K_K01, K_K05, K_K06
25	Sztuczna inteligencja	2	ITT	K_W08, K_W11, K_W12, K_W20, K_W24, K_U08, K_U09, K_U15, K_U17, K_U21
IV.	**Moduły związane z pracą dyplomową oraz praktyką zawodową i specjalistyczną**			
1	Seminarium przeddyplomowe	1	ITT	K_W02, K_W03, K_W04, K_W05, K_W06, K_W07, K_W08, K_W09, K_U02, K_U05, K_U06, K_U07, K_U08, K_U09, K_U10, K_U11, K_U12, K_U13, K_U14, K_K01
2	Seminarium dyplomowe	4	ITT	K_W02, K_W03, K_W04, K_W05, K_W06, K_W07, K_W08, K_W09, K_U02, K_U05, K_U06, K_U07, K_U08, K_U09, K_U10, K_U11, K_U12, K_U13, K_U14, K_K01
3	Praca dyplomowa	22	ITT	K_W02, K_W03, K_W04, K_W05, K_W06, K_W07, K_W08, K_W09, K_U02, K_U05, K_U06, K_U07, K_U08, K_U09, K_U10, K_U11, K_U12, K_U13, K_U14, K_K01
4	Egzamin na oficera			K_W06, K_W07, K_W08, K_W09, K_W10, K_W11, K_W12, K_W13, K_W14, K_W17, K_W23, K_U05,

				K_U06, K_U07, K_U08, K_U09, K_U10, K_U11, K_U12, K_U13, K_U14, K_U15, K_U16, K_U17, K_U18, K_K01, K_K02, K_K03, K_K04, K_K05
5	Praktyka dowódcy drużyny i Praktyka dowódcy plutonu	8		K_W06, K_W07, K_W08, K_W09, K_W10, K_W11, K_W12, K_W13, K_W14, K_W17, K_W23, K_U05, K_U06, K_U07, K_U08, K_U09, K_U10, K_U11, K_U12, K_U13, K_U14, K_U15, K_U16, K_U17, K_U18, K_K01, K_K02, K_K03, K_K04, K_K05
6	Praktyka zawodowa i Szkolenie specjalistyczne	8	ITT	K_W06, K_W07, K_W08, K_W09, K_W10, K_W11, K_W12, K_W13, K_W14, K_W17, K_W23, K_U05, K_U06, K_U07, K_U08, K_U09, K_U10, K_U11, K_U12, K_U13, K_U14, K_U15, K_U16, K_U17, K_U18, K_K01, K_K02, K_K03, K_K04, K_K05

Macierz pokrycia kierunkowych efektów uczenia się w zakresie treści kształcenia ogólnego, podstawowego, kierunkowego, pracy dyplomowej i praktyki zawodowej

	I. Grupa treści kształcenia				II. Grupa treści kształcenia podstawowego																	III. Grupa treści kształcenia kierunkowego																									Praca dyplomowa, praktyka zawodowa					
	Wprowadzenie do studiowania	Ochrona własności intelektualnych	Wprowadzenie do informatyki	Podstawy zarządzania i przedsiębiorczości	Wprowadzenie do metrologii	Podstawy grafiki inżynierskiej	Matematyka 1	Matematyka 2	Matematyka dyskretna 1	Analiza matematyczna	Fizyka 1	Matematyka dyskretna 2	Rachunek prawdopodobieństwa	Teoretyczne podstawy informatyki	Fizyka 2	Teoria grafów i sieci	Podstawy optymalizacji	Statystyka matematyczna	Modelowanie matematyczne	Bezpieczeństwo pracy i ergonomia	Podstawy bezpieczeństwa informacji	Wprowadzenie do programowania	Podstawy techniki komputerów	Architektura i organizacja komputerów	Podstawy podzespołów komputerów	Algorytmy i struktury danych	Teoria informacji i kodowania	Programowanie niskopoziomowe i analiza kodu	Programowanie obiektowe	Bazy danych	Zastosowanie kryptografii w systemach teleinformatycznych	Systemy operacyjne	Elementy teorii liczb	Wybrane elementy kryptologii	Interfejscy kompuerów	Zastosowania kryptografii w Internecie	Inżynieria oprogramowania	Sieci komputerowe	Protokoły kryptograficzne	Niezawodność systemów komputerowych	Bezpieczeństwo baz danych	Procesy stochastyczne	Metody symulacji komputerowej	Steganografia	Diagnostyka i tolerowanie uszkodzeń	Sztuczna inteligencja	Seminarium przeddyplomowe	Seminarium dyplomowe	Praca dyplomowa	Egzamin na oficera	Praktyka dowódcy drużyny i plutonu	Praktyka zawodowa i Szkolenie specjalistyczne
K_W01		+		+																																																
K_W02						+	+	+	+	+	+	+	+	+		+	+	+	+														+	+								+	+	+			+	+	+			
K_W03					+																																										+	+	+			
K_W04																							+		+																						+	+	+			
K_W05			+												+							+				+	+	+	+	+							+										+	+	+			
K_W06																						+															+				+						+	+	+	+	+	+
K_W07																+																															+	+	+	+	+	+
K_W08																						+							+	+							+				+					+	+	+	+	+	+	+
K_W09																						+							+								+										+	+	+	+	+	+
K_W10																+																								+										+	+	+
K_W11																			+																					+		+	+			+				+	+	+
K_W12																																+														+				+	+	+
K_W13																																						+												+	+	+
K_W14																					+																													+	+	+
K_W15																				+																																
K_W16																							+		+										+																	
K_W17																								+																+					+					+	+	+
K_W18																											+																									
K_W19																									+		+																									
K_W20		+	+	+																																	+									+						
K_W21		+	+	+																																																
K_W22																																	+											+								
K_W23																															+					+			+					+						+	+	+
K_W24																																														+						
K_U01				+																																																
K_U02																																															+	+	+			
K_U03						+	+	+	+	+	+	+	+	+	+	+	+	+	+														+	+								+										
K_U04					+																																															
K_U05																						+				+	+	+	+	+							+				+		+				+	+	+	+	+	+
K_U06																														+											+						+	+	+	+	+	+
K_U07																						+				+			+	+							+			+	+						+	+	+	+	+	+
K_U08																																											+			+	+	+	+	+	+	+
K_U09																																+														+	+	+	+	+	+	+
K_U10																																						+									+	+	+	+	+	+
K_U11																					+																			+	+			+			+	+	+	+	+	+
K_U12																				+											+																+	+	+	+	+	+
K_U13																						+	+	+	+										+					+					+		+	+	+	+	+	+
K_U14																											+																				+	+	+	+	+	+
K_U15																						+																								+				+	+	+
K_U16																										+																								+	+	+
K_U17																																		+												+				+	+	+
K_U18	+					+	+	+	+	+	+	+	+	+	+	+	+	+	+			+							+	+	+						+			+										+	+	+
K_U19																																				+			+					+								
K_U20																																				+			+					+								
K_U21																																														+						
K_K01	+	+																																									+	+	+		+	+	+	+	+	+
K_K02		+																																																+	+	+
K_K03		+		+																																														+	+	+
K_K04				+																																														+	+	+
K_K05		+																																											+					+	+	+
K_K06		+																																											+							

5. MODUŁ SPECJALISTYCZNY

5.1. Opis zakładanych efektów uczenia się określonych dla danego korpusu osobowego (grupy osobowej)

Zakładane są następujące specjalistyczne efekty uczenia się określone dla korpusu osobowego (grupy osobowej):

Symbol	Kompetencje oficera właściwe dla danego korpusu osobowego (grupy osobowej) w ujęciu efektów uczenia się i szkolenia	Odniesienie do kierunkowych efektów uczenia się
Kategoria efektów: *WIEDZA*	**Absolwent**	
W_29A	Posiada wiedzę z zakresu kryptologii i cyberbezpieczeństwa, projektowania, budowy i eksploatacji systemów opartych o rozwiązania kryptograficzne w oddziałach dowodzenia i łączności, a także instytucjach centralnych;	K_W01, K_W14, K_W15, K_W16
W_29B	Posiada wiedzę z zakresu zarządzania bezpieczeństwem w cyberprzestrzeni i bezpieczeństwem systemów będących na wyposażeniu SZ RP i instytucji centralnych;	K_W05, K_W07, K_W12
Kategoria efektów: *UMIEJĘTNOŚCI*	**Absolwent**	
U_29A	Posiada umiejętność budowania systemów opartych o rozwiązania kryptograficzne, kierowania ich wdrażaniem oraz zarządzania bezpieczeństwem w cyberprzestrzeni;	K_U02, K_U03, K_U11, K_U12, K_U13, K_U18
U_29B	Posiada umiejętność organizacji i obsługi systemów opartych o rozwiązania kryptograficzne oraz systemów cyberbezpieczeństwa w SZ RP;	K_U07, K_U08, K_U16, K_U21
Kategoria efektów: *KOMPETENCJE PERSONALNE I SPOŁECZNE*	**Absolwent**	
K_29A_1 K_29B_1	Jest gotowy do samodoskonalenia i pogłębiania wiedzy w zakresie rozwoju kryptologii w środowisku militarnym i cywilnym;	K_K01, K_K06
K_29A_2 K_29B_2	Jest otwarty na nowości technologiczne i inicjatywy we wprowadzaniu nowych technologii w SZ RP.	K_K03, K_K05

5.2. Opis procesu kształcenia

Zgodnie z przyjętym w Siłach Zbrojnych RP modelem studiów wojskowych kształcenie specjalistyczne (wojskowo-cywilne) określone jest dla specjalności kształcenia. Kształcenie specjalistyczne dla danego korpusu osobowego (grupy osobowej) realizowane jest w uczelni, w centrach szkolenia oraz w jednostkach wojskowych lub instytucjach.

Program studiów w części dotyczącej modułu specjalistycznego obejmuje:

- grupę treści specjalistycznych realizowaną oddzielnie dla każdej specjalności;
- grupę treści specjalistycznych realizowaną w Centrach Szkolenia w okresie letnich przerw międzysemestralnych, wspólną dla wszystkich specjalności;

- praktykę zawodową w dziedzinie IT/CYBER/CRYPTO w wymiarze 4 tygodni – dwukrotnie w trakcie studiów (w formie praktyk oraz szkolenia).

Praktyczne kształcenie specjalistyczne jest realizowane w wytypowanych jednostkach i centrach szkolenia i odbywa się po VI i VIII semestrze studiów. Kandydaci na oficerów odbywają czterotygodniowe praktyki zawodowe w jednostkach wojskowych lub instytucjach, realizując konkretne zadania projektowe, pracując pod nadzorem wytypowanych specjalistów Instytucji i jednostek wojskowych.

5.3. Sposób weryfikacji zakładanych specjalistycznych efektów uczenia się

Weryfikacja zakładanych efektów uczenia się specjalistycznego prowadzona jest systematycznie przez cały okres trwania szkolenia. Warunkiem zaliczenia każdego szkolenia jest uzyskanie pozytywnej oceny z obowiązującego rygoru dydaktycznego: zaliczenia na ocenę. Kandydaci na oficerów wykazać się muszą praktyczną znajomością zagadnień w zakresie eksploatacji sprzętu łączności i informatyki, merytorycznym udziałem w pracach programowo – implementacyjnych realizowanych w instytucjach, w których odbywają praktykę.

Szczegółowe informacje dotyczące weryfikacji zakładanych efektów uczenia się z poszczególnych przedmiotów i modułów kształcenia określone są w kartach informacyjnych przedmiotów i przedstawiane studentom wojskowym na miesiąc przed rozpoczęciem zajęć. Karty informacyjne przedmiotów związanych z kształceniem specjalistyczny opracowywane są w centrach szkolenia oraz instytucjach, w których odbywa się szkolenia oraz praktyki. Wszystkie karty informacyjne przedmiotów realizowanych w ramach szkoleń specjalistycznych i praktyk zawodowych uzgadniane są z Wydziałem Cybernetyki WAT, który reprezentuje Dziekan. Praktykę zalicza kierownik praktyk z Wydziału Cybernetyki WAT na podstawie opinii /oceny/ opiekuna praktyki z ramienia instytucji.

Wdrożenie koncepcji prowadzenia zajęć w oparciu o efekty uczenia się przekłada się na różnorodne formy i kryteria ewaluacji. Istotnym aspektem weryfikacji jest klarowne określenie kryteriów oceny w odniesieniu do poszczególnych efektów uczenia się. Na początku zajęć należy wyjaśnić, jakich efektów prowadzący oczekuje oraz jak są definiowane poszczególne poziomy osiągnięcia tych efektów. Same sposoby weryfikacji zakładanych efektów uczenia się zależą przede wszystkim od rodzaju zajęć. Szczegółowe zasady znajdują się w sylabusach do poszczególnych modułów kształcenia. Uogólniając, można jednakże wskazać wiele powtarzalnych zasad oceniania i weryfikacji.

Każdy przedmiot kształcenia kierunkowego zaliczany jest na podstawie egzaminu lub zaliczenia na ocenę. Egzamin może mieć formę pytań pisemną lub ustną w postaci: zadań, pytań otwartych lub testu (zwykłego albo komputerowego). Warunkiem dopuszczenia do zaliczenia/egzaminu jest zaliczenie pozytywne wszystkich innych rygorów, tj. ćwiczeń rachunkowych/konwersatoryjnych, ćwiczeń laboratoryjnych oraz seminarium i projektu.

Ćwiczenia laboratoryjne są prowadzone w salach komputerowych. Mogą być poprzedzane sprawdzeniem wiedzy studentów w zakresie zagadnień związanych z danym tematem. Po wykonaniu ćwiczenia studenci mogą wykonywać sprawozdania, w których muszą się wykazać umiejętnością podsumowania wykonanej pracy, analizy otrzymanych wyników i formułowania wniosków w oparciu o pozyskane umiejętności i doświadczenie.

Projekty zespołowe, jak również zadania laboratoryjne grupowe, dają podstawę do weryfikacji umiejętności działania w zespole, podziału, harmonogramowania i organizowania pracy a także odpowiedzialności za wspólne wyniki.

Ćwiczenia rachunkowe/konwersatoryjne są prowadzone w formie interaktywnej. Kolejne zajęcia realizowane są wg schematu: utrwalenie wiedzy teoretycznej z wykładów, zapoznanie studentów ze schematami rozwiązywania problemów na przykładach, samodzielna praca studentów nadzorowana przez prowadzącego, praca własna.

Karty informacyjne przedmiotów zawierają trójstronne powiązania pomiędzy poszczególnymi tematami zajęć a sposobami weryfikacji i wszystkimi wskazanymi dla modułu efektami.

Umiejętności samodzielnego rozwiązywania problemów i prezentowania ich w logicznie usystematyzowanej postaci (w tym pisemnej) weryfikowane są poprzez realizację projektów przejściowych oraz pracy dyplomowej. Jest to poprzedzone lub uzupełnione prezentowaniem multimedialnym w trakcie seminariów przedmiotowych i (przed)dyplomowych. Innym sposobem sprawdzenia zakładanych efektów uczenia się kierunkowego jest kształcenie specjalistyczne (praktyka zawodowa) – dotyczy to przede wszystkim umiejętności wykorzystania wiedzy teoretycznej w praktyce oraz współdziałania w zespole ludzkim.

5.4. Macierz pokrycia specjalistycznych efektów uczenia się

Grupy zajęć/ przedmiotów i przypisane do nich punkty ECTS i efekty uczenia (odniesienie do efektów specjalistycznych)

L.p.	Nazwa przedmiotu	Punkty ECTS	Kod dysc.	Symbol efektów uczenia się
Grupa treści kształcenia wybieralnego/specjalistycznego				
Specjalność *„systemy kryptograficzne”*				
1	Metody statystyczne w kryptologii	4	M	K_W02, K_W22, K_U03
2	Projekt zespołowy	4	ITT	K_W06, K_W08, K_W23, K_U05, K_U07, K_U20
3	Funkcje boolowskie w kryptologii	4	ITT	K_W22, K_W23, K_U19
4	Projektowanie kryptograficznych układów cyfrowych	5	ITT	K_W22, K_W23, K_U11, K_U19
5	Struktury algebraiczne	4	ITT	K_W23, K_U11, K_U19
6	Wstęp do kryptoanalizy algorytmów klucza publicznego	2	ITT	K_W02, K_W22, K_U19
7	Krzywe eliptyczne	2	M	K_W02, K_W22, K_W23, K_U19
8	Zastosowania teorii krat w kryptologii	3	ITT	K_W02, K_W22, K_U19

9	Algorytmy blokowe	4	ITT	K_W22, K_W23, K_U19
10	Algorytmy strumieniowe	3	ITT	K_W22, K_W23, K_U19
11	Jednokierunkowe funkcje skrótu	2	ITT	K_W22, K_W23, K_U19
12	Systemy zabezpieczeń pomieszczeń	2	ITT	K_W23, K_U19
13	Quantum and Post-Quantum Cryptology (w języku angielskim)	3	ITT	K_W06, K_W08, K_W14, K_U02, K_U11, K_U18, K_K01
14	Narzędzia kryptoanalizy	2	ITT	K_W22, K_W23, K_U19
15	Generacja i testowanie losowości	3	ITT	K_W02, K_U03
16	Teoria ciał skończonych	2	M	K_W02, K_U03
17	Projekt z zakresu matematycznych i informatycznych podstaw kryptologii	2	ITT	K_W02, K_W06, K_W08, K_U03, K_U11, K_U16, K_U18, K_K01
18	Projektowanie kryptograficznych układów cyfrowych II	4	ITT	K_W06, K_W08, K_W14, K_U05, K_U11, K_U18, K_K01
19	Akredytacja systemów teleinformatycznych	4	ITT	K_W08, K_W13, K_U10, K_U18, K_K01 K_K02, K_K05
20	Elements of Public-Key Cryptology	2	ITT	K_W02, K_W22, K_U02, K_U11
21	Ataki algebraiczne	3	ITT	K_W02, K_U03, K_U11
22	Kryptoanaliza algorytmów blokowych	3	ITT	K_W06, K_W08, K_W14, K_W22, K_U11, K_U18, K_K01
23	Kryptoanaliza algorytmów strumieniowych	5	ITT	K_W06, K_W08, K_W14, K_W22, K_U11, K_U18, K_K01
24	Metody numeryczne w kryptologii	5	M	K_W02, K_U03
25	Krzywe hipereliptyczne w kryptologii	4	ITT	K_W02, K_W12, K_U02, K_U15

Macierz pokrycia specjalistycznych efektów uczenia się
systemy kryptograficzne

	Systemy kryptograficzne																										
	Metody statystyczne w kryptologii	Projekt zespołowy	Funkcje boolowskie w kryptologii	Projektowanie kryptograficznych układów cyfrowych	Struktury algebraiczne	publicznego	Krzywe eliptyczne	Zastosowania teorii krat w kryptologii	Algorytmy blokowe	Algorytmy strumieniowe	Jednokierunkowe funkcje skrótu	Systemy zabezpieczeń pomieszczeń	Quantum and post-quantum cryptology	Narzędzia kryptoanalizy	Generacja i testowanie losowości	Teoria ciał skończonycfh	Projekt z zakresu matematycznych i informatycznych podstaw kryptologii	Projektowanie kryptograficznych układów cyfrowych II	Akredytacja systemów telenformatycznych	Element of Public-Key Cryptology	Ataki algebraiczne	Kryptoanaliza algorytmów blokowych	Kryptologia algorytmów strumieniowych	Metody numeryczne w kryptologii	Krzywe hiperliptyczne w kryptologii
K_W01																											
K_W02	+					+	+	+							+	+	+			+	+			+	+
K_W03																											
K_W04																											
K_W05																											
K_W06		+											+				+	+				+	+		
K_W07																											
K_W08		+											+				+	+	+			+	+		
K_W09																											
K_W10																											
K_W11																											
K_W12																											+
K_W13																			+								
K_W14													+					+					+	+		
K_W15																											
K_W16																											
K_W17																											
K_W18																											
K_W19																											
K_W20																											
K_W21																											
K_W22	+		+	+		+	+	+	+	+	+			+						+		+	+			
K_W23		+	+	+	+		+		+	+	+	+		+												
K_W24																											
K_U01																											
K_U02													+							+						+
K_U03	+														+	+	+				+			+		
K_U04																											
K_U05		+																+								
K_U06																											
K_U07		+																									
K_U08																											
K_U09																											
K_U10																			+								
K_U11				+	+								+				+	+		+	+	+	+			
K_U12																											
K_U13																											
K_U14																											
K_U15																											+
K_U16																	+										
K_U17																											
K_U18													+				+	+	+			+	+			
K_U19			+	+	+	+	+	+	+	+	+	+		+												
K_U20		+																									
K_U21																											
K_K01													+				+	+	+			+	+			
K_K02																			+								
K_K03																											
K_K04																											
K_K05																			+								
K_K06																											

L.p.	Nazwa przedmiotu	Punkty ECTS	Kod dysc.	Symbol efektów uczenia się
Grupa treści kształcenia wybieralnego/specjalistycznego				
Specjalność *„bezpieczeństwo informacyjne”*				
1	Hurtownie danych	2	ITT	K_W07, K_W08, K_U05, K_U06
2	Metody prognozowania	3	M	K_W02, K_W11, K_U03, K_U04, K_U06
3	Programowanie w językach funkcyjnych	3	ITT	K_W05, K_W06, K_W11, K_U05, K_U09
4	Metody numeryczne	2	ITT	K_W02, K_W11, K_U03, K_U04, K_U06
5	Automaty i języki formalne	3	ITT	K_W05, K_W06, K_U05
6	Analiza i wizualizacja danych	3	ITT	K_W02, K_W11, K_U03, K_U04, K_U06
7	Techniki algorytmiczne	3	ITT	K_W03, K_W04, K_W09, K_U03, K_U04
8	Bussines modeling in UML	2	ITT	K_W09, K_U10, K_U13
9	Modelowanie i symulacja procesów biznesowych	2	ITT	K_W07, K_W10, K_U06, K_U08, K_U17, K_K01
10	Metody uczenia maszynowego	3	ITT	K_W02, K_W11, K_W24, K_U03, K_U04, K_U06, K_U21
11	Metody projektowania i wdrażania systemów informatycznych	4	ITT	K_W06, K_W08, K_W09, K_U07, K_U17, K_K01
12	Metody eksploracji danych	3	ITT	K_W02, K_W11, K_W24, K_U03, K_U04, K_U06, K_U21
13	Technologie usługowe i mobilne	2	ITT	K_W06, K_W08, K_W09, K_W12, K_W13, K_U05, K_U07, K_U11, K_U17
14	Metody sztucznej inteligencji	2	ITT	K_W02, K_W05, K_W11, K_W22, K_W24, K_U09, K_U17, K_U21, K_K01
15	Metody ilościowe analizy ryzyka	2	ITT	K_W02, K_W10, K_W11, K_W14, K_U08, K_U09, K_K01
16	Bazy danych NoSQL	3	ITT	K_W03, K_W04, K_W09, K_U03, K_U04
17	Bezpieczeństwo systemów informacyjnych	3	ITT	K_W07, K_W08, K_W14, K_U06, K_U17, K_K01, K_K05

18	Metody i systemy wspomagania decyzji	3	ITT	K_W02, K_W11, K_W24, K_U03, K_U09, K_U21
19	Podstawy kryptologii współczesnej	2	ITT	K_W03, K_W04, K_W08, K_W09, K_W12, K_U03, K_U10, K_U12, K_U15
20	Modelowanie i analiza sieci złożonych	3	ITT	K_W02, K_W04, K_W05, K_U02, K_U05, K_U14
21	Rozproszone przetwarzanie danych	3	ITT	K_W03, K_W04, K_W09, K_U03, K_U04
22	Zarządzanie projektami	3	ITT	K_W03, K_W04, K_U03, K_U04, K_K01, K_K06
23	Ilościowe metody oceny bezpieczeństwa systemów teleinformatycznych	2	ITT	K_W02, K_W05, K_W08, K_U02, K_U05, K_U09, K_U14, K_K01
24	Zaawansowane metody uczenia maszynowego	3	ITT	K_W02, K_W05, K_W09, K_W24, K_U02, K_U04, K_U14, K_U21
25	Teoria wojny informacyjnej	2	ITT	K_W01, K_W02, K_W04, K_W05, K_U01, K_U02, K_U05, K_U14
26	Technologie Internetu rzeczy	4	ITT	K_W11, K_W13, K_U16, K_K03, K_K05
27	Przetwarzanie języka naturalnego (NLP)	3	ITT	K_W03, K_W04, K_W09, K_W22, K_W24, K_U03, K_U04, K_U21
28	Projekt z zakresu bezpieczeństwa informacji	4	ITT	K_W06, K_W09, K_W11, K_U03, K_U04, K_U05, K_U06, K_U12, K_K02, K_K03
29	Zarządzanie wiedzą	4	ITT	K_W02, K_W11, K_U03, K_U04, K_U06

Macierz pokrycia specjalistycznych efektów uczenia się: bezpieczeństwo informacyjne

	Bezpieczeństwo informacyjne																												
	Hurtownie danych	Metody prognozowania	Programowanie w językach funkcyjnych	Metody numeryczne	Automaty i języki formalne	Analiza i wizualizacja danych	Techniki algorytmiczne	Bussines modeling in UML	Modelowanie i symulacja procesów biznesowych	Metody uczenia maszynowego	Metody projektowania i wdrażania systemów informatycznych	Metody eksploracji danych	Technologie usługowe i mobilne	Metody sztucznej inteligencji	Metody ilościowe analizy ryzyka	Bazy danych NoSQL	Bezpieczeństwo systemów informacyjnych	Metody i systemy wspomagania decyzji	Podstawy kryptologii współczesnej	Modelowanie i analiza sieci złożonych	Rozproszone przetwarzanie danych	Zarządzanie projektami	Ilościowe metody oceny bezpieczeństwa systemów teleinformatycznych	Zaawansowane metody uczenia maszynowego	Teoria wojny informacyjnej	Technologie Internetu Rzeczy	Przetwarzanie jeżyka naturalnego (NLP)	Projekt z zakresu bezpieczeństwa informacji	Zarządzanie wiedzą
K_W01																									+				
K_W02		+		+		+				+		+		+	+			+		+			+	+	+				+
K_W03							+									+			+		+	+					+		
K_W04							+									+			+	+	+	+			+		+		
K_W05			+		+									+						+			+	+	+				
K_W06			+		+						+		+															+	
K_W07	+								+								+												
K_W08	+										+		+				+		+				+						
K_W09							+	+			+		+			+			+		+			+			+	+	
K_W10									+						+														
K_W11		+	+	+		+				+		+		+	+			+								+		+	+
K_W12													+						+										
K_W13													+													+			
K_W14															+		+												
K_W15																													
K_W16																													
K_W17																													
K_W18																													
K_W19																													
K_W20																													
K_W21																													
K_W22														+													+		
K_W23																													
K_W24										+		+		+				+						+			+		
K_U01																									+				
K_U02																				+			+	+	+				
K_U03		+		+		+	+			+		+				+		+	+		+	+					+	+	+
K_U04		+		+		+	+			+		+				+					+	+		+			+	+	+
K_U05	+		+		+								+							+				+		+			
K_U06	+	+		+		+			+	+		+					+											+	+
K_U07											+		+																
K_U08									+						+														
K_U09			+											+	+			+						+					
K_U10								+											+										
K_U11													+																
K_U12																			+									+	
K_U13								+																					
K_U14																				+			+	+	+				
K_U15																			+										
K_U16																										+			
K_U17									+		+		+	+			+												
K_U18																													
K_U19																													
K_U20																													
K_U21										+		+		+				+						+			+		
K_K01									+		+			+	+		+					+	+						
K_K02																												+	
K_K03																										+		+	
K_K04																													
K_K05																	+									+			
K_K06																						+							

L.p.	Nazwa przedmiotu	Punkty ECTS	Kod dysc.	Symbol efektów uczenia się
Grupa treści kształcenia wybieralnego/specjalistycznego				
Specjalność *„bezpieczeństwo systemów informatycznych”*				
1	Ataki sieciowe i złośliwe oprogramowanie	3	ITT	K_W11, K_W14, K_U09, K_U11
2	Bezpieczeństwo sieci komputerowych	3	ITT	K_W14, K_U11
3	Podstawy projektowania bezpiecznego oprogramowania	4	ITT	K_W06, K_W14, K_U05, K_U07, K_U12, K_U17
4	Automaty i języki formalne	3	ITT	K_W05, K_W06, K_U05
5	Programowanie w językach funkcyjnych	3	ITT	K_W05, K_W06, K_W11, K_U05, K_U09
6	Techniki algorytmiczne	3	ITT	K_W06, K_W08, K_W09, K_W14, K_U05, K_U07, K_U12, K_U17, K_K05
7	Bussines modeling in UML	2	ITT	K_W09, K_U10, K_U13
8	Modelowanie i symulacja procesów biznesowych	2	ITT	K_W07, K_W10, K_U06, K_U08, K_U17, K_K01
9	Metody eksploracji danych	3	ITT	K_W02, K_W11, K_W24, K_U03, K_U04, K_U06, K_U21
10	Metody i narzędzia generowania kodu wykonywalnego	4	ITT	K_W05, K_W06, K_U08, K_U15, K_U16
11	Metody projektowania i wdrażania systemów informatycznych	4	ITT	K_W06, K_W08, K_W09, K_U07, K_U17, K_K01
12	Technologie usługowe i mobilne	2	ITT	K_W06, K_W08, K_W09, K_W12, K_W13, K_U05, K_U07, K_U11, K_U17
13	Metody sztucznej inteligencji	2	ITT	K_W02, K_W05, K_W11, K_W22, K_W24, K_U09, K_U17, K_U21, K_K01
14	Metody ilościowe analizy ryzyka	2	ITT	K_W02, K_W10, K_W11, K_W14, K_U08, K_U09, K_K01
15	Systemy webowe	2	ITT	K_W03, K_W08, K_U05, K_U09
16	Bezpieczeństwo systemów informacyjnych	3	ITT	K_W07, K_W08, K_W14, K_U06, K_U17, K_K01, K_K05
17	Metody i systemy wspomagania decyzji	3	ITT	K_W02, K_W11, K_W24, K_U03, K_U09, K_U21

18	Obliczenia równoległe i rozproszone	3	ITT	K_W07, K_W14, K_U06, K_U12, K_U17
19	Podstawy kryptologii współczesnej	2	ITT	K_W03, K_W04, K_W08, K_W09, K_W12, K_U03, K_U10, K_U12, K_U15
20	Modelowanie i analiza sieci złożonych	3	ITT	K_W02, K_W04, K_W05, K_U02, K_U05, K_U14
21	Zarządzanie projektami	3	ITT	K_W03, K_W04, K_U03, K_U04, K_K01, K_K06
22	Ilościowe metody oceny bezpieczeństwa systemów teleinformatycznych	2	ITT	K_W02, K_W05, K_W08, K_U02, K_U05, K_U09, K_U14, K_K01
23	Architektura korporacyjna	3	ITT	K_W02, K_W03, K_W04, K_W10, K_U03, K_U04, K_U10
24	Teoria wojny informacyjnej	2	ITT	K_W03, K_W04, K_W09, K_U03, K_U04
25	Inżynieria wsteczna systemów informatycznych	4	ITT	K_W01, K_W02, K_W04, K_W05, K_U01, K_U02, K_U05, K_U14
26	Niezawodność i wydajność systemów informatycznych	3	ITT	K_W03, K_W08, K_U05, K_U09
27	Projekt z zakresu bezpieczeństwa systemów	4	ITT	K_W02, K_W05, K_U02, K_U05, K_U14
28	Inżynieria wsteczna złośliwego oprogramowania	4	ITT	K_W03, K_W08, K_U05, K_U09

Macierz pokrycia specjalistycznych efektów uczenia się: bezpieczeństwo systemów informatycznych

	Bezpieczeństwo systemów informatycznych																												
	Ataki sieciowe i złośliwe oprogramowanie	Bezpieczeństwo sieci komputerowych	Podstawy projektowania bezpiecznego oprogramowania	Automaty i języki formalne	Programowanie w językach funkcyjnych	Techniki algorytmiczne	Bussines modeling in UML	Modelowanie i symulacja procesów biznesowych	Metody eksploracji dannych	Metody i narzędzia generowania kodu wykonywalnego	Metody projektowania i wdrażania systemów informatycznych	Technologie usługowe i mobilne	Metody sztucznej inteligencji	Metody ilościowe analizy ryzyka	Systemy webowe	Bezpieczeństwo systemów informacyjnych	Metody i systemy wspomagania decyzji	Obliczenia równoległe i rozproszone	Podstawy kryptologii współczesnej	Modelowanie i analiza sieci złożonych	Zarządzanie projektami	Ilościowe metody oceny bezpieczeństwa systemów teleinformatycznych	Architektura korporacyjna	Teoria wojny informacyjnej	Inżynieria wsteczna systemów informatycznych	Niezawodność i wydajność systemów informatycznych	Projekt z zakresu bezpieczeństwa systemów	Inżynieria wsteczna złośliwego oprogramowania
_W01																									+				
_W02									+				+	+			+			+		+		+			+		
_W03															+				+		+			+	+		+		+
_W04																			+	+	+			+	+				
_W05				+	+					+			+							+		+			+		+		
_W06			+	+	+	+				+	+	+																	
_W07								+								+		+											
_W08						+					+	+			+	+			+			+				+		+	
_W09						+	+				+	+							+						+				
_W10								+						+										+					
_W11	+				+				+				+	+			+												
_W12												+							+										
_W13												+																	
_W14	+	+	+			+								+		+		+											
_W15																													
_W16																													
_W17																													
_W18																													
_W19																													
_W20																													
_W21																													
_W22														+															
_W23																													
_W24									+					+			+												
_U01																									+				
_U02																				+		+			+		+		
_U03																	+		+		+			+	+				
_U04																					+			+	+				
_U05			+	+	+	+						+			+					+		+			+	+	+	+	
_U06								+								+		+											
_U07			+			+					+	+																	
_U08								+		+				+															
_U09	+				+				+					+	+	+		+								+			+
_U10							+												+					+					
_U11	+	+											+																
_U12			+			+												+	+										
_U13							+																						
_U14																				+		+			+		+		
_U15										+									+										
_U16										+																			
_U17			+			+		+			+	+	+			+		+											
_U18																													
_U19																													
_U20																													
_U21									+					+			+												
_K01								+	+		+		+	+		+					+	+							
_K02																													
_K03																													
_K04																													
_K05						+										+													
_K06																					+								

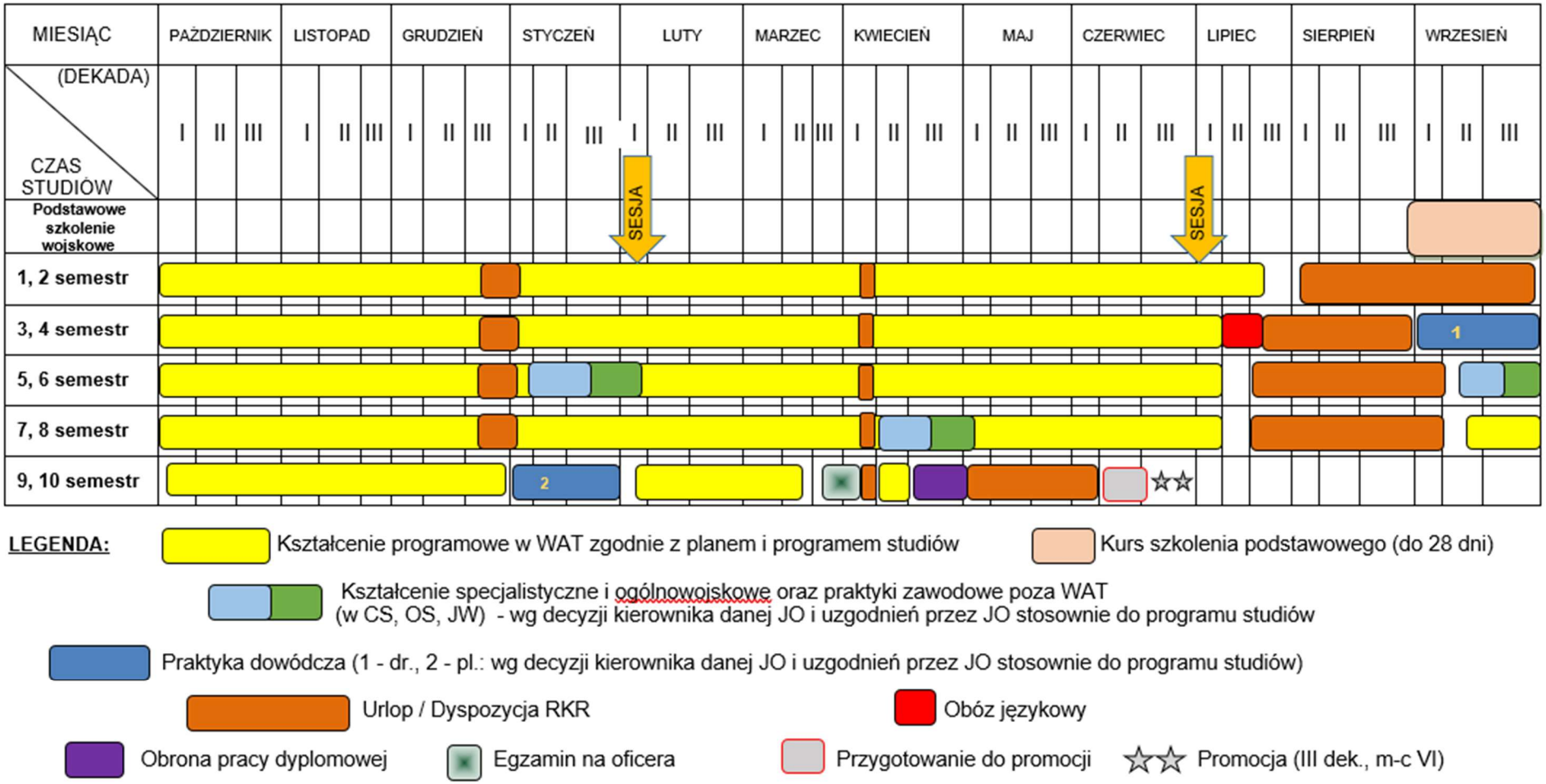
L.p.	Nazwa przedmiotu	Punkty ECTS	Kod dysc.	Symbol efektów uczenia się
Grupa treści kształcenia wybieralnego/specjalistycznego				
Specjalność *„cyberobrona”*				
1	Sieci komputerowe II	2	ITT	K_W13, K_U10
2	JavaEE Technologies	2	ITT	K_W05, K_W06, K_W08, K_U02, K_U05
3	HTML i aplikacje webowe	2	ITT	K_W06, K_U05
4	Systemy operacyjne UNIX	3	ITT	K_W12, K_U09
5	Ataki sieciowe	3	ITT	K_W14, K_U11
6	Oprogramowanie niepożądane i inspekcja kodu	3	ITT	K_W14, K_U11
7	Eksploracja sieci teleinformatycznych	3	ITT	K_W14, K_U11
8	Systemy wbudowane	3	M	K_W19 K_U14
9	Bezpieczeństwo sieci bezprzewodowych	2	ITT	K_W13, K_W14, K_U11
10	Modelowanie i analiza systemów teleinformatycznych	4	ITT	K_W08, K_W10, K_U05, K_U18, K_K01
11	Systemy bezpieczeństwa sieciowego	2	ITT	K_W13, K_W14, K_U11
12	Podstawy przetwarzania rozproszonego	2	ITT	K_W05, K_U05
13	Administrowanie środowiskiem Windows	4	ITT	K_W12, K_U09
14	Bezpieczeństwo sieci IPv6	3	ITT	K_W13, K_W14, K_U11, K_K05
15	Projektowanie i wytwarzanie systemów teleinformatycznych	4	ITT	K_W08, K_W13, K_U05, K_U10,
16	Zabezpieczenia teleinformatyczne	2	ITT	K_W13, KW14, K_U11
17	Zarządzanie bezpieczeństwem informacji	3	ITT	K_W08, K_W14, K_U06, K_K05
18	Techniki dochodzeniowe i śledcze	2	ITT	K_W08, K_W14, K_U11, K_K05
19	Zarządzanie sieciami teleinformatycznymi	3	ITT	K_W08, K_W13, K_U10, K_K02, K_K05
20	Technologie Internetu rzeczy	2	ITT	K_W11, K_W13, K_U16, K_K03, K_K05
21	Studium ataków i incydentów	2	ITT	K_W08, K_W14, K_U11, K_K02, K_K05
22	Wirtualizacja systemów IT	2	ITT	K_W09, K_W12, K_U16, K_K01

23	Walka w cyberprzestrzeni	3	ITT	K_W08, K_W14, K_U11, K_K03, K_K05
24	Projekt z zakresu cyberobrony	4	ITT	K_W08, K_U05, K_U07
25	Systemy rozproszone	4	ITT	K_W05, K_W06, K_U05, K_U08, K_K04
26	Trends in computer technology	4	ITT	K_W16, K_W20, K_U13, K_U16, K_K01
27	Technologie mobilne	3	ITT	K_W02, K_W13, K_U05, K_K05
28	Projektowanie systemów bezpieczeństwa informacji	5	ITT	K_W08, K_W14, K_U07, K_K02, K_K05

Macierz pokrycia specjalistycznych efektów uczenia się: cyberobrona

	Cyberobrona																												
	Seci komputerowe II	JavaEE Technologies	HTML i aplikacje webowe	Systemy operacyjne UNI+	Ataki sieciowe	Oprogramowanie niepożądane i inspekcja	Eksploracja sieci teleinformatycznych	Systemy wbudowane	Bezpieczeństwo sieci bezprzewodowych	Modelowanie i analiza systemów teleinformatycznych	Systemy bezpieczeństwa sieciowego	Podstawy przetwarzania rozproszonego	Administrowanie środowiskiem Windows	Bezpieczeństwo sieci IPv6	Projektowanie i wytwarzanie systemów teleinformatycznych	Zabezpieczenia teleinformatyczne	Zarządzanie bezpieczeństwem informacji	Techniki dochodzeniowe i śledcze	Zarządzanie sieciami teleinformatycznymi	Technologie Internetu Rzeczy	Studium ataków i incydentów	Wirtualizacja systemów IT	Walka w cyberprzestrzeni	Projekt z zakrsu cyberobrony	Systemy rozproszone	Trends in computer technology	Technologie mobilne	Projektowanie syetmów bezpieczeństwa informacji
K_W01																													
K_W02																											+		
K_W03																													
K_W04																													
K_W05		+										+													+				
K_W06		+	+																						+				
K_W07																													
K_W08		+								+					+		+	+	+		+		+	+				+
K_W09																						+							
K_W10										+																			
K_W11																				+									
K_W12				+									+									+							
K_W13	+								+		+			+	+	+			+	+							+		
K_W14					+	+	+		+		+			+		+	+	+			+		+						+
K_W15																													
K_W16																										+			
K_W17																													
K_W18																													
K_W19								+																					
K_W20																										+			
K_W21																													
K_W22																													
K_W23																													
K_W24																													
K_U01																													
K_U02		+																											
K_U03																													
K_U04																													
K_U05		+	+							+		+			+									+	+		+		
K_U06																	+												
K_U07																								+					+
K_U08																									+				
K_U09				+									+																
K_U10	+														+					+									
K_U11					+	+	+		+		+			+		+		+			+		+						
K_U12																													
K_U13																										+			
K_U14								+																					
K_U15																													
K_U16																				+		+				+			
K_U17																													
K_U18										+																			
K_U19																													
K_U20																													
K_U21																													
K_K01										+												+				+			
K_K02																			+		+								+
K_K03																				+			+						
K_K04																									+				
K_K05														+			+	+	+	+	+		+				+	+	
K_K06																													

6. KALENDARZOWY PLAN JEDNOLITYCH STUDIÓW MAGISTERSKICH – EDYCJA OD ROKU 2025, PROFIL OGÓLNOAKADEMICKI



7. PLAN JEDNOLITYCH STUDIÓW MAGISTERSKICH

PLAN SPECJALNOŚCI „SYSTEMY KRYPTOGRAFICZNE”

Wojskowa Akademia Techniczna

PLAN JEDNOLITYCH STUDIÓWMAGISTERSKICH DLA KANDYDATÓWNA OFICERÓWO PROFILU OGÓLNOAKADEMICKIM / ~~PRAKTYCZNYM~~*
NABÓR WROKU AKADEMICKIM 2025

Kierunek studiów: **kryptologia i cyberbezpieczeństwo** | Dyscyplina naukowa: **informatyka techniczna i**

Specjalność wojskowa: **Systemy kryptograficzne (SW 29A)** | Korpus osobowy: **kryptologii i cyberbezpieczeństwa**

Indeks	GRUPY ZAJĘĆ / PRZEDMIOTY	ogółem liczba godzin/ pkt ECTS: razem	w tym w CS	ECTS	Dyscyplina naukowa	Liczba godzin kontaktowych	Liczba godzin niekontaktowych	Liczba godzin razem	ECTS kształt. umiejętności naukowe	Liczba ECTS z udziałem NA	Liczba ECTS bez udziału NA	Liczba ECTS razem	wykł.	ćwicz.		lab.		proj.		semin.		zajęcia online WCP/S**
A. Grupa zajęć bloku wojskowego		722		2		30	20	50	2	1,2	0,8	2	248	472						2		
		174		2		30	20	50	2	1,2	0,8	2	82	92								
A.I.1	Działalność wychowawcza i profilaktyka dyscyplinarna	30											10	20								
A.I.2	Podstawy komunikacji strategicznej - teoria i praktyka	30											10	20								
A.I.3	Przywództwo w dowodzeniu	30											10	20								
A.I.4	Historia sztuki wojennej	20											10	10								
A.I.5	Historia Polski	30		2	NS	30	20	50	2	1,2	0,8	2	16	14								
A.I.6	Ochrona informacji niejawnych	10											8	2								
A.I.7	Profilaktyka antykorupcyjna	8											8									
A.I.8	Bezpieczeństwo w cyberprzestrzeni	10											4	6								
A.I.9	Bezpieczeństwo i higiena pracy (BHP)	6											6									
		548											166	380						2		
A.II.1	Podstawy dowodzenia	24											10	14								
A.II.2	Taktyka	40											10	30								
A.II.3	Podstawy survivalu	22												22								
A.II.4	Gotowość mobilizacyjna I bojowa	16											10	6								
A.II.5	Rozpoznanie i armie innych państw	20											8	10						2		
A.II.6	Topografia wojskowa	40											10	30								
A.II.7	Zabezpieczenie logistyczne działań taktycznych	16											8	8								
A.II.8	Szkolenie strzeleckie	88											10	78								
A.II.9	Systemy łączności i środki dowodzenia	20											8	12								
A.II.10	Działalność szkoleniowa i szkoleniowo - metodyczna	40											16	24								
A.II.11	Międzynarodowe prawo humanitarne konfliktów zbrojnych (MPHKZ)	20											10	10								
A.II.12	Wybrane zagadnienia bezpieczeństwa narodowego i międzynarodowego	20											8	12								
A.II.13	Podstawy eksploatacji sprzętu wojskowego (SpW)	14											6	8								
A.II.14	Działania niekinetyczne	10											4	6								
A.II.15	Ochrona środowiska	8											4	4								
A.II.16	Obrona powietrzna	18											8	10								
A.II.17	Obrona przed bronią masowego rażenia	30											8	22								
A.II.18	Połączone wsparcie ogniowe	18											8	10								
A.II.19	Zabezpieczenie inżynieryjne	20											6	14								
A.II.20	Zabezpieczenie medyczne	30											8	22								
A.II.21	Regulaminy SZ RP	34											6	28								
B. Grupa zajęć bloku sportowo - językowego		1070		24		480	120	600		19,2	4,8	24	10	1060								
B.1.1	Język angielski	480		24		480	120	600		19,2	4,8	24		480								
B.1.2	Wychowanie fizyczne	560											10	550								
B.1.3	Obóz językowy - język angielski	30												30								
C. Grupa zajęć bloku kierunku politechnicznego		2740		231		2740	3082	5822	141	108,1	122,9	231	1268	462		914		96				do 75%
I. Grupa treści kształcenia ogólnego		92		7		92	89	181	4	3,5	3,5	7	52	18		22						do 75%
C.I.1	Wprowadzenie do studiowania	6		0,5	NS	6	8	14		0,2	0,3	0,5	6									do 75%
C.I.2	Ochrona własności intelektualnych	14		1	NP	14	13	27	0,5	0,5	0,5	1	12	2								do 75%
C.I.3	Wprowadzenie do informatyki	38		3	ITT	38	38	76	1,5	1,5	1,5	3	16			22	+					do 75%
C.I.4	Podstawy zarzadzania i przedsiebiorczości	34		2,5	NZJ	34	30	64	2	1,3	1,2	2,5	18	16	+							do 75%
II. Grupa treści kształcenia podstawowego		688		56,5		688	733	1421	40	27,3	29,2	56,5	342	280		66						do 75%
C.II.1	Wprowadzenie do metrologii	38		3	AEE	38	38	76	1	1,5	1,5	3	18	20	+							do 75%
C.II.2	Podstawy grafiki inżynierskiej	38		3	IM	38	38	76	2	1,5	1,5	3	14	24	+							do 75%
C.II.3	Matematyka 1	68		6	M	68	83	151	4	2,7	3,3	6	30	38	+							do 75%
C.II.4	Matematyka 2	68		6	M	68	83	151	4	2,7	3,3	6	34	34	+							do 75%
C.II.5	Matematyka dyskretna 1	30		2,5	M	30	33	63	2	1,2	1,3	2,5	16	14	+							do 75%
C.II.6	Analiza matematyczna	44		4	M	44	58	102	3,5	1,7	2,3	4	20	24	+							do 75%
C.II.7	Fizyka 1	80		6	NF	80	70	150	5	3,2	2,8	6	40	30	+	10	+					do 75%
C.II.8	Matematyka dyskretna 2	30		3	M	30	45	75	2,5	1,2	1,8	3	16	14	+							do 75%
C.II.9	Rachunek prawdopodobieństwa	32		3	M	32	45	77	2	1,2	1,8	3	18	4		10	+					do 75%
C.II.10	Teoretyczne podstawy informatyki	30		3	ITT	30	45	75	2	1,2	1,8	3	14	12	+	4						do 75%
C.II.11	Fizyka 2	60		4	NF	60	40	100	3	2,4	1,6	4	30	20	+	10	+					do 75%
C.II.12	Teoria grafów i sieci	30		2	ITT	30	20	50	1,5	1,2	0,8	2	16	14	+							do 75%
C.II.13	Podstawy optymalizacji	30		3	ITT	30	45	75	2,5	1,2	1,8	3	14	16	+							do 75%
C.II.14	Statystyka matematyczna	30		2	M	30	20	50	1	1,2	0,8	2	16			14	+					do 75%
C.II.15	Modelowanie matematyczne	30		3	ITT	30	45	75	2,5	1,2	1,8	3	14	16	+							do 75%
C.II.16	Bezpieczeństwo pracy i ergonomia	20		1	ITT	20	5	25	0,5	0,8	0,2	1	12			8	+					do 75%
C.II.17	Podstawy bezpieczeństwa informacji	30		2	ITT	30	20	50	1	1,2	0,8	2	20			10	+					do 75%
III. Grupa treści kształcenia kierunkowego		964		86,5		964	1213	2177	50,5	38	48,5	86,5	422	78		450		14				do 75%
C.III.1	Wprowadzenie do programowania	30		3	ITT	30	45	75	1,5	1,2	1,8	3	10			20	+					do 75%
C.III.2	Podstawy techniki komputerów	52		5	ITT	52	75	127	3,5	2	3	5	28	8		16	+					do 75%
C.III.3	Architektura i organizacja komputerów	52		5	ITT	52	75	127	3	2	3	5	20			32	+					do 75%
C.III.4	Podstawy podzespołów komputerów	30		2	ITT	30	20	50	1	1,2	0,8	2	14			16	+					do 75%
C.III.5	Algorytmy i struktury danych	40		4	ITT	40	60	100	2,5	1,6	2,4	4	18			22	+					do 75%
C.III.6	Teoria informacji i kodowania	40		3	ITT	40	35	75	2	1,6	1,4	3	18	10		12	+					do 75%
C.III.7	Programowanie niskopoziomowe i analiza kodu	30		2	ITT	30	20	50	1	1,2	0,8	2	14			16	+					do 75%
C.III.8	Programowanie obiektowe	52		3	ITT	52	25	77	1,5	2	1	3	20			32	+					do 75%
C.III.9	Bazy danych	52		3	ITT	52	25	77	2	2	1	3	14	12		26	+					do 75%
C.III.10	Zastosowanie kryptografii w systemach teleinformatycznych	30		3	ITT	30	45	75	1,5	1,2	1,8	3	10			20	+					do 75%
C.III.11	Systemy operacyjne	52		5	ITT	52	75	127	3	2	3	5	26			26	+					do 75%
C.III.12	Elementy teorii liczb	30		3	M	30	45	75	2,5	1,2	1,8	3	16	14	+							do 75%
C.III.13	Wybrane elementy kryptologii	52		4	M	52	50	102	2,5	2	2	4	20			32	+					do 75%
C.III.14	Interfejsy komputerów	40		3	ITT	40	35	75	2	1,6	1,4	3	16	4		20	+					do 75%
C.III.15	Zastosowania kryptografii w Internecie	30		3	ITT	30	45	75	1,5	1,2	1,8	3	14			16	+					do 75%
C.III.16	Inżynieria oprogramowania	40		4	ITT	40	60	100	2	1,6	2,4	4	12			28	+					do 75%
C.III.17	Sieci komputerowe	52		5,5	ITT	52	88	140	3,5	2	3,5	5,5	28			24	+					do 75%
C.III.18	Protokoły kryptograficzne	30		3	ITT	30	45	75	1,5	1,2	1,8	3	16			14	+					do 75%
C.III.19	Niezawodność systemów komputerowych	30		2	ITT	30	20	50	1,5	1,2	0,8	2	14	16	+							do 75%
C.III.20	Bezpieczeństwo baz danych	30		4	ITT	30	70	100	2	1,2	2,8	4	14			16	+					do 75%
C.III.21	Procesy stochastyczne	30		2	M	30	20	50	1,5	1,2	0,8	2	16	14	+							do 75%
C.III.22	Metody symulacji komputerowej	40		4	ITT	40	60	100	2	1,6	2,4	4	16			24	+					do 75%
C.III.23	Steganografia	30		3	ITT	30	45	75	1,5	1,2	1,8	3	16			14	+					do 75%
C.III.24	Diagnostyka i tolerowanie uszkodzeń	40		6	ITT	40	110	150	3	1,6	4,4	6	16			10	+	14				do 75%
C.III.25	Sztuczna inteligencja	30		2	ITT	30	20	50	1	1,2	0,8	2	16			14	+					do 75%
IV. Grupa treści kształcenia specjalistycznego		996		81		996	1047	2043	46,5	39,3	41,7	81	452	86		376		82				do 75%
C.IV.1	Metody statystyczne w kryptologii	30		4	M	30	70	100	2	1,2	2,8	4	10			20	+					do 75%
C.IV.2	Projekt zespołowy	44		4	ITT	44	58	102	0,5	1,7	2,3	4						44	+			do 75%
C.IV.3	Funkcje boolowskie w kryptologii	44		4	ITT	44	58	102	3,5	1,7	2,3	4	24	20	+							do 75%
C.IV.4	Projektowanie kryptograficznych układów cyfrowych	60		5	ITT	60	65	125	3	2,4	2,6	5	20			40	+					do 75%
C.IV.5	Struktury algebraiczne	44		4	M	44	58	102	2,5	1,7	2,3	4	20			24	+					do 75%
C.IV.6	Wstep do kryptoanalizy algorytmów klucza publicznego	30		2	ITT	30	20	50	1	1,2	0,8	2	14			16	+					do 75%
C.IV.7	Krzywe eliptyczne	30		2	M	30	20	50	1	1,2	0,8	2	16			14	+					do 75%
C.IV.8	Zastosowania teorii krat w kryptologii	44		3	ITT	44	33	77	1,5	1,7	1,3	3	20			24	+					do 75%
C.IV.9	Algorytmy blokowe	60		4	ITT	60	40	100	3	2,4	1,6	4	40	12	+	8						do 75%
C.IV.10	Algorytmy strumieniowe	44		3	ITT	44	33	77	2	1,7	1,3	3	24	6		14	+					do 75%
C.IV.11	Jednokierunkowe funkcje skrótu	30		2	ITT	30	20	50	1	1,2	0,8	2	10	10		10	+					do 75%
C.IV.12	Systemy zabezpieczeń pomieszczeń	30		2	ITT	30	20	50	1	1,2	0,8	2	10			20	+					do 75%
C.IV.13	Quantum and Post-Quantum Cryptology	44		3	ITT	44	33	77	2,5	1,7	1,3	3	30	14	+							do 75%
C.IV.14	Narzedzia kryptoanalizy	30		2	ITT	30	20	50	1	1,2	0,8	2	14			16	+					do 75%
C.IV.15	Generacja i testowanie losowości	44		3	ITT	44	33	77	2	1,7	1,3	3	20	10		14	+					do 75%
C.IV.16	Teoria ciał skończonych	30		2	M	30	20	50	1,5	1,2	0,8	2	20	10	+							do 75%
C.IV.17	Projekt z zakresu matematycznych i informatycznych podstaw kryptologii	30		2	ITT	30	20	50	0,5	1,2	0,8	2	2					28	+			do 75%
C.IV.18	Projektowanie kryptograficznych układow cyfrowych II	60		4	ITT	60	40	100	2,5	2,4	1,6	4	24			36	+					do 75%
C.IV.19	Akredytacja systemów teleinformatycznych	60		4	ITT	60	40	100	2	2,4	1,6	4	20			40	+					do 75%
C.IV.20	Elements of Public-Key Cryptology	30		2	ITT	30	20	50	1	1,2	0,8	2	20			10	+					do 75%
C.IV.21	Ataki algebraiczne	30		3	ITT	30	45	75	2	1,2	1,8	3	20			10	+					do 75%
C.IV.22	Kryptoanaliza algorytmów blokowych	30		3	ITT	30	45	75	2	1,2	1,8	3	20	4	+	6	+					do 75%
C.IV.23	Kryptoanaliza algorytmów strumieniowych	44		5	ITT	44	83	127	3	1,7	3,3	5	24			20	+					do 75%
C.IV.24	Metody numeryczne w kryptologii	44		5	M	44	83	127	3	1,7	3,3	5	20			24	+					do 75%
C.IV.25	Krzywe hipereliptyczne w kryptologii	30		4	ITT	30	70	100	1,5	1,2	2,8	4	10			10	+	10				do 75%
D. Praca dyplomowa /egz. na oficera		164		27		164	513	677	8,5	6,5	20,5	27						100		64		
D.I.1	Seminarium przeddyplomowe	20		1	ITT	20	5	25	0,5	0,8	0,2	1								20	+	do 75%
D.I.2	Seminarium dyplomowe	44		4	ITT	44	58	102	3,5	1,7	2,3	4								44	+	do 75%
D.I.3	Praca dyplomowa	100		22	ITT	100	450	550	4,5	4	18	22						100				
D.I.4	Egzamin na oficera																					
E. Praktyki zawodowe		400	400	16		400				16		16										
E.I.1	Praktyka d-cy drużyny	100	100	4		100				4		4										
E.I.2	Praktyka d-cy plutonu	100	100	4		100				4		4										
E.I.3	Praktyka zawodowa	100	100	4	ITT	100				4		4										
E.I.4	Szkolenie specjalistyczne	100	100	4	ITT	100				4		4										
F. Inne													termin realizacji									Uwagi
F.I.1																						
	ogółem godzin / pkt. ECTS	5096	400	300	X	3814	3735	7149	151,5	151	149	300	1526	1994		914		196		66		X
	dopuszczalny deficyt pkt. ECTS (w semestrze / łącznie)																					
	ogółem godzin realizowanych w Centrach Szkolenia	w tym w CS																				
	rodzaje i liczba rygorów w semestrze:																					

Jednolite studia magisterskie – liczba godzin/rygor/pkt ECTS w semestrze:

Indeks	I godz.	I ryg.	I ECTS	II godz.	II ryg.	II ECTS	III godz.	III ryg.	III ECTS	IV godz.	IV ryg.	IV ECTS	V godz.	V ryg.	V ECTS	VI godz.	VI ryg.	VI ECTS	VII godz.	VII ryg.	VII ECTS	VIII godz.	VIII ryg.	VIII ECTS	IX godz.	IX ryg.	IX ECTS	X godz.	X ryg.	X ECTS	Jednostka organizacyjna (instytut/katedra) odpowiedzialna za przedmiot	Uwagi
A. Grupa zajęć bloku wojskowego	146		2	134			72			84			60			72			76			78										
	46		2	20			36			32									10			30										
A.I.1				8	Z					12	Zo								10	Zo											WLO-IOZ	
A.I.2																						30	Zo								WLO-IOZ	
A.I.3				8	Z		22	E																							WLO-IOZ	
A.I.4										20	Zo																				WLO-IOZ	
A.I.5	30	E	2																												WLO-IOZ	
A.I.6				4	Z		6	Zo																							SSW	
A.I.7							8	Z																							WLO-IOZ	
A.I.8	10	Zo																													WCY	
A.I.9	6	Z																													Sekcja BHP	
	100			114			36			52			60			72			66			48										
A.II.1	12	Z		12	Zo																										SSW	
A.II.2	10	Z		10	Zo		8	Z		12	Zo																				SSW	
A.II.3										22	Zo																				SSW	
A.II.4				6	Z								10	Zo																	SSW	
A.II.5	8	Z		12	Zo																										SSW	
A.II.6	20	Zo																				20	Zo								WIG	
A.II.7				8	Z														8	Z											WLO	
A.II.8	14	Zo		16	Zo		8	Zo		10	Zo		8	Zo		10	Zo		12	Zo		10	Zo								SSW	
A.II.9				10	Zo		10	Zo																							WEL	
A.II.10	6	Zo		10	Zo								14	Zo		10	Zo														WLO-IOZ/SSW	
A.II.11																			20	E											WLO-IOZ	
A.II.12																			20	Zo											WLO-IBO	
A.II.13																14	Zo														WML	
A.II.14																						10	Z								WLO	
A.II.15													8	Z																	WIG	
A.II.16	10	Zo								8	Zo																				SSW	
A.II.17	10	Zo														20	Zo														WTC	
A.II.18																18	Zo														WML	
A.II.19				10	Zo		10	Zo																							SSW	
A.II.20				10	Zo								20	E																	SSW	
A.II.21	10	Zo		10	Zo														6	Z		8	Zo								SSW	
B. Grupa zajęć bloku sportowo - językowego	120		3	120		3	120		3	150		3	120		3	120		3	130		3	120		3	60			10				
B.1.1	60	Zo	3	60	Zo	3	60	Zo	3	60	Zo	3	60	Zo	3	60	E	3	60	Zo	3	60	Zo	3							SJO	
B.1.2	60	Zo		60	Zo		60	Zo		60	Zo		60	Zo		60	Zo		70	Zo		60	Zo		60	Zo		10	E		SWF	
B.1.3										30	Z																				SJO	
C. Grupa zajęć bloku kierunku politechnicznego	300		25	298		27	342		27	296		23	308		27	252		23	372		27	324		23	248		29					
I. Grupa treści kształcenia ogólnego	58		4,5										34		2,5																	
C.I.1	6	+	0,5																												PJ	(*)
C.I.2	14	+	1																												WLO-IOZ	(*)
C.I.3	38	+	3																												WCY-ISI	(*)
C.I.4													34	+	2,5																WLO-IOZ	(*)
II. Grupa treści kształcenia podstawowego	242		20,5	216		19	150		11	50		4	30		2																	
C.II.1	38	+	3																												WEL/WTC	(*)
C.II.2	38	+	3																												WIM	(*)
C.II.3	68	x	6																												WCY-IMK	(*)
C.II.4	68	x	6																												WCY-IMK	(*)
C.II.5	30	+	2,5																												WCY-IMK	(*)
C.II.6				44	x	4																									WCY-IMK	(*)
C.II.7				80	x	6																									WTC	(*)
C.II.8				30	x	3																									WCY-IMK	(*)
C.II.9				32	+	3																									WCY-IMK	(*)
C.II.10				30	+	3																									WCY-ISI	(*)
C.II.11							60	x	4																						WTC	(*)
C.II.12							30	+	2																						WCY-ISI	(*)
C.II.13							30	+	3																						WCY-ISI	(*)
C.II.14							30	+	2																						WCY-IMK	(*)
C.II.15										30	+	3																			WCY-ISI	(*)
C.II.16										20	+	1																			WCY-ITC	(*)
C.II.17													30	+	2																WCY-ISI	(*)
III. Grupa treści kształcenia kierunkowego				82		8	192		16	246		19	244		22,5	30		2	60		6	40		4	70		9					
C.III.1				30	x	3																									WCY-ISI	(*)
C.III.2				52	+	5																									WCY-ITC	(*)
C.III.3							52	x	5																						WCY-ITC	(*)
C.III.4							30	+	2																						WCY-ISI	(*)
C.III.5							40	x	4																						WCY-ISI	(*)
C.III.6							40	+	3																						WCY-ITC	(*)
C.III.7							30	+	2																						WCY-ITC	(*)
C.III.8										52	+	3																			WCY-ISI	(*)
C.III.9										52	x	3																			WCY-ISI	(*)
C.III.10										30	x	3																			WCY-IMK	(*)
C.III.11										52	x	5																			WCY-ITC	(*)
C.III.12										30	+	3																			WCY-IMK	(*)
C.III.13													52	x	4																WCY-IMK	(*)
C.III.14													40	+	3																WCY-ITC	(*)
C.III.15													30	+	3																WCY-IMK	(*)
C.III.16													40	x	4																WCY-ISI	(*)
C.III.17													52	x	5,5																WCY-ITC	(*)
C.III.18													30	+	3																WCY-IMK	(*)
C.III.19																30	+	2													WCY-ISI	(*)
C.III.20																			30	+	4										WCY-ISI	(*)
C.III.21																			30	+	2										WCY-IMK	(*)
C.III.22																						40	x	4							WCY-ISI	(*)
C.III.23																									30	+	3				WCY-IMK	(*)
C.III.24																									40	x	6				WCY-ISI	(*)
C.III.25										30	+	2																			WCY-ISI	(*)
IV. Grupa treści kształcenia specjalistycznego																222		21	312		21	284		19	178		20					
C.IV.1																30	+	4													WCY-IMK	(*)
C.IV.2																44	+	4													WCY-IMK	(*)
C.IV.3																44	x	4													WCY-IMK	(*)
C.IV.4																60	x	5													WCY-IMK	(*)
C.IV.5																44	x	4													WCY-IMK	(*)
C.IV.6																			30	+	2										WCY-IMK	(*)
C.IV.7																			30	+	2										WCY-IMK	(*)
C.IV.8																			44	+	3										WCY-IMK	(*)
C.IV.9																			60	x	4										WCY-IMK	(*)
C.IV.10																			44	x	3										WCY-IMK	(*)
C.IV.11																			30	+	2										WCY-IMK	(*)
C.IV.12																			30	+	2										WCY-IMK	(*)
C.IV.13																			44	x	3										WCY-IMK	(*), w jęz. ang.
C.IV.14																						30	+	2							WCY-IMK	(*)
C.IV.15																						44	+	3							WCY-IMK	(*)
C.IV.16																						30	+	2							WCY-IMK	(*)
C.IV.17																						30	+	2							WCY-IMK	(*)
C.IV.18																						60	+	4							WCY-IMK	(*)
C.IV.19																						60	x	4							WCY-IMK	(*)
C.IV.20																						30	x	2							WCY-IMK	(*), w jęz. ang.
C.IV.21																									30	+	3				WCY-IMK	(*)
C.IV.22																									30	+	3				WCY-IMK	(*)
C.IV.23																									44	+	5				WCY-IMK	(*)
C.IV.24																									44	x	5				WCY-IMK	(*)
C.IV.25																									30	+	4				WCY-IMK	(*)
D. Praca dyplomowa /egz. na oficera																									20		1	144		26		
D.I.1																									20	+	1				WCY	(*)
D.I.2																												44	+	4	WCY	(*)
D.I.3																												100	x	22	WCY	
D.I.4																													E		SSW	
E. Praktyki zawodowe										100		4				100		4				100		4				100		4		
E.I.1										100	+	4																			CS/JW	
E.I.2																												100	+	4	CS/JW	
E.I.3																100	+	4													CS/JW	
E.I.4																						100	+	4							CS/JW	
ogółem godzin / pkt. ECTS	566		30	552		30	534		30	630		30	488		30	544		30	578		30	622		30	328		30	254		30		
dopuszczalny deficyt pkt. ECTS (w semestrze / łącznie)	15/15			18/18			15/25			15/25			15/25			15/25			15/25			15/25			15/25			15/25				

rodzaje i liczba rygorów w semestrze:	I	II	III	IV	V	VI	VII	VIII	IX	X
egzaminy (E, x)	3	4	4	3	4	4	4	3	2	2
zaliczenia z oceną (Zo, +)	15	14	12	13	10	9	12	11	7	1
zaliczenia bez oceny (Z, z)	6	10	4	2	2		4	2		
projekty przejściowe (P)										

* niepotrzebne skreślić, a arkusz dostosować pod względem programu dla profilu studiów.
** W - wykład, C - ćwiczenia, P - projekt, S - seminarium.

Obowiązuje kandydatówna żołnierzy zawodowych rozpoczynających kształcenie od roku akademickiego 2025/2026

Senat WAT
Plan studiów uchwalony przez .... w dniu ....
25 września 2025 r.

....

PLAN SPECJALNOŚCI „BEZPIECZEŃSTWO INFORMACYJNE”

Wojskowa Akademia Techniczna

PLAN JEDNOLITYCH STUDIÓW MAGISTERSKICH DLA KANDYDATÓW NA OFICERÓW O PROFILU OGÓLNOAKADEMICKIM / ~~PRAKTYCZNYM~~*
NABÓR W ROKU AKADEMICKIM 2025

Kierunek studiów: **kryptologia i cyberbezpieczeństwo** | Dyscyplina naukowa: **informatyka techniczna i**
Specjalność: **Bezpieczeństwo informacyjne (SW29B)** | Korpus osobowy: **kryptologii i cyberbezpieczeństwa**

Indeks	GRUPY ZAJĘĆ / PRZEDMIOTY	ogółem liczba godzin/ pkt ECTS: razem	w tym w CS	ECTS	Dyscyplina naukowa	Liczba godzin kontaktowych	Liczba godzin niekontaktowych	Liczba godzin razem	ECTS kształt. umiejętności naukowe	Liczba ECTS z udziałem NA	Liczba ECTS bez udziału NA	Liczba ECTS razem	Liczba godzin według formy zajęć: wykł.	ćwicz.	lab.	proj.	semin.	zajęcia online WCP/S**	Jednostka organizacyjna (instytut/katedra) odpowiedzialna za przedmiot	Uwagi
	A. Grupa zajęć bloku wojskowego	722		2		30	20	50	2	1,2	0,8	2	248	472			2			
		174		2		30	20	50	2	1,2	0,8	2	82	92						
A.I.1	Działalność wychowawcza i profilaktyka dyscyplinarna	30											10	20					WLO-IOZ	
A.I.2	Podstawy komunikacji strategicznej - teoria i praktyka	30											10	20					WLO-IOZ	
A.I.3	Przywództwo w dowodzeniu	30											10	20					WLO-IOZ	
A.I.4	Historia sztuki wojennej	20											10	10					WLO-IOZ	
A.I.5	Historia Polski	30		2	NS	30	20	50	2	1,2	0,8	2	16	14					WLO-IOZ	
A.I.6	Ochrona informacji niejawnych	10											8	2					SSW	
A.I.7	Profilaktyka antykorupcyjna	8											8						WLO-IOZ	
A.I.8	Bezpieczeństwo w cyberprzestrzeni	10											4	6					WCY	
A.I.9	Bezpieczeństwo i higiena pracy (BHP)	6											6						Sekcja BHP	
		548											166	380			2			
A.II.1	Podstawy dowodzenia	24											10	14					SSW	
A.II.2	Taktyka	40											10	30					SSW	
A.II.3	Podstawy survivalu	22												22					SSW	
A.II.4	Gotowość mobilizacyjna i bojowa	16											10	6					SSW	
A.II.5	Rozpoznanie i armie innych państw	20											8	10			2		SSW	
A.II.6	Topografia wojskowa	40											10	30					WIG	
A.II.7	Zabezpieczenie logistyczne działań taktycznych	16											8	8					WLO	
A.II.8	Szkolenie strzeleckie	88											10	78					SSW	
A.II.9	Systemy łączności i środki dowodzenia	20											8	12					WEL	
A.II.10	Działalność szkoleniowa i szkoleniowo - metodyczna	40											16	24					WLO-IOZ/SSW	
A.II.11	Międzynarodowe prawo humanitarne konfliktów zbrojnych (MPHKZ)	20											10	10					WLO-IOZ	
A.II.12	Wybrane zagadnienia bezpieczeństwa narodowego i międzynarodowego	20											8	12					WLO-IBO	
A.II.13	Podstawy eksploatacji sprzętu wojskowego (SpW)	14											6	8					WML	
A.II.14	Działania niekinetyczne	10											4	6					WLO	
A.II.15	Ochrona środowiska	8											4	4					WIG	
A.II.16	Obrona powietrzna	18											8	10					SSW	
A.II.17	Obrona przed bronią masowego rażenia	30											8	22					WTC	
A.II.18	Połączone wsparcie ogniowe	18											8	10					WML	
A.II.19	Zabezpieczenie inżynieryjne	20											6	14					SSW	
A.II.20	Zabezpieczenie medyczne	30											8	22					SSW	
A.II.21	Regulaminy SZ RP	34											6	28					SSW	
	B. Grupa zajęć bloku sportowo - językowego	1070		24		480	120	600		19,2	4,8	24	10	1060						
B.I.1	Język angielski	480		24		480	120	600		19,2	4,8	24		480					SJO	
B.I.2	Wychowanie fizyczne	560											10	550					SWF	
B.I.3	Obóz językowy - język angielski	30												30					SJO	
	C. Grupa zajęć bloku kierunku politechnicznego	2714		231		2714	3100	5814	133,5	107,3	123,7	231	1206	392	992	124		do 75%		
	I. Grupa treści kształcenia ogólnego	92		7		92	89	181	4	3,5	3,5	7	52	18	22			do 75%		
C.I.1	Wprowadzenie do studiowania	6		0,5	NS	6	8	14		0,2	0,3	0,5	6					do 75%	PJ	(*)
C.I.2	Ochrona własności intelektualnych	14		1	NP	14	13	27	0,5	0,5	0,5	1	12	2				do 75%	WLO-IOZ	(*)
C.I.3	Wprowadzenie do informatyki	38		3	ITT	38	38	76	1,5	1,5	1,5	3	16		22 +			do 75%	WCY-ISI	(*)
C.I.4	Podstawy zarządzania i przedsiębiorczości	34		2,5	NZJ	34	30	64	2	1,3	1,2	2,5	18	16 +				do 75%	WLO-IOZ	(*)
	II. Grupa treści kształcenia podstawowego	688		56,5		688	733	1421	40	27,3	29,2	56,5	342	280	66			do 75%		
C.II.1	Wprowadzenie do metrologii	38		3	AEE	38	38	76	1	1,5	1,5	3	18	20 +				do 75%	WEL/WTC	(*)
C.II.2	Podstawy grafiki inżynierskiej	38		3	IM	38	38	76	2	1,5	1,5	3	14	24 +				do 75%	WIM	(*)
C.II.3	Matematyka 1	68		6	M	68	83	151	4	2,7	3,3	6	30	38 +				do 75%	WCY-IMK	(*)
C.II.4	Matematyka 2	68		6	M	68	83	151	4	2,7	3,3	6	34	34 +				do 75%	WCY-IMK	(*)
C.II.5	Matematyka dyskretna 1	30		2,5	M	30	33	63	2	1,2	1,3	2,5	16	14 +				do 75%	WCY-IMK	(*)
C.II.6	Analiza matematyczna	44		4	M	44	58	102	3,5	1,7	2,3	4	20	24 +				do 75%	WCY-IMK	(*)
C.II.7	Fizyka 1	80		6	NF	80	70	150	5	3,2	2,8	6	40	30 +	10 +			do 75%	WTC	(*)
C.II.8	Matematyka dyskretna 2	30		3	M	30	45	75	2,5	1,2	1,8	3	16	14 +				do 75%	WCY-IMK	(*)
C.II.9	Rachunek prawdopodobieństwa	32		3	M	32	45	77	2	1,2	1,8	3	18	4	10 +			do 75%	WCY-IMK	(*)
C.II.10	Teoretyczne podstawy informatyki	30		3	ITT	30	45	75	2	1,2	1,8	3	14	12 +	4			do 75%	WCY-ISI	(*)
C.II.11	Fizyka 2	60		4	NF	60	40	100	3	2,4	1,6	4	30	20 +	10 +			do 75%	WTC	(*)
C.II.12	Teoria grafów i sieci	30		2	ITT	30	20	50	1,5	1,2	0,8	2	16	14 +				do 75%	WCY-ISI	(*)
C.II.13	Podstawy optymalizacji	30		3	ITT	30	45	75	2,5	1,2	1,8	3	14	16 +				do 75%	WCY-ISI	(*)
C.II.14	Statystyka matematyczna	30		2	M	30	20	50	1	1,2	0,8	2	16		14 +			do 75%	WCY-IMK	(*)
C.II.15	Modelowanie matematyczne	30		3	ITT	30	45	75	2,5	1,2	1,8	3	14	16 +				do 75%	WCY-ISI	(*)
C.II.16	Bezpieczeństwo pracy i ergonomia	20		1	ITT	20	5	25	0,5	0,8	0,2	1	12		8 +			do 75%	WCY-ITC	(*)
C.II.17	Podstawy bezpieczeństwa informacji	30		2	ITT	30	20	50	1	1,2	0,8	2	20		10 +			do 75%	WCY-ISI	(*)
	III. Grupa treści kształcenia kierunkowego	964		86,5		964	1213	2177	50,5	38	48,5	86,5	422	78	450	14		do 75%		
C.III.1	Wprowadzenie do programowania	30		3	ITT	30	45	75	1,5	1,2	1,8	3	10		20 +			do 75%	WCY-ISI	(*)
C.III.2	Podstawy techniki komputerów	52		5	ITT	52	75	127	3,5	2	3	5	28	8	16 +			do 75%	WCY-ITC	(*)
C.III.3	Architektura i organizacja komputerów	52		5	ITT	52	75	127	3	2	3	5	20		32 +			do 75%	WCY-ITC	(*)
C.III.4	Podstawy podzespołów komputerów	30		2	ITT	30	20	50	1	1,2	0,8	2	14		16 +			do 75%	WCY-ISI	(*)
C.III.5	Algorytmy i struktury danych	40		4	ITT	40	60	100	2,5	1,6	2,4	4	18		22 +			do 75%	WCY-ISI	(*)
C.III.6	Teoria informacji i kodowania	40		3	ITT	40	35	75	2	1,6	1,4	3	18	10	12 +			do 75%	WCY-ITC	(*)
C.III.7	Programowanie niskopoziomowe i analiza kodu	30		2	ITT	30	20	50	1	1,2	0,8	2	14		16 +			do 75%	WCY-ITC	(*)
C.III.8	Programowanie obiektowe	52		3	ITT	52	25	77	1,5	2	1	3	20		32 +			do 75%	WCY-ISI	(*)
C.III.9	Bazy danych	52		3	ITT	52	25	77	2	2	1	3	14	12	26 +			do 75%	WCY-ISI	(*)
C.III.10	Zastosowanie kryptografii w systemach teleinformatycznych	30		3	ITT	30	45	75	1,5	1,2	1,8	3	10		20 +			do 75%	WCY-IMK	(*)
C.III.11	Systemy operacyjne	52		5	ITT	52	75	127	3	2	3	5	26		26 +			do 75%	WCY-ITC	(*)
C.III.12	Elementy teorii liczb	30		3	M	30	45	75	2,5	1,2	1,8	3	16	14 +				do 75%	WCY-IMK	(*)
C.III.13	Wybrane elementy kryptologii	52		4	M	52	50	102	2,5	2	2	4	20		32 +			do 75%	WCY-IMK	(*)
C.III.14	Interfejsy komputerów	40		3	ITT	40	35	75	2	1,6	1,4	3	16	4	20 +			do 75%	WCY-ITC	(*)
C.III.15	Zastosowania kryptografii w Internecie	30		3	ITT	30	45	75	1,5	1,2	1,8	3	14		16 +			do 75%	WCY-IMK	(*)
C.III.16	Inżynieria oprogramowania	40		4	ITT	40	60	100	2	1,6	2,4	4	12		28 +			do 75%	WCY-ISI	(*)
C.III.17	Sieci komputerowe	52		5,5	ITT	52	88	140	3,5	2	3,5	5,5	28		24 +			do 75%	WCY-ITC	(*)
C.III.18	Protokoły kryptograficzne	30		3	ITT	30	45	75	1,5	1,2	1,8	3	16		14 +			do 75%	WCY-IMK	(*)
C.III.19	Niezawodność systemów komputerowych	30		2	ITT	30	20	50	1,5	1,2	0,8	2	14	16 +				do 75%	WCY-ISI	(*)
C.III.20	Bezpieczeństwo baz danych	30		4	ITT	30	70	100	2	1,2	2,8	4	14		16 +			do 75%	WCY-ISI	(*)
C.III.21	Procesy stochastyczne	30		2	M	30	20	50	1,5	1,2	0,8	2	16	14 +				do 75%	WCY-IMK	(*)
C.III.22	Metody symulacji komputerowej	40		4	ITT	40	60	100	2	1,6	2,4	4	16		24 +			do 75%	WCY-ISI	(*)
C.III.23	Steganografia	30		3	ITT	30	45	75	1,5	1,2	1,8	3	16		14 +			do 75%	WCY-IMK	(*)
C.III.24	Diagnostyka i tolerowanie uszkodzeń	40		6	ITT	40	110	150	3	1,6	4,4	6	16		10 +	14		do 75%	WCY-ISI	(*)
C.III.25	Sztuczna inteligencja	30		2	ITT	30	20	50	1	1,2	0,8	2	16		14 +			do 75%	WCY-ISI	(*)
	IV. Grupa treści kształcenia specjalistycznego	970		81		970	1065	2035	39	38,5	42,5	81	390	16	454	110		do 75%		
C.IV.1	Hurtownie danych	30		2	ITT	30	20	50	1	1,2	0,8	2	14		16 +			do 75%	WCY-ISI	(*)
C.IV.2	Metody prognozowania	30		3	M	30	45	75	1,5	1,2	1,8	3	14		16 +			do 75%	WCY-ISI	(*)
C.IV.3	Programowanie w językach funkcyjnych	30		3	ITT	30	45	75	1,5	1,2	1,8	3	14		16 +			do 75%	WCY-ISI	(*)
C.IV.4	Metody numeryczne	30		2	ITT	30	20	50	1	1,2	0,8	2	10		20 +			do 75%	WCY-ISI	(*)
C.IV.5	Automaty i języki formalne	30		3	ITT	30	45	75	1,5	1,2	1,8	3	12		18 +			do 75%	WCY-ISI	(*)
C.IV.6	Analiza i wizualizacja danych	30		3	ITT	30	45	75	1,5	1,2	1,8	3	14		16 +			do 75%	WCY-ISI	(*)
C.IV.7	Techniki algorytmiczne	30		3	ITT	30	45	75	1,5	1,2	1,8	3	14		4	12 +		do 75%	WCY-ISI	(*)
C.IV.8	Bussines modeling in UML	30		2	ITT	30	20	50	1	1,2	0,8	2	10		20 +			do 75%	WCY-ISI	(*), w jęz.ang.
C.IV.9	Modelowanie i symulacja procesów biznesowych	30		2	ITT	30	20	50	1	1,2	0,8	2	14		16 +			do 75%	WCY-ISI	(*)
C.IV.10	Metody uczenia maszynowego	30		3	ITT	30	45	75	1,5	1,2	1,8	3	14		16 +			do 75%	WCY-ISI	(*)
C.IV.11	Metody projektowania i wdrażania systemów informatycznych	60		4	ITT	60	40	100	2,5	2,4	1,6	4	30		18 +	12 +		do 75%	WCY-ISI	(*)
C.IV.12	Metody eksploracji danych	30		3	ITT	30	45	75	1,5	1,2	1,8	3	12		18 +			do 75%	WCY-ISI	(*)
C.IV.13	Technologie usługowe i mobilne	30		2	ITT	30	20	50	0,5	1,2	0,8	2	10		10 +	10 +		do 75%	WCY-ISI	(*)
C.IV.14	Metody sztucznej inteligencji	30		2	ITT	30	20	50	1	1,2	0,8	2	16		14 +			do 75%	WCY-ISI	(*)
C.IV.15	Metody ilościowe analizy ryzyka	30		2	ITT	30	20	50	1	1,2	0,8	2	10	6 +	14 +			do 75%	WCY-ISI	(*)
C.IV.16	Bazy danych NoSQL	30		3	ITT	30	45	75	1	1,2	1,8	3	6		24 +			do 75%	WCY-ISI	(*)
C.IV.17	Bezpieczeństwo systemów informacyjnych	30		3	ITT	30	45	75	1,5	1,2	1,8	3	16		14 +			do 75%	WCY-ISI	(*)
C.IV.18	Metody i systemy wspomagania decyzji	30		3	ITT	30	45	75	1,5	1,2	1,8	3	14		8 +	8 +		do 75%	WCY-ISI	(*)
C.IV.19	Podstawy kryptologii współczesnej	30		2	ITT	30	20	50	1	1,2	0,8	2	14		16 +			do 75%	WCY-IMK	(*)
C.IV.20	Modelowanie i analiza sieci złożonych	44		3	ITT	44	33	77	2	1,7	1,3	3	18	10 +	16 +			do 75%	WCY-ISI	(*)
C.IV.21	Rozproszone przetwarzanie danych	44		3	ITT	44	33	77	1,5	1,7	1,3	3	14		30 +			do 75%	WCY-ISI	(*)
C.IV.22	Zarządzanie projektami	30		3	ITT	30	45	75	1,5	1,2	1,8	3	16		14 +			do 75%	WCY-ISI	(*)
C.IV.23	Ilościowe metody oceny bezpieczeństwa systemów teleinformatycznych	30		2	ITT	30	20	50	1	1,2	0,8	2	14		16 +			do 75%	WCY-ISI	(*)
C.IV.24	Zaawansowane metody uczenia maszynowego	30		3	ITT	30	45	75	1,5	1,2	1,8	3	10		20 +			do 75%	WCY-ISI	(*)
C.IV.25	Teoria wojny informacyjnej	30		2	ITT	30	20	50	1	1,2	0,8	2	16		14 +			do 75%	WCY-ISI	(*)
C.IV.26	Technologie Internetu rzeczy	44		4	ITT	44	58	102	2,5	1,7	2,3	4	20		24 +			do 75%	WCY-ISI	(*)
C.IV.27	Przetwarzanie języka naturalnego (NLP)	30		3	ITT	30	45	75	1,5	1,2	1,8	3	12		18 +			do 75%	WCY-ISI	(*)
C.IV.28	Projekt z zakresu bezpieczeństwa informacji	44		4	ITT	44	58	102	0,5	1,7	2,3	4				44 +		do 75%	WCY-ISI	(*)
C.IV.29	Zarządzanie wiedzą	44		4	ITT	44	58	102	1,5	1,7	2,3	4	12		8 +	24 +		do 75%	WCY-ISI	(*)
	D. Praca dyplomowa / egz. na oficera	164		27		164	513	677	8,5	6,5	20,5	27				100	64			
D.I.1	Seminarium przeddyplomowe	20		1	ITT	20	5	25	0,5	0,8	0,2	1					20 +	do 75%	WCY	(*)
D.I.2	Seminarium dyplomowe	44		4	ITT	44	58	102	3,5	1,7	2,3	4					44 +	do 75%	WCY	(*)
D.I.3	Praca dyplomowa	100		22	ITT	100	450	550	4,5	4	18	22				100			WCY	
D.I.4	Egzamin na oficera																		SSW	
	E. Praktyki zawodowe	400	400	16		400				16		16								
E.I.1	Praktyka d-cy drużyny	100	100	4		100				4		4							CS /JW	
E.I.2	Praktyka d-cy plutonu	100	100	4		100				4		4							CS /JW	
E.I.3	Praktyka zawodowa	100	100	4	ITT	100				4		4							CS /JW	
E.I.4	Szkolenie specjalistyczne	100	100	4	ITT	100				4		4							CS /JW	
	F. Inne												termin realizacji							
F.I.1																				
	ogółem godzin / pkt. ECTS	5070	400	300	X	3788	3753	7141	144	150,2	149,8	300	1464	1924	992	224	66	X		
	dopuszczalny deficyt pkt. ECTS (w semestrze / łącznie)																			
	ogółem godzin realizowanych w Centrach Szkolenia	w tym w CS																		

Jednolite studia magisterskie – liczba godzin/rygor/pkt ECTS w semestrze:

Indeks	I godz.	I f/z	I ECTS	II godz.	II f/z	II ECTS	III godz.	III f/z	III ECTS	IV godz.	IV f/z	IV ECTS	V godz.	V f/z	V ECTS	VI godz.	VI f/z	VI ECTS	VII godz.	VII f/z	VII ECTS	VIII godz.	VIII f/z	VIII ECTS	IX godz.	IX f/z	IX ECTS	X godz.	X f/z	X ECTS
A. Grupa zajęć bloku wojskowego	146		2	134			72			84			60			72			76			78								
(A.I)	46		2	20			36			32									10			30								
A.I.1				8	Z					12	Zo								10	Zo										
A.I.2																						30	Zo							
A.I.3				8	Z		22	E																						
A.I.4										20	Zo																			
A.I.5	30	E	2																											
A.I.6				4	Z		6	Zo																						
A.I.7							8	Z																						
A.I.8	10	Zo																												
A.I.9	6	Z																												
(A.II)	100			114			36			52			60			72			66			48								
A.II.1	12	Z		12	Zo																									
A.II.2	10	Z		10	Zo		8	Z		12	Zo																			
A.II.3										22	Zo																			
A.II.4				6	Z								10	Zo																
A.II.5	8	Z		12	Zo																									
A.II.6	20	Zo																				20	Zo							
A.II.7				8	Z														8	Z										
A.II.8	14	Zo		16	Zo		8	Zo		10	Zo		8	Zo		10	Zo		12	Zo		10	Zo							
A.II.9				10	Zo		10	Zo																						
A.II.10	6	Zo		10	Zo								14	Zo		10	Zo													
A.II.11																			20	E										
A.II.12																			20	Zo										
A.II.13																14	Zo													
A.II.14																						10	Z							
A.II.15													8	Z																
A.II.16	10	Zo								8	Zo																			
A.II.17	10	Zo														20	Zo													
A.II.18																18	Zo													
A.II.19				10	Zo		10	Zo																						
A.II.20				10	Zo								20	E																
A.II.21	10	Zo		10	Zo														6	Z		8	Zo							
B. Grupa zajęć bloku sportowo - językowego	120		3	120		3	120		3	150		3	120		3	120		3	130		3	120		3	60			10		
B.I.1	60	Zo	3	60	Zo	3	60	Zo	3	60	Zo	3	60	Zo	3	60	E	3	60	Zo	3	60	Zo	3						
B.I.2	60	Zo		60	Zo		60	Zo		60	Zo		60	Zo		60	Zo		70	Zo		60	Zo		60	Zo		10	E	
B.I.3										30	Z																			
C. Grupa zajęć bloku kierunku politechnicznego	300		25	298		27	342		27	296		23	308		27	270		23	330		27	278		23	292		29			
I. Grupa treści kształcenia ogólnego	58		4,5										34		2,5															
C.I.1	6	+	0,5																											
C.I.2	14	+	1																											
C.I.3	38	+	3																											
C.I.4													34	+	2,5															
II. Grupa treści kształcenia podstawowego	242		20,5	216		19	150		11	50		4	30		2															
C.II.1	38	+	3																											
C.II.2	38	+	3																											
C.II.3	68	x	6																											
C.II.4	68	x	6																											
C.II.5	30	+	2,5																											
C.II.6				44	x	4																								
C.II.7				80	x	6																								
C.II.8				30	x	3																								
C.II.9				32	+	3																								
C.II.10				30	+	3																								
C.II.11							60	x	4																					
C.II.12							30	+	2																					
C.II.13							30	+	3																					
C.II.14							30	+	2																					
C.II.15										30	+	3																		
C.II.16										20	+	1																		
C.II.17													30	+	2															
III. Grupa treści kształcenia kierunkowego				82		8	192		16	246		19	244		22,5	30		2	60		6	40		4	70		9			
C.III.1				30	x	3																								
C.III.2				52	+	5																								
C.III.3							52	x	5																					
C.III.4							30	+	2																					
C.III.5							40	x	4																					
C.III.6							40	+	3																					
C.III.7							30	+	2																					
C.III.8										52	+	3																		
C.III.9										52	x	3																		
C.III.10										30	x	3																		
C.III.11										52	x	5																		
C.III.12										30	+	3																		
C.III.13													52	x	4															
C.III.14													40	+	3															
C.III.15													30	+	3															
C.III.16													40	x	4															
C.III.17													52	x	5,5															
C.III.18													30	+	3															
C.III.19																30	+	2												
C.III.20																			30	+	4									
C.III.21																			30	+	2									
C.III.22																						40	x	4						
C.III.23																									30	+	3			
C.III.24																									40	x	6			
C.III.25										30	+	2																		
IV. Grupa treści kształcenia specjalistycznego																240		21	270		21	238		19	222		20			
C.IV.1																30	+	2												
C.IV.2																30	+	3												
C.IV.3																30	+	3												
C.IV.4																30	+	2												
C.IV.5																30	x	3												
C.IV.6																30	+	3												
C.IV.7																30	x	3												
C.IV.8																30	+	2												
C.IV.9																			30	+	2									
C.IV.10																			30	+	3									
C.IV.11																			60	x	4									
C.IV.12																			30	x	3									
C.IV.13																			30	+	2									
C.IV.14																			30	+	2									
C.IV.15																			30	+	2									
C.IV.16																			30	+	3									
C.IV.17																						30	+	3						
C.IV.18																						30	+	3						
C.IV.19																						30	+	2						
C.IV.20																						44	x	3						
C.IV.21																						44	+	3						
C.IV.22																						30	+	3						
C.IV.23																						30	+	2						
C.IV.24																									30	x	3			
C.IV.25																									30	+	2			
C.IV.26																									44	x	4			
C.IV.27																									30	+	3			
C.IV.28																									44	+	4			
C.IV.29																									44	+	4			
D. Praca dyplomowa / egz. na oficera																									20		1	144		26
D.I.1																									20	+	1			
D.I.2																												44	+	4
D.I.3																												100	x	22
D.I.4																													E	
E. Praktyki zawodowe										100		4				100		4				100		4				100		4
E.I.1										100	+	4																		
E.I.2																												100	+	4
E.I.3																100	+	4												
E.I.4																						100	+	4						
F. Inne (Uwagi)																														
ogółem godzin / pkt. ECTS	566		30	552		30	534		30	630		30	488		30	562		30	536		30	576		30	372		30	254		30
dopuszczalny deficyt pkt. ECTS (w semestrze / łącznie)	15/15			18/18			15/25			15/25			15/25			15/25			15/25			15/25			15/25			15/25		
rodzaje i liczba rygorów w semestrze: egzaminy (E, x)	3			4			4			3			4			3			3			2			3			2		
zaliczenia z oceną (Zo, +)	15			14			12			13			10			13			13			12			7			1		
zaliczenia bez oceny (Z, z)	6			10			4			2			2						4			2								
projekty przejściowe (P)																														

* niepotrzebne skreślić, a arkusz dostosować pod względem programu dla profilu studiów.
** W - wykład, C - ćwiczenia, P - projekt, S - seminarium.

Obowiązuje kandydatów na żołnierzy zawodowych rozpoczynających kształcenie od roku akademickiego 2025/2026

Plan studiów uchwalony przez Senat WAT w dniu 25 września 2025 r.

....

Plan specjalności „Bezpieczeństwo systemów informatycznych”

Wojskowa Akademia Techniczna

PLAN JEDNOLITYCH STUDIÓW MAGISTERSKICH DLA KANDYDATÓW NA OFICERÓW O PROFILU OGÓLNOAKADEMICKIM / ~~PRAKTYCZNYM~~*
NABÓR W ROKU AKADEMICKIM 2025

Kierunek studiów: **kryptologia i cyberbezpieczeństwo** | Dyscyplina naukowa: **informatyka techniczna i**
Specjalność: **Bezpieczeństwo systemów informatycznych (SW 29B)** | Korpus osobowy: **kryptologii i cyberbezpieczeństwa**

Indeks	GRUPY ZAJĘĆ / PRZEDMIOTY	ogółem liczba godzin/pkt ECTS: razem	w tym w CS	ECTS	Dyscyplina naukowa	Liczba godzin kontaktowych	Liczba godzin niekontaktowych	Liczba godzin razem	ECTS kształt. umiejętności naukowe	Liczba ECTS z udziałem NA	Liczba ECTS bez udziału NA	Liczba ECTS razem	wykł.	ćwicz.	ryg.	lab.	ryg.	proj.	ryg.	semin.	ryg.	zajęcia online W/C/P/S**
A. Grupa zajęć bloku wojskowego		722		2		30	20	50	2	1,2	0,8	2	248	472						2		
		174		2		30	20	50	2	1,2	0,8	2	82	92								
A.I.1	Działalność wychowawcza i profilaktyka dyscyplinarna	30											10	20								
A.I.2	Podstawy komunikacji strategicznej - teoria i praktyka	30											10	20								
A.I.3	Przywództwo w dowodzeniu	30											10	20								
A.I.4	Historia sztuki wojennej	20											10	10								
A.I.5	Historia Polski	30		2	NS	30	20	50	2	1,2	0,8	2	16	14								
A.I.6	Ochrona informacji niejawnych	10											8	2								
A.I.7	Profilaktyka antykorupcyjna	8											8									
A.I.8	Bezpieczeństwo w cyberprzestrzeni	10											4	6								
A.I.9	Bezpieczeństwo i higiena pracy (BHP)	6											6									
		548											166	380						2		
A.II.1	Podstawy dowodzenia	24											10	14								
A.II.2	Taktyka	40											10	30								
A.II.3	Podstawy survivalu	22												22								
A.II.4	Gotowość mobilizacyjna i bojowa	16											10	6								
A.II.5	Rozpoznanie i armie innych państw	20											8	10						2		
A.II.6	Topografia wojskowa	40											10	30								
A.II.7	Zabezpieczenie logistyczne działań taktycznych	16											8	8								
A.II.8	Szkolenie strzeleckie	88											10	78								
A.II.9	Systemy łączności i środki dowodzenia	20											8	12								
A.II.10	Działalność szkoleniowa i szkoleniowo - metodyczna	40											16	24								
A.II.11	Międzynarodowe prawo humanitarne konfliktów zbrojnych (MPHKZ)	20											10	10								
A.II.12	Wybrane zagadnienia bezpieczeństwa narodowego i międzynarodowego	20											8	12								
A.II.13	Podstawy eksploatacji sprzętu wojskowego (SpW)	14											6	8								
A.II.14	Działania niekinetyczne	10											4	6								
A.II.15	Ochrona środowiska	8											4	4								
A.II.16	Obrona powietrzna	18											8	10								
A.II.17	Obrona przed bronią masowego rażenia	30											8	22								
A.II.18	Połączone wsparcie ogniowe	18											8	10								
A.II.19	Zabezpieczenie inżynieryjne	20											6	14								
A.II.20	Zabezpieczenie medyczne	30											8	22								
A.II.21	Regulaminy SZ RP	34											6	28								
B. Grupa zajęć bloku sportowo - językowego		1070		24		480	120	600		19,2	4,8	24	10	1060								
B.I.1	Język angielski	480		24		480	120	600		19,2	4,8	24		480								
B.I.2	Wychowanie fizyczne	560											10	550								
B.I.3	Obóz językowy - język angielski	30												30								
C. Grupa zajęć bloku kierunku politechnicznego		2740		231		2740	3082	5822	133	108,1	122,9	231	1198	402		964		176				do 75%
I. Grupa treści kształcenia ogólnego		92		7		92	89	181	4	3,5	3,5	7	52	18		22						do 75%
C.I.1	Wprowadzenie do studiowania	6		0,5	NS	6	8	14		0,2	0,3	0,5	6									do 75%
C.I.2	Ochrona własności intelektualnych	14		1	NP	14	13	27	0,5	0,5	0,5	1	12	2								do 75%
C.I.3	Wprowadzenie do informatyki	38		3	ITT	38	38	76	1,5	1,5	1,5	3	16			22	+					do 75%
C.I.4	Podstawy zarządzania i przedsiębiorczości	34		2,5	NZJ	34	30	64	2	1,3	1,2	2,5	18	16	+							do 75%
II. Grupa treści kształcenia podstawowego		688		56,5		688	733	1421	40	27,3	29,2	56,5	342	280		66						do 75%
C.II.1	Wprowadzenie do metrologii	38		3	AEE	38	38	76	1	1,5	1,5	3	18	20	+							do 75%
C.II.2	Podstawy grafiki inżynierskiej	38		3	IM	38	38	76	2	1,5	1,5	3	14	24	+							do 75%
C.II.3	Matematyka 1	68		6	M	68	83	151	4	2,7	3,3	6	30	38	+							do 75%
C.II.4	Matematyka 2	68		6	M	68	83	151	4	2,7	3,3	6	34	34	+							do 75%
C.II.5	Matematyka dyskretna 1	30		2,5	M	30	33	63	2	1,2	1,3	2,5	16	14	+							do 75%
C.II.6	Analiza matematyczna	44		4	M	44	58	102	3,5	1,7	2,3	4	20	24	+							do 75%
C.II.7	Fizyka 1	80		6	NF	80	70	150	5	3,2	2,8	6	40	30	+	10	+					do 75%
C.II.8	Matematyka dyskretna 2	30		3	M	30	45	75	2,5	1,2	1,8	3	16	14	+							do 75%
C.II.9	Rachunek prawdopodobieństwa	32		3	M	32	45	77	2	1,2	1,8	3	18	4		10	+					do 75%
C.II.10	Teoretyczne podstawy informatyki	30		3	ITT	30	45	75	2	1,2	1,8	3	14	12	+	4						do 75%
C.II.11	Fizyka 2	60		4	NF	60	40	100	3	2,4	1,6	4	30	20	+	10	+					do 75%
C.II.12	Teoria grafów i sieci	30		2	ITT	30	20	50	1,5	1,2	0,8	2	16	14	+							do 75%
C.II.13	Podstawy optymalizacji	30		3	ITT	30	45	75	2,5	1,2	1,8	3	14	16	+							do 75%
C.II.14	Statystyka matematyczna	30		2	M	30	20	50	1	1,2	0,8	2	16			14	+					do 75%
C.II.15	Modelowanie matematyczne	30		3	ITT	30	45	75	2,5	1,2	1,8	3	14	16	+							do 75%
C.II.16	Bezpieczeństwo pracy i ergonomia	20		1	ITT	20	5	25	0,5	0,8	0,2	1	12			8	+					do 75%
C.II.17	Podstawy bezpieczeństwa informacji	30		2	ITT	30	20	50	1	1,2	0,8	2	20			10	+					do 75%
III. Grupa treści kształcenia kierunkowego		964		86,5		964	1213	2177	50,5	38	48,5	86,5	422	78		450		14				do 75%
C.III.1	Wprowadzenie do programowania	30		3	ITT	30	45	75	1,5	1,2	1,8	3	10			20	+					do 75%
C.III.2	Podstawy techniki komputerów	52		5	ITT	52	75	127	3,5	2	3	5	28	8		16	+					do 75%
C.III.3	Architektura i organizacja komputerów	52		5	ITT	52	75	127	3	2	3	5	20			32	+					do 75%
C.III.4	Podstawy podzespołów komputerów	30		2	ITT	30	20	50	1	1,2	0,8	2	14			16	+					do 75%
C.III.5	Algorytmy i struktury danych	40		4	ITT	40	60	100	2,5	1,6	2,4	4	18			22	+					do 75%
C.III.6	Teoria informacji i kodowania	40		3	ITT	40	35	75	2	1,6	1,4	3	18	10		12	+					do 75%
C.III.7	Programowanie niskopoziomowe i analiza kodu	30		2	ITT	30	20	50	1	1,2	0,8	2	14			16	+					do 75%
C.III.8	Programowanie obiektowe	52		3	ITT	52	25	77	1,5	2	1	3	20			32	+					do 75%
C.III.9	Bazy danych	52		3	ITT	52	25	77	2	2	1	3	14	12		26	+					do 75%
C.III.10	Zastosowanie kryptografii w systemach teleinformatycznych	30		3	ITT	30	45	75	1,5	1,2	1,8	3	10			20	+					do 75%
C.III.11	Systemy operacyjne	52		5	ITT	52	75	127	3	2	3	5	26			26	+					do 75%
C.III.12	Elementy teorii liczb	30		3	M	30	45	75	2,5	1,2	1,8	3	16	14	+							do 75%
C.III.13	Wybrane elementy kryptologii	52		4	M	52	50	102	2,5	2	2	4	20			32	+					do 75%
C.III.14	Interfejsy komputerów	40		3	ITT	40	35	75	2	1,6	1,4	3	16	4		20	+					do 75%
C.III.15	Zastosowania kryptografii w Internecie	30		3	ITT	30	45	75	1,5	1,2	1,8	3	14			16	+					do 75%
C.III.16	Inżynieria oprogramowania	40		4	ITT	40	60	100	2	1,6	2,4	4	12			28	+					do 75%
C.III.17	Sieci komputerowe	52		5,5	ITT	52	88	140	3,5	2	3,5	5,5	28			24	+					do 75%
C.III.18	Protokoły kryptograficzne	30		3	ITT	30	45	75	1,5	1,2	1,8	3	16			14	+					do 75%
C.III.19	Niezawodność systemów komputerowych	30		2	ITT	30	20	50	1,5	1,2	0,8	2	14	16	+							do 75%
C.III.20	Bezpieczeństwo baz danych	30		4	ITT	30	70	100	2	1,2	2,8	4	14			16	+					do 75%
C.III.21	Procesy stochastyczne	30		2	M	30	20	50	1,5	1,2	0,8	2	16	14	+							do 75%
C.III.22	Metody symulacji komputerowej	40		4	ITT	40	60	100	2	1,6	2,4	4	16			24	+					do 75%
C.III.23	Steganografia	30		3	ITT	30	45	75	1,5	1,2	1,8	3	16			14	+					do 75%
C.III.24	Diagnostyka i tolerowanie uszkodzeń	40		6	ITT	40	110	150	3	1,6	4,4	6	16			10	+	14				do 75%
C.III.25	Sztuczna inteligencja	30		2	ITT	30	20	50	1	1,2	0,8	2	16			14	+					do 75%
IV. Grupa treści kształcenia specjalistycznego		996		81		996	1047	2043	38,5	39,3	41,7	81	382	26		426		162				do 75%
C.IV.1	Ataki sieciowe i złośliwe oprogramowanie	44		3	ITT	44	33	77	1	1,7	1,3	3	10			20	+	14	+			do 75%
C.IV.2	Bezpieczeństwo sieci komputerowych	30		3	ITT	30	45	75	1,5	1,2	1,8	3	10			20	+					do 75%
C.IV.3	Podstawy projektowania bezpiecznego oprogramowania	44		4	ITT	44	58	102	1,5	1,7	2,3	4	12			8	+	24	+			do 75%
C.IV.4	Automaty i języki formalne	30		3	ITT	30	45	75	1,5	1,2	1,8	3	12			18	+					do 75%
C.IV.5	Programowanie w językach funkcyjnych	30		3	ITT	30	45	75	1,5	1,2	1,8	3	14			16	+					do 75%
C.IV.6	Techniki algorytmiczne	30		3	ITT	30	45	75	1,5	1,2	1,8	3	14			4		12	+			do 75%
C.IV.7	Bussines modeling in UML	30		2	ITT	30	20	50	1	1,2	0,8	2	10			20	+					do 75%
C.IV.8	Modelowanie i symulacja procesów biznesowych	30		2	ITT	30	20	50	1	1,2	0,8	2	14			16	+					do 75%
C.IV.9	Metody eksploracji danych	30		3	ITT	30	45	75	1,5	1,2	1,8	3	12			18	+					do 75%
C.IV.10	Metody i narzędzia generowania kodu wykonywalnego	44		4	ITT	44	58	102	2	1,7	2,3	4	12			32	+					do 75%
C.IV.11	Metody projektowania i wdrażania systemów informatycznych	60		4	ITT	60	40	100	2,5	2,4	1,6	4	30			18	+	12	+			do 75%
C.IV.12	Technologie usługowe i mobilne	30		2	ITT	30	20	50	0,5	1,2	0,8	2	10			10	+	10	+			do 75%
C.IV.13	Metody sztucznej inteligencji	30		2	ITT	30	20	50	1	1,2	0,8	2	16			14	+					do 75%
C.IV.14	Metody ilościowe analizy ryzyka	30		2	ITT	30	20	50	1	1,2	0,8	2	10	6	+	14	+					do 75%
C.IV.15	Systemy webowe	30		2	ITT	30	20	50	1	1,2	0,8	2	14			16	+					do 75%
C.IV.16	Bezpieczeństwo systemów informacyjnych	30		3	ITT	30	45	75	1,5	1,2	1,8	3	14			16	+					do 75%
C.IV.17	Metody i systemy wspomagania decyzji	30		3	ITT	30	45	75	1,5	1,2	1,8	3	14			8	+	8	+			do 75%
C.IV.18	Obliczenia równoległe i rozproszone	44		3	ITT	44	33	77	1	1,7	1,3	3	14			16	+	14	+			do 75%
C.IV.19	Podstawy kryptologii współczesnej	30		2	ITT	30	20	50	1	1,2	0,8	2	14			16	+					do 75%
C.IV.20	Modelowanie i analiza sieci złożonych	44		3	ITT	44	33	77	2	1,7	1,3	3	18	10	+	16	+					do 75%
C.IV.21	Zarządzanie projektami	30		3	ITT	30	45	75	1,5	1,2	1,8	3	14			16	+					do 75%
C.IV.22	Ilościowe metody oceny bezpieczeństwa systemów teleinformatycznych	30		2	ITT	30	20	50	1	1,2	0,8	2	14			16	+					do 75%
C.IV.23	Architektura korporacyjna	30		3	ITT	30	45	75	1,5	1,2	1,8	3	14			16	+					do 75%
C.IV.24	Teoria wojny informacyjnej	30		2	ITT	30	20	50	1	1,2	0,8	2	16			14	+					do 75%
C.IV.25	Inżynieria wsteczna systemów informatycznych	44		4	ITT	44	58	102	2,5	1,7	2,3	4	20			24	+					do 75%
C.IV.26	Niezawodność i wydajność systemów informatycznych	44		3	ITT	44	33	77	2	1,7	1,3	3	18	10	+	16	+					do 75%
C.IV.27	Projekt z zakresu bezpieczeństwa systemów	44		4	ITT	44	58	102	0,5	1,7	2,3	4						44	+			do 75%
C.IV.28	Inżynieria wsteczna złośliwego oprogramowania	44		4	ITT	44	58	102	1,5	1,7	2,3	4	12			8	+	24	+			do 75%
D. Praca dyplomowa / egz. na oficera		164		27		164	513	677	8,5	6,5	20,5	27						100		64		
D.I.1	Seminarium przeddyplomowe	20		1	ITT	20	5	25	0,5	0,8	0,2	1								20	+	do 75%
D.I.2	Seminarium dyplomowe	44		4	ITT	44	58	102	3,5	1,7	2,3	4								44	+	do 75%
D.I.3	Praca dyplomowa	100		22	ITT	100	450	550	4,5	4	18	22						100				
D.I.4	Egzamin na oficera																					
E. Praktyki zawodowe		400	400	16		400				16		16										
E.I.1	Praktyka d-cy drużyny	100	100	4		100				4		4										
E.I.2	Praktyka d-cy plutonu	100	100	4		100				4		4										
E.I.3	Praktyka zawodowa	100	100	4	ITT	100				4		4										
E.I.4	Szkolenie specjalistyczne	100	100	4	ITT	100				4		4										
F. Inne													termin realizacji									Uwagi
F.I.1																						
	ogółem godzin / pkt. ECTS	5096	400	300	X	3814	3735	7149	143,5	151	149	300	1456	1934		964		276		66		X

Liczba godzin/rygor/pkt ECTS w semestrze (jednolite studia magisterskie):

Indeks	I godz.	I ryg.	I ECTS	II godz.	II ryg.	II ECTS	III godz.	III ryg.	III ECTS	IV godz.	IV ryg.	IV ECTS	V godz.	V ryg.	V ECTS	VI godz.	VI ryg.	VI ECTS	VII godz.	VII ryg.	VII ECTS	VIII godz.	VIII ryg.	VIII ECTS	IX godz.	IX ryg.	IX ECTS	X godz.	X ryg.	X ECTS	Jednostka organizacyjna (instytut/katedra) odpowiedzialna za przedmiot	Uwagi
A.	146		2	134			72			84			60			72			76			78										
	46		2	20			36			32									10			30										
A.I.1				8	Z					12	Zo								10	Zo											WLO-IOZ	
A.I.2																						30	Zo								WLO-IOZ	
A.I.3				8	Z		22	E																							WLO-IOZ	
A.I.4										20	Zo																				WLO-IOZ	
A.I.5	30	E	2																												WLO-IOZ	
A.I.6				4	Z		6	Zo																							SSW	
A.I.7							8	Z																							WLO-IOZ	
A.I.8	10	Zo																													WCY	
A.I.9	6	Z																													Sekcja BHP	
	100			114			36			52			60			72			66			48										
A.II.1	12	Z		12	Zo																										SSW	
A.II.2	10	Z		10	Zo		8	Z		12	Zo																				SSW	
A.II.3										22	Zo																				SSW	
A.II.4				6	Z								10	Zo																	SSW	
A.II.5	8	Z		12	Zo																										SSW	
A.II.6	20	Zo																				20	Zo								WIG	
A.II.7				8	Z														8	Z											WLO	
A.II.8	14	Zo		16	Zo		8	Zo		10	Zo		8	Zo		10	Zo		12	Zo		10	Zo								SSW	
A.II.9				10	Zo		10	Zo																							WEL	
A.II.10	6	Zo		10	Zo								14	Zo		10	Zo														WLO-IOZ/SSW	
A.II.11																			20	E											WLO-IOZ	
A.II.12																			20	Zo											WLO-IBO	
A.II.13																14	Zo														WML	
A.II.14																						10	Z								WLO	
A.II.15													8	Z																	WIG	
A.II.16	10	Zo								8	Zo																				SSW	
A.II.17	10	Zo														20	Zo														WTC	
A.II.18																18	Zo														WML	
A.II.19				10	Zo		10	Zo																							SSW	
A.II.20				10	Zo								20	E																	SSW	
A.II.21	10	Zo		10	Zo														6	Z		8	Zo								SSW	
B.	120		3	120		3	120		3	150		3	120		3	120		3	130		3	120		3	60			10				
B.I.1	60	Zo	3	60	Zo	3	60	Zo	3	60	Zo	3	60	Zo	3	60	E	3	60	Zo	3	60	Zo	3							SJO	
B.I.2	60	Zo		60	Zo		60	Zo		60	Zo		60	Zo		60	Zo		70	Zo		60	Zo		60	Zo		10	E		SWF	
B.I.3										30	Z																				SJO	
C.	300		25	298		27	342		27	296		23	308		27	268		23	344		27	278		23	306		29					
I.	58		4,5										34		2,5																	
C.I.1	6	+	0,5																												PJ	(*)
C.I.2	14	+	1																												WLO-IOZ	(*)
C.I.3	38	+	3																												WCY-ISI	(*)
C.I.4													34	+	2,5																WLO-IOZ	(*)
II.	242		20,5	216		19	150		11	50		4	30		2																	
C.II.1	38	+	3																												WEL/WTC	(*)
C.II.2	38	+	3																												WIM	(*)
C.II.3	68	x	6																												WCY-IMK	(*)
C.II.4	68	x	6																												WCY-IMK	(*)
C.II.5	30	+	2,5																												WCY-IMK	(*)
C.II.6				44	x	4																									WCY-IMK	(*)
C.II.7				80	x	6																									WTC	(*)
C.II.8				30	x	3																									WCY-IMK	(*)
C.II.9				32	+	3																									WCY-IMK	(*)
C.II.10				30	+	3																									WCY-ISI	(*)
C.II.11							60	x	4																						WTC	(*)
C.II.12							30	+	2																						WCY-ISI	(*)
C.II.13							30	+	3																						WCY-ISI	(*)
C.II.14							30	+	2																						WCY-IMK	(*)
C.II.15										30	+	3																			WCY-ISI	(*)
C.II.16										20	+	1																			WCY-ITC	(*)
C.II.17													30	+	2																WCY-ISI	(*)
III.				82		8	192		16	246		19	244		22,5	30		2	60		6	40		4	70		9					
C.III.1				30	x	3																									WCY-ISI	(*)
C.III.2				52	+	5																									WCY-ITC	(*)
C.III.3							52	x	5																						WCY-ITC	(*)
C.III.4							30	+	2																						WCY-ISI	(*)
C.III.5							40	x	4																						WCY-ISI	(*)
C.III.6							40	+	3																						WCY-ITC	(*)
C.III.7							30	+	2																						WCY-ITC	(*)
C.III.8										52	+	3																			WCY-ISI	(*)
C.III.9										52	x	3																			WCY-ISI	(*)
C.III.10										30	x	3																			WCY-IMK	(*)
C.III.11										52	x	5																			WCY-ITC	(*)
C.III.12										30	+	3																			WCY-IMK	(*)
C.III.13													52	x	4																WCY-IMK	(*)
C.III.14													40	+	3																WCY-ITC	(*)
C.III.15													30	+	3																WCY-IMK	(*)
C.III.16													40	x	4																WCY-ISI	(*)
C.III.17													52	x	5,5																WCY-ITC	(*)
C.III.18													30	+	3																WCY-IMK	(*)
C.III.19																30	+	2													WCY-ISI	(*)
C.III.20																			30	+	4										WCY-ISI	(*)
C.III.21																			30	+	2										WCY-IMK	(*)
C.III.22																						40	x	4							WCY-ISI	(*)
C.III.23																									30	+	3				WCY-IMK	(*)
C.III.24																									40	x	6				WCY-ISI	(*)
C.III.25										30	+	2																			WCY-ISI	(*)
IV.																238		21	284		21	238		19	236		20					
C.IV.1																44	+	3													WCY-ITC	(*)
C.IV.2																30	+	3													WCY-ITC	(*)
C.IV.3																44	+	4													WCY-ISI	(*)
C.IV.4																30	x	3													WCY-ISI	(*)
C.IV.5																30	+	3													WCY-ISI	(*)
C.IV.6																30	x	3													WCY-ISI	(*)
C.IV.7																30	+	2													WCY-ISI	(*), w jęz. ang.
C.IV.8																			30	+	2										WCY-ISI	(*)
C.IV.9																			30	x	3										WCY-ISI	(*)
C.IV.10																			44	x	4										WCY-ISI	(*)
C.IV.11																			60	x	4										WCY-ISI	(*)
C.IV.12																			30	+	2										WCY-ISI	(*)
C.IV.13																			30	+	2										WCY-ISI	(*)
C.IV.14																			30	+	2										WCY-ISI	(*)
C.IV.15																			30	+	2										WCY-ISI	(*)
C.IV.16																						30	+	3							WCY-ISI	(*)
C.IV.17																						30	+	3							WCY-ISI	(*)
C.IV.18																						44	+	3							WCY-ISI	(*)
C.IV.19																						30	+	2							WCY-IMK	(*)
C.IV.20																						44	x	3							WCY-ISI	(*)
C.IV.21																						30	+	3							WCY-ISI	(*)
C.IV.22																						30	+	2							WCY-ISI	(*)
C.IV.23																									30	+	3				WCY-ISI	(*)
C.IV.24																									30	+	2				WCY-ISI	(*)
C.IV.25																									44	x	4				WCY-ISI	(*)
C.IV.26																									44	+	3				WCY-ISI	(*)
C.IV.27																									44	+	4				WCY-ISI	(*)
C.IV.28																									44	x	4				WCY-ISI	(*)
D.																									20		1	144		26		
D.I.1																									20	+	1				WCY	(*)
D.I.2																												44	+	4	WCY	(*)
D.I.3																												100	x	22	WCY	
D.I.4																													E		SSW	
E.										100		4				100		4				100		4				100		4		
E.I.1										100	+	4																			CS/JW	
E.I.2																												100	+	4	CS/JW	
E.I.3																100	+	4													CS/JW	
E.I.4																						100	+	4							CS/JW	
ogółem godzin / pkt. ECTS	566		30	552		30	534		30	630		30	488		30	560		30	550		30	576		30	386		30	254		30		

	I	II	III	IV	V	VI	VII	VIII	IX	X
dopuszczalny deficyt pkt. ECTS (w semestrze / łącznie)	15/15	18/18	15/25	15/25	15/25	15/25	15/25	15/25	15/25	15/25
ogółem godzin realizowanych w Centrach Szkolenia (w tym w CS)										
rodzaje i liczba rygorów w semestrze: egzaminy (E, x)	3	4	4	3	4	3	4	2	3	2
zaliczenia z oceną (Zo, +)	15	14	12	13	10	12	12	12	7	1
zaliczenia bez oceny (Z, z)	6	10	4	2	2		4	2		
projekty przejściowe (P)										

* niepotrzebne skreślić, a arkusz dostosować pod względem programu dla profilu studiów.
** W - wykład, C - ćwiczenia, P - projekt, S - seminarium.

Obowiązuje kandydatów na żołnierzy zawodowych rozpoczynających kształcenie od roku akademickiego 2025/2026

Plan studiów uchwalony przez Senat WAT w dniu 25 września 2025 r.

PLAN SPECJALNOŚCI „CYBEROBRONA”

Wojskowa Akademia Techniczna

PLAN JEDNOLITYCH STUDIÓW MAGISTERSKICH DLA KANDYDATÓW NA OFICERÓW O PROFILU OGÓLNOAKADEMICKIM / ~~PRAKTYCZNYM~~*
NABÓR W ROKU AKADEMICKIM 2025

Kierunek studiów: **kryptologia i cyberbezpieczeństwo** | Dyscyplina naukowa: **informatyka techniczna i**

Specjalność: **Cyberobrona (SW29B)** | Korpus osobowy: **kryptologii i cyberbezpieczeństwa**

jednolite studia magisterskie – liczba godzin/rygor/pkt ECTS w semestrze:

Indeks	GRUPY ZAJĘĆ / PRZEDMIOTY	ogółem liczba godzin/ pkt ECTS: razem	w tym w CS	ECTS	Dyscyplina naukowa	Liczba godzin kontaktowych	Liczba godzin niekontaktowych	Liczba godzin razem	ECTS kształt. umiejętności naukowe	Liczba ECTS z udziałem NA	Liczba ECTS bez udziału NA	Liczba ECTS razem	wykł.	ćwicz.	lab.	proj.	semin.	zajęcia online WCP/S**	I godz.	I ryg.	I ECTS	II godz.	II ryg.	II ECTS	III godz.	III ryg.	III ECTS	IV godz.	IV ryg.	IV ECTS	V godz.	V ryg.	V ECTS	VI godz.	VI ryg.	VI ECTS	VII godz.	VII ryg.	VII ECTS	VIII godz.	VIII ryg.	VIII ECTS	IX godz.	IX ryg.	IX ECTS	X godz.	X ryg.	X ECTS	jednostka organizacyjna (instytut/katedra) odpowiedzialna za przedmiot	Uwagi
A. Grupa zajęć bloku wojskowego		722		2		30	20	50	2	1,2	0,8	2	248	472			2		146		2	134			72			84			60			72			76			78										
		174		2		30	20	50	2	1,2	0,8	2	82	92					46		2	20			36			32									10			30										
A.I.1	Działalność wychowawcza i profilaktyka dyscyplinarna	30											10	20								8	Z					12	Zo								10	Zo											WLO-IOZ	
A.I.2	Podstawy komunikacji strategicznej - teoria i praktyka	30											10	20																										30	Zo								WLO-IOZ	
A.I.3	Przywództwo w dowodzeniu	30											10	20								8	Z		22	E																							WLO-IOZ	
A.I.4	Historia sztuki wojennej	20											10	10														20	Zo																				WLO-IOZ	
A.I.5	Historia Polski	30		2	NS	30	20	50	2	1,2	0,8	2	16	14					30	E	2																												WLO-IOZ	
A.I.6	Ochrona informacji niejawnych	10											8	2								4	Z		6	Zo																							SSW	
A.I.7	Profilaktyka antykorupcyjna	8											8												8	Z																							WLO-IOZ	
A.I.8	Bezpieczeństwo w cyberprzestrzeni	10											4	6					10	Zo																													WCY	
A.I.9	Bezpieczeństwo i higiena pracy (BHP)	6											6						6	Z																													Sekcja BHP	
		548											166	380			2		100			114			36			52			60			72			66			48										
A.II.1	Podstawy dowodzenia	24											10	14					12	Z		12	Zo																										SSW	
A.II.2	Taktyka	40											10	30					10	Z		10	Zo		8	Z		12	Zo																				SSW	
A.II.3	Podstawy survivalu	22												22														22	Zo																				SSW	
A.II.4	Gotowość mobilizacyjna i bojowa	16											10	6								6	Z								10	Zo																	SSW	
A.II.5	Rozpoznanie i armie innych państw	20											8	10			2		8	Z		12	Zo																										SSW	
A.II.6	Topografia wojskowa	40											10	30					20	Zo																				20	Zo								WIG	
A.II.7	Zabezpieczenie logistyczne działań taktycznych	16											8	8								8	Z														8	Z											WLO	
A.II.8	Szkolenie strzeleckie	88											10	78					14	Zo		16	Zo		8	Zo		10	Zo		8	Zo		10	Zo		12	Zo		10	Zo								SSW	
A.II.9	Systemy łączności i środki dowodzenia	20											8	12								10	Zo		10	Zo																							WEL	
A.II.10	Działalność szkoleniowa i szkoleniowo - metodyczna	40											16	24					6	Zo		10	Zo								14	Zo		10	Zo														WLO-IOZ/SSW	
A.II.11	Międzynarodowe prawo humanitarne konfliktów zbrojnych (MPHKZ)	20											10	10																							20	E											WLO-IOZ	
A.II.12	Wybrane zagadnienia bezpieczeństwa narodowego I	20											8	12																							20	Zo											WLO-IBO	
A.II.13	Podstawy eksploatacji sprzętu wojskowego (SpW)	14											6	8																				14	Zo														WML	
A.II.14	Działania niekinetyczne	10											4	6																										10	Z								WLO	
A.II.15	Ochrona środowiska	8											4	4																	8	Z																	WIG	
A.II.16	Obrona powietrzna	18											8	10					10	Zo								8	Zo																				SSW	
A.II.17	Obrona przed bronią masowego rażenia	30											8	22					10	Zo														20	Zo														WTC	
A.II.18	Połączone wsparcie ogniowe	18											8	10																				18	Zo														WML	
A.II.19	Zabezpieczenie inżynieryjne	20											6	14								10	Zo		10	Zo																							SSW	
A.II.20	Zabezpieczenie medyczne	30											8	22								10	Zo								20	E																	SSW	
A.II.21	Regulaminy SZ RP	34											6	28					10	Zo		10	Zo														6	Z		8	Zo								SSW	
B. Grupa zajęć bloku sportowo - językowego		1070		24		480	120	600		19,2	4,8	24	10	1060					120		3	120		3	120		3	150		3	120		3	120		3	130		3	120		3	60			10				
B.I.1	Język angielski	480		24		480	120	600		19,2	4,8	24		480					60	Zo	3	60	Zo	3	60	Zo	3	60	Zo	3	60	Zo	3	60	E	3	60	Zo	3	60	Zo	3							SJO	
B.I.2	Wychowanie fizyczne	560											10	550					60	Zo		60	Zo		60	Zo		60	Zo		60	Zo		60	Zo		70	Zo		60	Zo		60	Zo		10	E		SWF	
B.I.3	Obóz językowy - język angielski	30												30														30	Z																				SJO	
C. Grupa zajęć bloku kierunku politechnicznego		2762		231		2762	3056	5818	132,5	109,1	121,9	231	1194	386	1030	152		do 75%	300		25	298		27	342		27	296		23	308		27	356		23	328		27	300		23	234		29					
I. Grupa treści kształcenia ogólnego		92		7		92	89	181	4	3,5	3,5	7	52	18	22			do 75%	58		4,5										34		2,5																	
C.I.1	Wprowadzenie do studiowania	6		0,5	NS	6	8	14		0,2	0,3	0,5	6					do 75%	6	+	0,5																												PJ	(*)
C.I.2	Ochrona własności intelektualnych	14		1	NP	14	13	27	0,5	0,5	0,5	1	12	2				do 75%	14	+	1																												WLO-IOZ	(*)
C.I.3	Wprowadzenie do informatyki	38		3	ITT	38	38	76	1,5	1,5	1,5	3	16		22 +			do 75%	38	+	3																												WCY-ISI	(*)
C.I.4	Podstawy zarządzania i przedsiębiorczości	34		2,5	NZJ	34	30	64	2	1,3	1,2	2,5	18	16 +				do 75%													34	+	2,5																WLO-IOZ	(*)
II. Grupa treści kształcenia podstawowego		688		56,5		688	733	1421	40	27,3	29,2	56,5	342	280	66			do 75%	242		20,5	216		19	150		11	50		4	30		2																	
C.II.1	Wprowadzenie do metrologii	38		3	AEE	38	38	76	1	1,5	1,5	3	18	20 +				do 75%	38	+	3																												WEL/WTC	(*)
C.II.2	Podstawy grafiki inżynierskiej	38		3	IM	38	38	76	2	1,5	1,5	3	14	24 +				do 75%	38	+	3																												WIM	(*)
C.II.3	Matematyka 1	68		6	M	68	83	151	4	2,7	3,3	6	30	38 +				do 75%	68	x	6																												WCY-IMK	(*)
C.II.4	Matematyka 2	68		6	M	68	83	151	4	2,7	3,3	6	34	34 +				do 75%	68	x	6																												WCY-IMK	(*)
C.II.5	Matematyka dyskretna 1	30		2,5	M	30	33	63	2	1,2	1,3	2,5	16	14 +				do 75%	30	+	2,5																												WCY-IMK	(*)
C.II.6	Analiza matematyczna	44		4	M	44	58	102	3,5	1,7	2,3	4	20	24 +				do 75%				44	x	4																									WCY-IMK	(*)
C.II.7	Fizyka 1	80		6	NF	80	70	150	5	3,2	2,8	6	40	30 +	10 +			do 75%				80	x	6																									WTC	(*)
C.II.8	Matematyka dyskretna 2	30		3	M	30	45	75	2,5	1,2	1,8	3	16	14 +				do 75%				30	x	3																									WCY-IMK	(*)
C.II.9	Rachunek prawdopodobieństwa	32		3	M	32	45	77	2	1,2	1,8	3	18	4	10 +			do 75%				32	+	3																									WCY-IMK	(*)
C.II.10	Teoretyczne podstawy informatyki	30		3	ITT	30	45	75	2	1,2	1,8	3	14	12 +	4			do 75%				30	+	3																									WCY-ISI	(*)
C.II.11	Fizyka 2	60		4	NF	60	40	100	3	2,4	1,6	4	30	20 +	10 +			do 75%							60	x	4																						WTC	(*)
C.II.12	Teoria grafów i sieci	30		2	ITT	30	20	50	1,5	1,2	0,8	2	16	14 +				do 75%							30	+	2																						WCY-ISI	(*)
C.II.13	Podstawy optymalizacji	30		3	ITT	30	45	75	2,5	1,2	1,8	3	14	16 +				do 75%							30	+	3																						WCY-ISI	(*)
C.II.14	Statystyka matematyczna	30		2	M	30	20	50	1	1,2	0,8	2	16		14 +			do 75%							30	+	2																						WCY-IMK	(*)
C.II.15	Modelowanie matematyczne	30		3	ITT	30	45	75	2,5	1,2	1,8	3	14	16 +				do 75%										30	+	3																			WCY-ISI	(*)
C.II.16	Bezpieczeństwo pracy i ergonomia	20		1	ITT	20	5	25	0,5	0,8	0,2	1	12		8 +			do 75%										20	+	1																			WCY-ITC	(*)
C.II.17	Podstawy bezpieczeństwa informacji	30		2	ITT	30	20	50	1	1,2	0,8	2	20		10 +			do 75%													30	+	2																WCY-ISI	(*)
III. Grupa treści kształcenia kierunkowego		964		86,5		964	1213	2177	50,5	38	48,5	86,5	422	78	450	14		do 75%				82		8	192		16	246		19	244		22,5	30		2	60		6	40		4	70		9					
C.III.1	Wprowadzenie do programowania	30		3	ITT	30	45	75	1,5	1,2	1,8	3	10		20 +			do 75%				30	x	3																									WCY-ISI	(*)
C.III.2	Podstawy techniki komputerów	52		5	ITT	52	75	127	3,5	2	3	5	28	8	16 +			do 75%				52	+	5																									WCY-ITC	(*)
C.III.3	Architektura i organizacja komputerów	52		5	ITT	52	75	127	3	2	3	5	20		32 +			do 75%							52	x	5																						WCY-ITC	(*)
C.III.4	Podstawy podzespołów komputerów	30		2	ITT	30	20	50	1	1,2	0,8	2	14		16 +			do 75%							30	+	2																						WCY-ISI	(*)
C.III.5	Algorytmy i struktury danych	40		4	ITT	40	60	100	2,5	1,6	2,4	4	18		22 +			do 75%							40	x	4																						WCY-ISI	(*)
C.III.6	Teoria informacji i kodowania	40		3	ITT	40	35	75	2	1,6	1,4	3	18	10	12 +			do 75%							40	+	3																						WCY-ITC	(*)
C.III.7	Programowanie niskopoziomowe i analiza kodu	30		2	ITT	30	20	50	1	1,2	0,8	2	14		16 +			do 75%							30	+	2																						WCY-ITC	(*)
C.III.8	Programowanie obiektowe	52		3	ITT	52	25	77	1,5	2	1	3	20		32 +			do 75%										52	+	3																			WCY-ISI	(*)
C.III.9	Bazy danych	52		3	ITT	52	25	77	2	2	1	3	14	12	26 +			do 75%										52	x	3																			WCY-ISI	(*)
C.III.10	Zastosowanie kryptografii w systemach teleinformatycznych	30		3	ITT	30	45	75	1,5	1,2	1,8	3	10		20 +			do 75%										30	x	3																			WCY-IMK	(*)
C.III.11	Systemy operacyjne	52		5	ITT	52	75	127	3	2	3	5	26		26 +			do 75%										52	x	5																			WCY-ITC	(*)
C.III.12	Elementy teorii liczb	30		3	M	30	45	75	2,5	1,2	1,8	3	16	14 +				do 75%										30	+	3																			WCY-IMK	(*)
C.III.13	Wybrane elementy kryptologii	52		4	M	52	50	102	2,5	2	2	4	20		32 +			do 75%													52	x	4																WCY-IMK	(*)
C.III.14	Interfejsy komputerów	40		3	ITT	40	35	75	2	1,6	1,4	3	16	4	20 +			do 75%													40	+	3																WCY-ITC	(*)
C.III.15	Zastosowania kryptografii w Internecie	30		3	ITT	30	45	75	1,5	1,2	1,8	3	14		16 +			do 75%													30	+	3																WCY-IMK	(*)
C.III.16	Inżynieria oprogramowania	40		4	ITT	40	60	100	2	1,6	2,4	4	12		28 +			do 75%													40	x	4																WCY-ISI	(*)
C.III.17	Sieci komputerowe	52		5,5	ITT	52	88	140	3,5	2	3,5	5,5	28		24 +			do 75%													52	x	5,5																WCY-ITC	(*)
C.III.18	Protokoły kryptograficzne	30		3	ITT	30	45	75	1,5	1,2	1,8	3	16		14 +			do 75%													30	+	3																WCY-IMK	(*)
C.III.19	Niezawodność systemów komputerowych	30		2	ITT	30	20	50	1,5	1,2	0,8	2	14	16 +				do 75%																30	+	2													WCY-ISI	(*)
C.III.20	Bezpieczeństwo baz danych	30		4	ITT	30	70	100	2	1,2	2,8	4	14		16 +			do 75%																			30	+	4										WCY-ISI	(*)
C.III.21	Procesy stochastyczne	30		2	M	30	20	50	1,5	1,2	0,8	2	16	14 +				do 75%																			30	+	2										WCY-IMK	(*)
C.III.22	Metody symulacji komputerowej	40		4	ITT	40	60	100	2	1,6	2,4	4	16		24 +			do 75%																						40	x	4							WCY-ISI	(*)
C.III.23	Steganografia	30		3	ITT	30	45	75	1,5	1,2	1,8	3	16		14 +			do 75%																									30	+	3				WCY-IMK	(*)
C.III.24	Diagnostyka i tolerowanie uszkodzeń	40		6	ITT	40	110	150	3	1,6	4,4	6	16		10 +	14		do 75%																									40	x	6				WCY-ISI	(*)
C.III.25	Sztuczna inteligencja	30		2	ITT	30	20	50	1	1,2	0,8	2	16		14 +			do 75%										30	+	2																			WCY-ISI	(*)
IV. Grupa treści kształcenia specjalistycznego		1018		81		1018	1021	2039	38	40,3	40,7	81	378	10	492	138		do 75%																326		21	268		21	260		19	164		20					
C.IV.1	Sieci komputerowe II	30		2	ITT	30	20	50	1	1,2	0,8	2	10		20 +			do 75%																30	+	2													WCY-ITC	(*)
C.IV.2	JavaEE Technologies	30		2	ITT	30	20	50	1	1,2	0,8	2	10		20 +			do 75%																30	+	2													WCY-ITC	(*), w jęz. ang.
C.IV.3	HTML i aplikacje webowe	30		2	ITT	30	20	50	1	1,2	0,8	2	14		16 +			do 75%																30	+	2													WCY-ITC	(*)
C.IV.4	Systemy operacyjne UNIX	60		3	ITT	60	15	75	1,5	2,4	0,6	3	20		40 +			do 75%																60	x	3													WCY-ITC	(*)
C.IV.5	Ataki sieciowe	44		3	ITT	44	33	77	1,5	1,7	1,3	3	16		28 +			do 75%																44	+	3													WCY-ITC	(*)
C.IV.6	Oprogramowanie niepożądane i inspekcja kodu	44		3	ITT	44	33	77	1	1,7	1,3	3	14		14 +	16 +		do 75%																44	+	3													WCY-ITC	(*)
C.IV.7	Eksploracja sieci teleinformatycznych	44		3	ITT	44	33	77	1,5	1,7	1,3	3	14		20 +	10 +		do 75%																44	x	3													WCY-ITC	(*)
C.IV.8	Systemy wbudowane	44		3	ITT	44	33	77	1,5	1,7	1,3	3	20		24 +			do 75%																44	+	3													WCY-ITC	(*)
C.IV.9	Bezpieczeństwo sieci bezprzewodowych	30		2	ITT	30	20	50	1	1,2	0,8	2	14		16 +			do 75%																			30	+	2										WCY-ITC	(*)
C.IV.10	Modelowanie i analiza systemów teleinformatycznych	44		4	ITT	44	58	102	2	1,7	2,3	4	14		20 +	10 +		do 75%																			44	x	4										WCY-ITC	(*)
C.IV.11	Systemy bezpieczeństwa sieciowego	30		2	ITT	30	20	50	1	1,2	0,8	2	10		20 +			do 75%																			30	+	2										WCY-ITC	(*)
C.IV.12	Podstawy przetwarzania rozproszonego	30		2	ITT	30	20	50	1	1,2	0,8	2	10		20 +			do 75%																			30	+	2										WCY-ITC	(*)
C.IV.13	Administrowanie środowiskiem Windows	44		4	ITT	44	58	102	2	1,7	2,3	4	14		30 +			do 75%																			44	x	4										WCY-ITC	(*)
C.IV.14	Bezpieczeństwo sieci IPv6	30		3	ITT	30	45	75	1,5	1,2	1,8	3	10		20 +			do 75%																			30	+	3										WCY-ITC	(*)
C.IV.15	Projektowanie i wytwarzanie systemów teleinformatycznych	60		4	ITT	60	40	100	2	2,4	1,6	4	24		24 +	12 +		do 75%																			60	x	4										WCY-ITC	(*)
C.IV.16	Zabezpieczenia teleinformatyczne	30		2	ITT	30	20	50	1	1,2	0,8	2	10		20 +			do 75%																						30	+	2							WCY-ITC	(*)
C.IV.17	Zarządzanie bezpieczeństwem informacji	40		3	ITT	40	35	75	2	1,6	1,4	3	20	10 +	10 +			do 75%																						40	+	3							WCY-ITC	(*)
C.IV.18	Techniki dochodzeniowe i śledcze	30		2	ITT	30	20	50	1	1,2	0,8	2	10		20 +			do 75%																						30	+	2							WCY-ITC	(*)
C.IV.19	Zarządzanie sieciami teleinformatycznymi	40		3	ITT	40	35	75	1	1,6	1,4	3	10		20 +	10 +		do 75%																						40	x	3							WCY-ITC	(*)
C.IV.20	Technologie Internetu rzeczy	30		2	ITT	30	20	50	1	1,2	0,8	2	16			14 +		do 75%																						30	+	2							WCY-ITC	(*)
C.IV.21	Studium ataków i incydentów	30		2	ITT	30	20	50	1	1,2	0,8	2	14		16 +			do 75%																						30	+	2							WCY-ITC	(*)
C.IV.22	Wirtualizacja systemów IT	30		2	ITT	30	20	50	0,5	1,2	0,8	2	10		12 +	8 +		do 75%																						30	+	2							WCY-ITC	(*)
C.IV.23	Walka w cyberprzestrzeni	30		3	ITT	30	45	75	1,5	1,2	1,8	3	10		20 +			do 75%																						30	x	3							WCY-ITC	(*)
C.IV.24	Projekt z zakresu cyberobrony	30		4	ITT	30	70	100	0,5	1,2	2,8	4				30 +		do 75%																									30	+	4				WCY-ITC	(*)
C.IV.25	Systemy rozproszone	30		4	ITT	30	70	100	2	1,2	2,8	4	16			14 +		do 75%																									30	x	4				WCY-ITC	(*)
C.IV.26	Trends in computer technology	30		4	ITT	30	70	100	2,5	1,2	2,8	4	20		10 +			do 75%																									30	+	4				WCY-ITC	(*), w jęz. ang.
C.IV.27	Technologie mobilne	30		3	ITT	30	45	75	1,5	1,2	1,8	3	14		16 +			do 75%																									30	+	3				WCY-ITC	(*)
C.IV.28	Projektowanie systemów bezpieczeństwa informacji	44		5	ITT	44	83	127	2	1,7	3,3	5	14		16 +	14 +		do 75%																									44	x	5				WCY-ITC	(*)
D. Praca dyplomowa /egz. na oficera		164		27		164	513	677	8,5	6,5	20,5	27				100	64																										20		1	144		26		
D.I.1	Seminarium przeddyplomowe	20		1	ITT	20	5	25	0,5	0,8	0,2	1					20 +	do 75%																									20	+	1				WCY	(*)
D.I.2	Seminarium dyplomowe	44		4	ITT	44	58	102	3,5	1,7	2,3	4					44 +	do 75%																												44	+	4	WCY	(*)
D.I.3	Praca dyplomowa	100		22	ITT	100	450	550	4,5	4	18	22				100																														100	x	22	WCY	
D.I.4	Egzamin na oficera																																														E		SSW	
E. Praktyki zawodowe		400	400	16		400				16		16																100		4				100		4				100		4				100		4		
E.I.1	Praktyka d-cy drużyny	100	100	4		100				4		4																100	+	4																			CS/JW	
E.I.2	Praktyka d-cy plutonu	100	100	4		100				4		4																																		100	+	4	CS/JW	
E.I.3	Praktyka zawodowa	100	100	4	ITT	100				4		4																						100	+	4													CS/JW	
E.I.4	Szkolenie specjalistyczne	100	100	4	ITT	100				4		4																												100	+	4							CS/JW	
F. Inne													termin realizacji						Uwagi																															
F.I.1																																																		
	ogółem godzin / pkt. ECTS	5118	400	300		3836	3709	7145	143	152	148	300	1452	1918	1030	252	66		566		30	552		30	534		30	630		30	488		30	648		30	534		30	598		30	314		30	254		30		

ogółem godzin realizowanych w Centrach Szkolenia – w tym w CS

	I	II	III	IV	V	VI	VII	VIII	IX	X
dopuszczalny deficyt pkt. ECTS (w semestrze / łącznie)	15/15	18/18	15/25	15/25	15/25	15/25	15/25	15/25	15/25	15/25
rodzaje i liczba rygorów w semestrze: egzaminy (E, x)	3	4	4	3	4	3	4	3	3	2
zaliczenia z oceną (Zo, +)	15	14	12	13	10	13	11	12	6	1
zaliczenia bez oceny (Z, z)	6	10	4	2	2		4	2		
projekty przejściowe (P)										

* niepotrzebne skreślić, a arkusz dostosować pod względem programu dla profilu studiów.
** W - wykład, C - ćwiczenia, P - projekt, S - seminarium.

Obowiązuje kandydatów na żołnierzy zawodowych rozpoczynających kształcenie od roku akademickiego 2025/2026

Plan studiów uchwalony przez Senat WAT w dniu 25 września 2025 r.

8. PRZEDMIOTOWY PROGRAM STUDIÓW

8.1. Przedmioty modułu wojskowego

8.1.1. GRUPA TREŚCI KSZTAŁCENIA OGÓLNEGO A.I.

Ramowy opis przedmiotów

Przedmiot: A.I.1. DZIAŁALNOŚĆ WYCHOWAWCZA I PROFILAKTYKA DYSCYPLINARNA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
II	8					8		8				Z	O
IV	2	10				12		12				Zo	O
VII		10				10		10				Zo	O
Ogółem	10	20				30		30				Zo-2 Z-1	

Celem kształcenia jest ukształtowanie postaw i zachowań żołnierza – obywatela w mundurze oraz umiejętności w zakresie prowadzenia profilaktyki dyscyplinarnej i działalności wychowawczej w pododdziale.

Treści kształcenia:

System działalności wychowawczej w SZ RP. Kierunki działalności kulturalno-oświatowej w resorcie Obrony Narodowej. Ordery i odznaczenia państwowe i wojskowe. Order Krzyża Wojskowego. Wybrane zagadnienia z kształcenia obywatelskiego. Rodzaje, zasady oraz tryb udzielania wyróżnień. Reagowanie dyscyplinarne. Wymierzanie kar dyscyplinarnych i stosowanie środków dyscyplinarnych. Dyscyplinarne środki zapobiegawcze. Postępowanie dyscyplinarne. Postępowanie po uprawomocnieniu się orzeczenia. Dokumentacja i ewidencja dyscyplinarna. Analiza dyscypliny wojskowej na szczeblu pododdziału; działalność profilaktyczna ŻW. Podstawowe treści, formy i metody pracy profilaktycznej w pododdziale. Rozmowy indywidualne w pracy wychowawczej. Praca wychowawcza w działaniach bojowych. Rola etyki i moralności w życiu społecznym. Etyka żołnierska w tradycji oręża polskiego. Etyka żołnierska jako etyka zawodu. Moralny sens służby wojskowej. Moralność a dowodzenie. Etyka walki zbrojnej. *Kodeks Honorowy Żołnierza Zawodowego Wojska Polskiego*. Patologie społeczne jako zagrożenia dyscypliny wojskowej. Profilaktyka patologii społecznych w wojsku. Zagadnienia równości płci w warunkach służby wojskowej. Funkcjonowanie żołnierzy w środowisku

wielokulturowym. Równe traktowanie – przeciwdziałanie dyskryminacji z każdego powodu. Choroby XXI w. Rola dowódcy w kształtowaniu morale i nastrojów.

Opis efektów uczenia się:

Postawy patriotyczne, prospołeczne i moralno-etyczne oraz sposoby ich kształtowania; rozumienie systemu działalności wychowawczej w SZ RP; umiejętność posługiwania się oraz stosowania przepisów prawa w zakresie działalności wychowawczej w SZ RP; znajomość orderów i odznaczeń państwowych, rozumienie istoty honorowania Orderem Krzyża Wojskowego; umiejętność wykorzystywania informacji bieżącej do podnoszenia morale i nastrojów żołnierzy; umiejętność doboru tematyki zajęć kształcenia obywatelskiego do prowadzenia działalności wychowawczej w pododdziale; umiejętności i możliwości wykorzystywania form i metod działalności kulturalno-oświatowej w pracy wychowawczej; znajomość odpowiedzialności karnej i dyscyplinarnej oraz konsekwencji w przypadku naruszenia dyscypliny wojskowej; znajomość rodzajów, trybu oraz zasad udzielania wyróżnień, kar oraz środków dyscyplinarnych i dyscyplinarnych środków zapobiegawczych; znajomość zasad i przebiegu postępowania dyscyplinarnego; umiejętność prowadzenia analizy i oceny dyscypliny wojskowej w pododdziale; rozumienie istoty i podstawowych zagadnień etyki walki zbrojnej; definiowanie uniwersalnych norm moralnych w aspekcie zachowania się uczestników walki zbrojnej; rozumienie moralnych zasad zachowania się wobec chronionych osób i obiektów oraz moralnych powinności dowódcy w walce; umiejętności rozpoznawania oraz przeciwdziałania patologiom w życiu społecznym wojska; rozumienie istoty oraz kompleksowego podejścia do płci kulturowej; kształtowanie odpowiedzialności za własne zdrowie oraz edukację w zakresie unikania ryzykownych zachowań seksualnych.

Przedmiot: A.I.2. PODSTAWY KOMUNIKACJI STRATEGICZNEJ – TEORIA I PRAKTYKA

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
VIII	10	20				30		30				Zo	O
Ogółem	10	20				30		30				Zo-1	

Celem kształcenia jest przygotowanie do funkcjonowania we współczesnym środowisku informacyjnym oraz nauczenie poprawnej pod względem językowym wymiany informacji w formie ustnej i pisemnej.

Treści kształcenia:

Komunikacja strategiczna jako sposób zarządzania informacją – zadania, struktury, elementy. Poprawna polszczyzna. Zasady prostego języka. Autoprezentacja. Zasady prowadzenia dialogu i wystąpień publicznych. Współczesne media – informacja, manipulacja, dezinformacja. Polityka informacyjna MON. Zasady współpracy wojska z mediami. Sztuka komunikacji w sytuacjach kryzysowych. Budowanie spójnej narracji w czasie pokoju, kryzysu i wojny. Redagowanie komunikatów i informacji prasowych – case study. Prowadzenie mediów społecznościowych. Prawo prasowe i wewnętrzne regulacje resortu obrony narodowej. Treningi medialne – wywiad radiowy, wywiad telewizyjny. Organizacja wydarzeń medialnych - case study. StratCom w praktyce – koordynacja działań w środowisku informacyjnym. Wykorzystanie umiejętności przywódczych.

Opis efektów uczenia się:

Rozumienie podstawowych pojęć związanych z komunikacją strategiczną, istoty komunikacji strategicznej, jej funkcji i zdolności w czasie pokoju, kryzysu i wojny; rozumienie znaczenia środowiska informacyjnego w komunikacji strategicznej NATO i Sił Zbrojnych RP; znajomość zasad działania w środowisku informacyjnym; znajomość reguł językowych, stosowania zasad prostego języka oraz poprawnej polszczyzny; znajomość obowiązujących uregulowań prawnych oraz przepisów regulujących zasady informacji publicznej; znajomość zasad budowania strategii komunikowania się; umiejętność poprawnego artykułowania informacji, myśli i uczuć w formie ustnej i pisemnej; umiejętność wykorzystania zasad retoryki i metod erystyki w komunikacji; umiejętność wypowiadania się do mediów i współpracy z mediami; znajomość zasad realizacji polityki informacyjnej resortu; umiejętność nawiązywania kontaktów interpersonalnych; umiejętność opracowania planu organizacji i przebiegu wydarzenia medialnego; umiejętność rozpoznania, zdiagnozowania, rozwiązania i koordynacji sytuacji kryzysowych w komunikacji strategicznej.

Przedmiot: A.I.3. PRZYWÓDZTWO W DOWODZENIU

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
II	4	4				8		8				Z	O
III	6	16				22		22				E	O
Ogółem	10	20				30		30				E-1 Z-1	

Celem kształcenia jest opanowanie umiejętności przywództwa w pododdziale.

Treści kształcenia:

Istota i znaczenie przywództwa w dowodzeniu pododdziałem. Władza a przywództwo. Funkcje kierownicze dowódcy: planowanie, podejmowanie decyzji, organizowanie działań, kierowanie ludźmi i kontrolowanie. Tradycyjne i nowe koncepcje przywództwa. Zasady skutecznego przewodzenia. Kompetencje przywódcze. Reagowanie na niepożądane zachowania podwładnych. Techniki pracy z ludźmi: motywowania podwładnych, organizacji pracy zespołowej; delegowanie uprawnień; rozwiązywania konfliktów i negocjowania; gospodarowania czasem (własnym i podwładnych). Przywództwo w sytuacjach ekstremalnych. Przywództwo a kultura organizacyjna w wojsku. Proces doskonalenia zawodowego. Opiniowanie podwładnych. Praktyczne dowodzenie drużyną i plutonem w codziennym toku służby.

Opis efektów uczenia się:

Umiejętność skutecznego przywództwa w grupie formalnej i nieformalnej; znajomość technik zarządzania kapitałem ludzkim organizacji; umiejętność postawienia czytelnych zadań podwładnym według obowiązujących regulaminów; umiejętność kreowania własnego autorytetu w organizacji; zdolność zasad przejmowania inicjatywy i skutecznej realizacji zadań zespołowych; umiejętność opiniowania oraz sporządzania opinii służbowej; utożsamianie się z kulturą organizacyjną w wojsku oraz jej doskonalenie.

Przedmiot: A.I.4. HISTORIA SZTUKI WOJENNEJ

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
IV	10	10				20		20				Zo	O
Ogółem	10	10				20		20				Zo-1	

Celem kształcenia jest nabycie wiedzy historyczno-wojskowej o wojnie, jej zasadach i charakterze oraz sposobach prowadzenia walk, bitew, operacji.

Treści kształcenia:

Wojna w starożytności i średniowieczu. Wojskowość europejska w czasach nowożytnych (XVI-XVIII wiek). Strategia i taktyka w wojnach epoki napoleońskiej oraz w XIX w. Nowoczesna sztuka wojenna - od I wojny światowej do początku XXI wieku. Polskie doświadczenia wojenne z epoki walk o niepodległość i granice oraz z okresu II wojny światowej.

Opis efektów uczenia się:

Znajomość poglądów wybranych strategów na sztukę wojenną; umiejętność uzasadniania historycznego charakteru ewolucji zasad sztuki wojennej; uogólniania doświadczeń wojennych i stosowania wiedzy historyczno-wojskowej do rozwiązywania problemów dowodzenia na szczeblu taktycznym; umiejętność wykorzystywania wiadomości z historii w dobieraniu treści do szkolenia patriotycznego i obywatelskiego w pododdziale; umiejętność upowszechniania wiedzy historyczno-wojskowej w środowisku wojskowym i cywilnym; umiejętność interpretowania ważniejszych wydarzeń z historii wojskowości oraz korzystania z różnych źródeł wiedzy historyczno-wojskowej.

Przedmiot: A.I.5. HISTORIA POLSKI

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
I	16	14				30	20	50	1,2	0,8	2	E	O
Ogółem	16	14				30	20	50	1,2	0,8	2	E-1	

Celem kształcenia jest przekazanie przyszłym oficerom SZ RP wiedzy z zakresu historii Polski od X w. do XX w. ze szczególnym uwzględnieniem historii politycznej, wojskowości oraz społeczno-gospodarczych uwarunkowań.

Treści kształcenia:

Początki państwa polskiego, kryzys monarchii piastowskiej i odrodzenie Królestwa (X-XV wiek). „Złoty wiek" XVI i powstanie Rzeczypospolitej Obojga Narodów. Wojny Rzeczypospolitej w XVII wieku. Kryzys demokracji szlacheckiej i próby reformy państwa (XVIII wiek). Polska pod zaborami: powstania narodowe, polityka zaborców, narodziny nowoczesnych ruchów politycznych. Sprawa polska w czasie I wojny światowej. Odzyskanie Niepodległości i walki II RP o granice. Sukcesy i porażki Polski w okresie międzywojennym. Wrzesień 1939 r., początek okupacji i działalność Rządu RP na Uchodźstwie. Polacy na frontach II wojny światowej. Sprawa polska w czasie II wojny światowej: polityka aliantów zachodnich i Stalina, Powstanie Warszawskie. Budowa systemu komunistycznego i stalinizm w Polsce (1944-1956). Polska pod rządami PZPR, powstanie „Solidarności" i stan wojenny (1956-1989). Transformacja ustrojowa i początki III RP.

Opis efektów uczenia się:

Znajomość historii Polski od X do XX wieku; umiejętność definiowania podstawowych pojęć z historii Polski – opisywania i wyjaśnianie kluczowych procesów i wydarzeń historycznych; umiejętność analizy procesów historycznych ich genezy i konsekwencji; umiejętność weryfikacji i krytycznej analizy źródeł historycznych; umiejętność wykorzystania wiedzy w działalności wychowawczej, służbowej oraz w kontaktach ze społeczeństwem i żołnierzami armii sojuszniczych.

Przedmiot: A.I.6. OCHRONA INFORMACJI NIEJAWNYCH

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
II	4					4		4				Z	O
III	4	2				6		6				Zo	O
Ogółem	8	2				10		10				Zo-1 Z-1	

Celem kształcenia jest zapoznanie z przepisami dotyczącymi ochrony informacji niejawnych, w tym ochrony informacji niejawnych pochodzących z wymiany międzynarodowej oraz z zasadami ich bezpiecznego przetwarzania w różnych warunkach.

Treści kształcenia:

Dokumenty prawne oraz przepisy dotyczące ochrony informacji niejawnych w RP. Przepisy regulujące ochronę informacji niejawnych pochodzących z wymiany międzynarodowej. Ochrona informacji niejawnych organizacji międzynarodowych. Klasyfikacja informacji niejawnych, klauzule tajności. Klauzule materiałów niejawnych pochodzących z wymiany międzynarodowej oraz ich polskie odpowiedniki. Dostęp do informacji niejawnych, bezpieczeństwo osobowe. Obieg materiałów niejawnych – system kancelarii tajnych i kancelarii tajnych międzynarodowych. Ochrona fizyczna informacji niejawnych. Ochrona informacji niejawnych przetwarzanych w systemach teleinformatycznych. Bezpieczeństwo przemysłowe. Kontrola oraz nadzór nad przestrzeganiem przepisów i zasad dotyczących ochrony informacji niejawnych. Postępowanie z materiałami niejawnymi w przypadku zagrożenia lub ich ujawnienia. Ochrona informacji niejawnych w warunkach polowych oraz poza granicami państwa. Ochrona informacji niejawnych w warunkach kryzysu i wojny. Odpowiedzialność karna, dyscyplinarna i służbowa za naruszenie przepisów o ochronie informacji niejawnych.

Opis efektów uczenia się:

Znajomość obowiązujących przepisów prawa regulujących zasady ochrony informacji niejawnych, w tym ochrony informacji niejawnych pochodzących z wymiany międzynarodowej; umiejętność postępowania z materiałami niejawnymi, znajomość zasad ich bezpiecznego przetwarzania; umiejętność właściwego korzystania z niejawnych systemów teleinformatycznych; umiejętność postępowania z materiałami niejawnymi pochodzącymi z wymiany międzynarodowej; umiejętność przetwarzania materiałów niejawnych w warunkach polowych, poza granicami państwa oraz w przypadku zagrożenia.

Przedmiot: A.I.7. PROFILAKTYKA ANTYKORUPCYJNA

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
III	8					8		8				Z	O
Ogółem	8					8		8				Z-1	

Celem kształcenia jest nabycie wiedzy i umiejętności z zakresu tematyki antykorupcyjnej w tym nauczenie się prawidłowego funkcjonowania w środowisku narażonym na korupcję.

Treści kształcenia:

Podstawowe zagadnienia dotyczące korupcji, niekaralnych form korupcji i zjawiska konfliktu interesów. Mechanizmy socjologiczne i psychologiczne rządzące zjawiskiem korupcji i konfliktu interesów. Obszary zagrożeń korupcyjnych w SZ RP. Systemowe sposoby zapobiegania i walki z korupcją. Narzędzia antykorupcyjne wykorzystywane w resorcie obrony narodowej w zakresie przeciwdziałania korupcji i nadużyciom. Wewnętrzne mechanizmy obronne instytucji. Sposoby postępowania w przypadku zetknięcia się z korupcją i nadużyciem. Podmioty zaangażowane w wykrywanie korupcji oraz nadużyć. Konsekwencje korupcji. Rola żołnierza w zapobieganiu korupcji. Analiza przypadków i przykłady niepożądanych działań - warsztat.

Opis efektów uczenia się:

Znajomość podstawowych definicji dotyczących korupcji i zjawiska konfliktu interesów, okoliczności, w których może do nich dojść oraz karalnych i niekaralnych form korupcji; znajomość metod zapobiegania i walki z korupcją; znajomość zagrożeń korupcyjnych występujących w SZ RP oraz narzędzi antykorupcyjnych wykorzystywanych w resorcie obrony narodowej; znajomość możliwych do zastosowania przez instytucje wewnętrznych mechanizmów obrony przed korupcją i nadużyciami, konsekwencji korupcji oraz podmiotów zaangażowanych w wykrywanie korupcji i nadużyć; uświadomienie roli żołnierza w zapobieganiu korupcji oraz nabycie umiejętności postępowania w przypadku zetknięcia się z korupcją i nadużyciami.

Przedmiot: A.I.8. BEZPIECZEŃSTWO W CYBERPRZESTRZENI

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
I	4	6				10		10				Zo	O
Ogółem	4	6				10		10				Zo-1	

Celem kształcenia jest zbudowanie świadomości o zagrożeniach oraz przygotowanie do bezpiecznego funkcjonowania w cyberprzestrzeni.

Treści kształcenia:

Wprowadzenie do cyberbezpieczeństwa – zdefiniowanie podsatwowych zagrożeń (kradzież tożsamości, spam, phishing, smishing, spoofing, sniffing, cracking, deedpfake). Cyberprzestrzeń jako domena walki (wojna informacyjna, rola informacji i dezinformacji). System bezpieczeństwa sieci i systemów SZ RP. Bezpieczne korzystanie z sieci Internet. Bezpieczeństwo poczty elektronicznej. Bezpieczeństwo komunikatorów. Bezpieczne korzystanie z mediów społecznościowych. Bezpieczeństwo urządzeń mobilnych. Zasady bezpieczeństwa sieci i systemów.

Opis efektów uczenia się:

Znajomość podstawowych pojęć z zakresu cyberbezpieczeństwa i zagrożeń występujących w cyberprzestrzeni. Umiejętność bezpiecznego funkcjonowania w cyberprzestrzeni. Zrozumienie cyberprzestrzeni jako domeny walki. Umiejętność bezpiecznego korzystania z sieci Internet. Umiejętność konfigurowania ustawień bezpieczeństwa użytkownika dla podstawowych urządzeń i usług.

Przedmiot: A.I.9. BEZPIECZEŃSTWO I HIGIENA PRACY (BHP)

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
I	6					6		6				Z	O
Ogółem	6					6		6				Z-1	

Celem kształcenia jest zapoznanie z wybranymi regulacjami prawnymi, organizacją i metodyką szkolenia w zakresie bezpieczeństwa i higieny pracy oraz uświadomienie zagrożeń i przyczyn wypadków w służbie wojskowej.

Treści kształcenia:

Wybrane regulacje prawne z zakresu prawa pracy dotyczące BHP (dyrektywy UE, konwencje Międzynarodowej Organizacji Pracy (MOP), Kodeks pracy, przepisy resortu obrony narodowej). Organizacja i metodyka szkolenia żołnierzy w zakresie BHP z uwzględnieniem prowadzenia instruktażu stanowiskowego. Zagrożenia czynnikami szkodliwymi dla zdrowia, uciążliwymi i niebezpiecznymi podczas pełnienia czynnej służby wojskowej. Okoliczności i przyczyny charakterystycznych wypadków w związku z pełnieniem służby wojskowej. Tryb postępowania powypadkowego. Podstawy prawne w zakresie ochrony ppoż., systemy wykrywania pożarów, substancję palne i wybuchowe. Zapobieganie zagrożeniom pożarowym, postępowanie w czasie pożaru. Użycie podręcznego sprzętu gaśniczego, ewakuacja.

Opis efektów uczenia się:

Znajomość regulacji prawnych w zakresie BHP, zagrożeń czynnikami szkodliwymi uciążliwymi i niebezpiecznymi dla zdrowia; świadomość zagrożeń wypadkami podczas realizacji działalności służbowej; umiejętność prowadzenia instruktażu stanowiskowego; znajomość procedur postępowania powypadkowego.

8.1.2. GRUPA TREŚCI KSZTAŁCENIA KIERUNKOWEGO A.II.

Ramowy opis przedmiotów

Przedmiot: A.II.1. PODSTAWY DOWODZENIA

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
I	6	6				12		12				Z	O
II	4	8				12		12				Zo	O
Ogółem	10	14				24		24				Zo-1 Z-1	

Celem kształcenia jest wyposażenie podchorążych i słuchaczy w wiedzę z zakresu funkcjonowania systemu dowodzenia pododdziału.

Treści kształcenia:

Podstawowe pojęcia i definicje z zakresu dowodzenia. Organizacja dowodzenia. Czynności dowódcy pododdziału w procesie dowodzenia. Układ i treść zarządzenia, rozkazu i meldunku bojowego. Organizacja i prowadzenie rekonesansu – praca dowódcy w terenie. Wojskowe symbole graficzne. Dokumenty dowodzenia na szczeblu pododdziału. Środki dowodzenia. Sposoby opracowania dokumentów graficznych. Nanoszenie sytuacji taktycznej na mapie i szkicu działania. Ogólne zasady standaryzacji operacyjnej. Doktryny i architektura dokumentów doktrynalnych. Cel i istota After Action Review (AAR). Rodzaje omówień oraz specyfika AAR w rodzajach SZ RP. Planowanie, przygotowanie i przeprowadzenie AAR oraz zasady wdrażania zmian po omówieniu. Prowadzenie AAR w roli dowódcy plutonu.

Opis efektów uczenia się:

Znajomość podstawowych pojęć i definicji z zakresu dowodzenia; znajomość organizacji i środków dowodzenia na szczeblu pododdziału; rozumienie przedsięwzięć realizowanych w procesie dowodzenia; rozumienie toku postępowania podczas wypracowania decyzji; znajomość i umiejętność stosowania wojskowych symboli graficznych; znajomość układu i treści dokumentów dowodzenia wykonywanych na szczeblu pododdziału; znajomość architektury dokumentów doktrynalnych; znajomość celów i zasad realizacji AAR, świadomość roli dowódcy w procesie umożliwiającym poprawę realizacji procesu szkolenia (ćwiczeń).

Przedmiot: A.II.2. TAKTYKA

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
I	4	6				10		10				Z	O
II	4	6				10		10				Zo	O
III	2	6				8		8				Z	O
IV		12				12		12				E	O
Ogółem	10	30				40		40				Z-2 Zo-1 E- 1	

Celem kształcenia jest nabycie podstawowej wiedzy na temat organizacji i zasad prowadzenia działań taktycznych, struktur organizacyjnych i wyposażenia pododdziałów rodzajów wojsk oraz umiejętności stawiania zadań w walce.

Treści kształcenia:

Ogólna charakterystyka działań zbrojnych. Klasyfikacja działań taktycznych. Charakterystyka zasad i czynników walki. Podział, struktury organizacyjne i wyposażenie pododdziałów rodzajów SZ RP. Zasady użycia pododdziałów rodzajów wojsk w działaniach taktycznych. Prowadzenie działań taktycznych przez pododdziały rodzajów wojsk w różnorodnych środowiskach pola walki. Dowodzenie pododdziałem w różnorodnych środowiskach pola walki. Wykorzystanie bezzałogowych statków powietrznych w działaniach bojowych.

Opis efektów uczenia się:

Znajomość działań zbrojnych, zasad i czynników walki; podstawowa znajomość przeznaczenia, zadań oraz struktur organizacyjnych i wyposażenia pododdziałów rodzajów SZ RP; znajomość działań taktycznych oraz rozumienie zasad ich prowadzenia przez pododdziały rodzajów wojsk w różnorodnym środowisku walki; rozumienie zasad wykorzystania pododdziałów i ich możliwości bojowych w walce; podstawowe umiejętności dowodzenia pododdziałem w wybranych działaniach bojowych.

Przedmiot: A.II.3. PODSTAWY SURVIVALU

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
IV		22				22		22				Zo	O
Ogółem		22				22		22				Zo-1	

Celem kształcenia jest nauczenie metod zwiększenia szans na przeżycie oraz efektywności działania w warunkach środowiska naturalnego stosując techniki survivalowe.

Treści kształcenia:

Organizacja i funkcjonowanie systemu odzyskiwania izolowanego personelu w SZ RP i NATO. Budowa schronień oraz ogniska survivalowe. Techniki podawania lokalizacji z wykorzystaniem improwizowanych metod. Pozyskiwanie wody oraz zdobywanie i przygotowanie pożywienia. Wykorzystanie umiejętności przywódczych.

Opis efektów uczenia się:

Znajomość zasad, taktyki i techniki unikania zagrożeń; znajomość czynników fizjologicznych i ich wpływ na ograniczanie wydolności organizmu człowieka w sytuacji walki o przetrwanie, w różnych warunkach terenowych i klimatycznych; znajomość zasady, metody i formy ochrony własnej, budowy schronień poszukiwania i spożywania wody oraz pożywienia, umożliwiające doraźne utrzymanie się przy życiu oraz metod i technik ustalania własnego położenia (lokalizacji); znajomość teoretycznych podstaw prowadzenia standardowych „Bojowych Akcji Poszukiwawczo-Ratowniczych" (CSAR – Combat Search and Rescue) oraz „Akcji Bojowego Odzyskiwania" (CR – Combat Recovery); sposoby wykorzystania posiadanego wyposażenia osobistego w celu zwiększenia szans na przeżycie. Znajomość zasad wykorzystania sprzętu etatowego i nieetatowego sprzętu survivalowego; umiejętność przygotowania indywidualnego pakietu survivalowego oraz wyposażenia osobistego; znajomość zasad improwizacji w survivalu; umiejętność stosowania odpowiednich priorytetów w survivalu (ang. PLWF, P – protection, L – location, W – water, F – food); umiejętność budowania schronienia, ognisk survivalowych i utrzymania właściwego stanu higieny; znajomość zasad wykorzystania improwizowanych metod orientacji; umiejętność stosowania techniki pozyskania wody i pożywienia.

Przedmiot: A.II.4. GOTOWOŚĆ MOBILIZACYJNA I BOJOWA

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
II	6					6		6				Z	O
V	4	6				10		10				Zo	O
Ogółem	10	6				16		16				Zo-1 Z-1	

Celem kształcenia jest nabycie umiejętności definiowania podstawowych wskaźników i pojęć dotyczących gotowości mobilizacyjnej i bojowej oraz umiejętności kierowania procesem osiągania gotowości do podjęcia działań w pododdziale.

Treści kształcenia:

Geneza i rozwój systemu mobilizacyjnego wojska. Podstawowe wskaźniki i definicje dotyczące gotowości mobilizacyjnej i bojowej. Zasady utrzymania stałej i osiągania gotowości do podjęcia działań oraz stanów gotowości kryzysowej w pododdziale. Funkcjonowanie elementów bazy mobilizacyjnej. Dokumentacja osiągania gotowości do podjęcia działań na szczeblu pododdziału. Prowadzenie apelu ewidencyjnego w pododdziale. Kierowanie procesem osiągania gotowości do podjęcia działań po otrzymaniu sygnału w pododdziale oraz przez służbę nadrzędną.

Opis efektów uczenia się:

Znajomość podstawowych wskaźników i definicji dotyczących mobilizacji i utrzymania normatywów gotowości bojowej w pododdziale; znajomość zasad utrzymania stałej gotowości bojowej i osiągania gotowości do podjęcia działań oraz stanów gotowości kryzysowej; znajomość elementów bazy mobilizacyjnej; znajomość dokumentacji gotowości bojowej na szczeblu pododdziału. Kierowanie procesem osiągania gotowości do podjęcia działań w pododdziale.

Przedmiot: A.II.5. ROZPOZNANIE I ARMIE INNYCH PAŃSTW

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
I	4	4				8		8				Z	O
II	4	6			2	12		12				Zo	O
Ogółem	8	10			2	20		20				Z-1 Zo-1	

Celem kształcenia jest zrozumienie roli rozpoznania wojskowego, typologii, sposobów i zasad prowadzenia rozpoznania znajomość struktur organizacyjnych i uzbrojenia wybranych armii innych państw szczebla batalionu oraz nabycie podstawowych umiejętności w organizowaniu i prowadzeniu rozpoznania wzrokowego.

Treści kształcenia:

Rola rozpoznania wojskowego we współczesnych konfliktach zbrojnych. Typologia rozpoznania wojskowego. Zasadnicze zadania rozpoznania wojskowego. Zasady prowadzenia działań rozpoznawczych na szczeblu pododdziału. Znaki rozpoznawcze innych państw. Struktury organizacyjne i uzbrojenie wybranych armii innych państw do szczebla batalionu. Obiekty rozpoznania. Cechy demaskujące użycia uzbrojenia w działaniach bojowych. Przygotowanie pododdziału do prowadzenia rozpoznania. Sposoby prowadzenia rozpoznania przez pododdział. Prowadzenie rozpoznania w punkcie obserwacyjnym. Noktowizja i termowizja w prowadzeniu rozpoznania. Prowadzenie rozpoznania z wykorzystaniem bezzałogowych statków powietrznych.

Opis efektów uczenia się:

Rozumienie podstawowych pojęć z zakresu rozpoznania wojskowego; rozumienie roli rozpoznania wojskowego podczas organizacji i prowadzenia walki; znajomość struktur organizacyjnych i uzbrojenia jednostek organizacyjnych wybranych armii innych państw; znajomość poglądów na temat prowadzenia działań bojowych przez jednostki organizacyjne armii innych państw, znajomość cech demaskujących obiekty rozpoznania; znajomość wybranych sylwetek sprzętu i znaków rozpoznawczych wybranych armii innych państw znajomość sposobów prowadzenia rozpoznania; umiejętność stawiania zadań i prowadzenia rozpoznania w punkcie obserwacyjnym; umiejętność obsługi wybranych indywidualnych urządzeń noktowizyjnych i termowizyjnych.

Przedmiot: A.II.6. TOPOGRAFIA WOJSKOWA

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
I	6	14				20		20				Zo	O
VIII	4	16				20		20				E	O
Ogółem	10	30				40		40				Zo-1 E-1	

Celem kształcenia jest nabycie wiedzy i umiejętności w zakresie wykorzystania elementów składowych terenu i wiedzy na ich temat do prowadzenia działań na współczesnym polu walki, tj. orientowanie się w terenie bez mapy, pracę z mapą, wykorzystanie prostych przyrządów i urządzeń nawigacyjnych (busola, kompas, odbiorniki globalnego systemu nawigacji satelitarnej (GNSS) będących na wyposażeniu SZ RP w działaniach taktycznych oraz podstaw obsługi systemów informacji geograficznej (GIS).

Treści kształcenia:

Charakterystyczne formy rzeźby terenu i obiekty terenowe (naturalne i antropogeniczne) oraz ich właściwości taktyczne. Pomiary w terenie. Orientowanie się w terenie bez mapy w dzień i w nocy. Przygotowanie i wykonanie marszu wg azymutu. Wydawnictwa kartograficzne (mapy papierowe i cyfrowe) i ich charakterystyka. Układy współrzędnych i wojskowe systemy meldunkowe. Znaki umowne map topograficznych. Pomiary na mapach topograficznych. Wykorzystanie mapy podczas pracy w terenie. Orientowanie się w terenie wg mapy i przyrządów nawigacyjnych. Przyrządy i urządzenia nawigacyjne wykorzystywanie w pododdziałach rodzajów wojsk. Współczesne systemy informacji przestrzennej (oprogramowanie komercyjne, przeglądarki internetowe , Serwer Informacji i Usług Geograficznych GEOSERWER). Fotointerpretacja danych obrazowych.

Opis efektów uczenia się:

Umiejętność wykonywania pomiarów różnymi sposobami; umiejętność posługiwania się mapą w różnych warunkach terenowych (papierową i cyfrową, mapą topograficzną i ortofotomapą); umiejętność orientowania się w terenie z mapą i bez mapy; umiejętność przygotowania i wykonania marszu wg azymutu; wykorzystanie przyrządów i urządzeń nawigacyjnych w działaniach taktycznych wojsk; umiejętność prowadzenia orientacji topograficznej oraz oceny terenu; znajomość podstawowego oprogramowania (PGO, darmowe przeglądarki GIS); umiejętność korzystania z danych geograficznych dostępnych w sieci teleinformatycznej MILNET-Z.

Przedmiot: A.II.7. ZABEZPIECZENIE LOGISTYCZNE DZIAŁAŃ TAKTYCZNYCH

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
II	8					8		8				Z	O
VII		8				8		8				Z	O
Ogółem	8	8				16		16				Z-2	

Celem kształcenia jest znajomość istoty i przedmiotu logistyki wojskowej oraz zasad organizacji zabezpieczenia logistycznego pododdziału w działaniach taktycznych na polu walki oraz zasad funkcjonowania terytorialnego systemu zabezpieczenia, a także zasad, obowiązków i przedsięwzięć realizowanych w ramach wsparcia wojsk sojuszniczych przez państwo-gospodarza.

Treści kształcenia:

Istota i zadania logistyki wojskowej; podział i zadania systemu funkcjonalnego logistyki Sił Zbrojnych RP; struktura i funkcjonowanie terytorialnego systemu zabezpieczenia SZ RP; podział zadań i kompetencji pomiędzy WOG/jednostką pełniącą funkcję WOG a JW w zakresie realizacji zabezpieczenia logistycznego i finansowego; zabezpieczenie materiałowe i techniczne na szczeblu pododdziału; organizacja, wyposażenie i możliwości taktyczne pododdziałów logistycznych; zasady planowania i organizacji transportu i ruchu wojsk; systemy informatyczne wykorzystywane w logistyce SZ RP; zasady planowania i realizacja zadań wynikających z obowiązków państwa-gospodarza; ogólne zasady współpracy z układem pozamilitarnym w zakresie realizacji zadań wynikających z obowiązku państwa-gospodarza; rola punktów kontaktowych HNS w procesie wsparcia państwa-gospodarza; zasadnicze zadania i dokumenty podczas planowania i realizacji HNS; ogólne zasady współdziałania w zakresie logistyki wielonarodowej.

Opis efektów uczenia się:

Znajomość istoty, celów i treści logistyki wojskowej oraz struktur systemu logistycznego SZ RP; rozumienie funkcjonowania gospodarki wojskowej; znajomość podstaw zabezpieczenia logistycznego działań taktycznych na szczeblu pododdziału; znajomość struktur, przeznaczenia oraz zasad użycia pododdziałów logistycznych; znajomość programów informatycznych wspierających proces zabezpieczenia logistycznego; znajomość założeń i zadań normujących problematykę HNS w państwie; znajomość dokumentacji normującej proces planowania i realizacji zadań wynikających z obowiązków państwa-gospodarza.

Przedmiot: A.II.8. SZKOLENIE STRZELECKIE

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
I	2	12				14		14				Zo	O
II	1	15				16		16				Zo	O
III	2	6				8		8				Zo	O
IV	1	9				10		10				Zo	O
V	2	6				8		8				Zo	O
VI	1	9				10		10				Zo	O
VII		12				12		12				Zo	O
VIII	1	9				10		10				Zo	O
Ogółem	10	78				88		88				Zo-8	

Celem kształcenia jest zrozumienie istoty działania broni strzeleckiej, amunicji i granatów ręcznych, nabycie umiejętności ich wykorzystania w walce oraz planowania, organizowania i prowadzenia szkolenia strzeleckiego.

Treści kształcenia:

Budowa i działanie podstawowych rodzajów broni strzeleckiej, amunicji i granatów ręcznych. Podział i znakowanie amunicji. Wybrane elementy teorii strzału i balistyki. Zasady strzelania z broni strzeleckiej. Warunki bezpieczeństwa podczas użytkowania i obchodzenia się z bronią i amunicją. Ćwiczenia w obserwacji w ocenie odległości określanych różnymi sposobami. Przyrządy celownicze i celowniki do broni strzeleckiej. Ćwiczenia przygotowawcze z broni strzeleckiej oraz z wykorzystaniem urządzeń szkolno-treningowych (UST). Ćwiczenia w rzucaniu granatami ręcznymi. Strzelania z broni strzeleckiej. Planowanie, przygotowanie i prowadzenie zajęć ze szkolenia strzeleckiego. Przystrzeliwanie broni strzeleckiej. Organizacja i doprowadzanie broni strzeleckiej do prawidłowej celności. Zacięcia broni strzeleckiej w czasie strzelania – charakterystyka zacięć, ich przyczyny i sposób usunięcia. Rzut granatem bojowym. Konfiguracja oporządzenia. Przygotowanie i obsługa broni do/po strzelaniu. Postawy strzeleckie: stojąc, klęcząc, leżąc z mocnej i słabej strony. Wymiana magazynka sposobem awaryjnym i taktycznym. Zwroty w miejscu z bronią w postawie strzeleckiej stojąc, klęcząc i leżąc.

Opis efektów uczenia się:

Rozumienie istoty działania broni strzeleckiej, amunicji i granatów ręcznych; definiowanie i rozpoznawanie znakowania amunicji strzeleckiej; umiejętność prowadzenia celnego ognia z broni strzeleckiej; definiowanie i stosowanie warunków bezpieczeństwa podczas

obchodzenia się z bronią i amunicją, a także podczas strzelań i rzutu granatem bojowym; umiejętność prowadzenia obserwacji oraz wykrywania, rozpoznania, oraz określania odległości do obiektów za pomocą wzoru rozwarcia i innymi sposobami, umiejętność prowadzenia ognia z pistoletu, i karabinka; umiejętność rzucania granatem bojowym oraz organizowania i prowadzenia szkolenia na rzutni granatem w roli kierownika zajęć; rozumienie zasad i norm przystrzeliwania broni oraz umiejętność doprowadzenia broni strzeleckiej do prawidłowej celności; umiejętność planowania, organizowania i prowadzenia zajęć dowódcy - kierownika zajęć oraz organizowania i prowadzenia szkolenia w roli instruktora w punkcie nauczania, umiejętność skonfigurowania swojego oporządzenia w zależności od zadania, rozkładania i składania etatowego uzbrojenia, prawidłowego przyjmowania postaw strzeleckich: stojąc, klęcząc, leżąc z mocnej i słabej strony, prowadzenia celnego i powtarzalnego ognia z pistoletu wojskowego, karabinka szturmowego i pistoletu maszynowego zza, spod i znad przesłony (z mocnej i słabej strony) do celów stałych, ukazujących się i ruchomych w postawie strzeleckiej stojąc, klęcząc i leżąc, w dzień i w nocy, wymiany magazynka sposobem awaryjnym i taktycznym, wykonywania zwrotów w miejscu z bronią w postawie strzeleckiej stojąc, klęcząc i leżąc, obserwowania wyników prowadzonego ognia oraz nanoszenia poprawek, wykonywania strzelań sprawdzających/sytuacyjnych z broni strzeleckiej (PW, kbs i PM).

Przedmiot: A.II.9. SYSTEM ŁĄCZNOŚCI I ŚRODKI DOWODZENIA

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
II	4	6				10		10				Zo	O
III	4	6				10		10				Zo	O
Ogółem	8	12				20		20				Zo-2	

Celem kształcenia jest nabycie wiedzy z zakresu organizacji łączności na poziomie taktycznym, sposobów wykorzystania i posługiwania się środkami łączności i informatyki będącymi na wyposażeniu pododdziału oraz przepisów korespondencji radiowej.

Treści kształcenia:

Podstawowe zagadnienia z zakresu systemów łączności i informatyki. Organizacja systemów łączności na poziomie taktycznym oraz sposoby wykorzystania sprzętu łączności i informatyki w działaniach bojowych (w tym również zautomatyzowane systemy dowodzenia i kierowania środkami walki). Zasadniczy sprzęt łączności i informatyki będący na wyposażeniu SZ RP (dane taktyczno-techniczne, zastosowanie). Zasady organizacji

systemów łączności i sposoby wykorzystywania sprzętu łączności i informatyki (w tym również zautomatyzowane systemy dowodzenia i kierowania środkami walki). Przepisy korespondencji radiowej i ogólne zasady zarządzania częstotliwościami radiowymi w SZ RP. Bezpieczeństwo i ochrona systemów teleinformatycznych. Posługiwanie się wybranymi środkami wsparcia dowodzenia (łączności oraz zautomatyzowanymi systemami dowodzenia i kierowania środkami walki) będącymi na wyposażeniu pododdziału.

Opis efektów uczenia się:

Umiejętność praktycznego wykorzystania technicznych możliwości środków łączności i informatyki w zależności od rodzaju wykonywanych działań bojowych pododdziału; znajomość zasad organizacji dokumentów eksploatacyjnych łączności oraz obowiązujących przepisów w zakresie eksploatacji sprzętu łączności i informatyki; umiejętność przygotowania i praktycznego posługiwania się środkami łączności i informatyki będącymi na wyposażeniu pododdziału oraz przekazywania komend (sygnałów) i wymiana wiadomości.

Przedmiot: A.II.10. DZIAŁALNOŚĆ SZKOLENIOWA I SZKOLENIOWO METODYCZNA

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
I	4	2				6		6				Zo	O
II	4	6				10		10				Zo	O
V	6	8				14		14				Zo	O
VI	2	8				10		10				Zo	O
Ogółem	16	24				40		40				Zo-4	

Celem kształcenia jest przygotowanie kandydatów na oficerów do planowania, organizowania i realizacji szkolenia oraz działalności metodycznej w pododdziale.

Treści kształcenia:

Rola dydaktyki w szkoleniu wojskowym. Podstawowe pojęcia szkolenia wojskowego. Organizacja systemu szkolenia w jednostce wojskowej. System działalności szkoleniowo - metodycznej w SZ RP. Zasady dydaktyczne. Formy działalności szkoleniowo-metodycznej w pododdziale. Formy i metody szkolenia w pododdziale. Formy organizacyjne zajęć. Modele instruowania. Dokumentacja szkoleniowo-metodyczna i ewidencja w procesie szkolenia pododdziału. Działalność szkoleniowa i szkoleniowo-metodyczna dowódcy w pododdziale. Przygotowanie rejonu zajęć i ich zabezpieczenie materiałowo-techniczne. Tok zajęć teoretycznych i praktycznych. Rola, miejsce oraz zadania kierownika zajęć oraz

instruktorów w procesie planowania, organizowania oraz realizowania szkolenia w pododdziale. Formułowanie celów szkolenia. Dobór treści szkolenia. Kontrola i ocena w procesie szkolenia. Przygotowanie i prowadzenie szkolenia w punkcie nauczania do zajęć z przedmiotów szkolenia bojowego. Prowadzenie instruktażu w roli kierownika zajęć z przedmiotów szkolenia bojowego. Planowanie, organizowanie i realizacja zajęć w roli kierownika zajęć z przedmiotów szkolenia bojowego. Przygotowanie i prowadzenie zajęć instruktorsko-metodycznych i metodycznych zajęć grupowych. Kształcenie na odległość - E-learning. Organizacja i funkcjonowanie Systemu Wykorzystania Doświadczeń w SZ RP (SWD).

Opis efektów uczenia się:

Znajomość organizacji systemu szkolenia w jednostce wojskowej i pododdziale; rozumienie roli, miejsca oraz zadań osób funkcyjnych w zakresie szkolenia plutonu (drużyny); umiejętność identyfikowania nowoczesnych metod szkolenia z uwzględnieniem ich efektywności; umiejętność wykonywania i prowadzenia dokumentacji szkoleniowej, ewidencyjnej oraz metodycznej w plutonie; rozumienie stosowania różnorodnych form działalności szkoleniowo-metodycznej w profesjonalnym przygotowaniu dowódców i instruktorów do szkolenia; umiejętność korzystania z wojskowych wydawnictw specjalistycznych; umiejętność dobierania elementów bazy szkoleniowej oraz środków dydaktycznych do wymogów procesu szkolenia, umiejętność prowadzenia szkolenia w roli instruktora oraz planowania, organizowania i prowadzenia zajęć w pododdziale z wykorzystaniem różnorodnych form szkolenia, form organizacyjnych zajęć; umiejętność przygotowania i prowadzenia instruktaży i innych form działalności szkoleniowo – metodycznej na szczeblu plutonu; znajomość organizacji i funkcjonowania SWD w SZ RP; rozumienie miejsca i roli personelu oraz użytkowników SWD w procesie wykorzystania doświadczeń.

Przedmiot: A.II.11. MIĘDZYNARODOWE PRAWO HUMANITARNE KONFLIKTÓW ZBROJNYCH (MPHKZ)

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
VII	10	10				20		20				E	O
Ogółem	10	10				20		20				E-1	

Celem kształcenia jest dostarczenie niezbędnej wiedzy wymaganej do realizacji zadań zgodnie z MPHKZ oraz nabycie zdolności koniecznych do właściwego zastosowania i odpowiedniego reagowania podczas prowadzenia działań zbrojnych.

Treści kształcenia:

Geneza i rozwój prawa wojennego. Główne założenia i zasady MPHKZ (definicja MPHKZ, źródła MPHKZ a zasady użycia siły (ROE), MPHKZ a prawo krajowe). Międzynarodowy Ruch Czerwonego Krzyża i Czerwonego Półksiężyca. Pojęcie kombatanta, osoby uprawnione do statusu kombatanta. Pojęcie neutralności wojennej. Obowiązki państw neutralnych. Ochrona i uprawnienia jeńców wojennych. Ochrona rannych, chorych i rozbitków. Ochrona ludności cywilnej. Metody i środki walki w świetle MPHKZ. Środki prowadzenia zbrojnych działań wojennych objęte zakazem badań, produkcji, posiadania i handlu. Środki objęte zakazem użycia, środki walki, których użycie jest dopuszczalne pod pewnymi warunkami. Ograniczenia w zakresie stosowania dopuszczalnych środków walki zbrojnej, metody prowadzenia działań zbrojnych – dozwolone i zakazane. Ochrona dóbr kultury. MPHKZ a konflikty wewnętrzne. Znaki i oznaczenia stosowane w MPHKZ. Odpowiedzialność za naruszania MPHKZ (zbrodnie wojenne, zbrodnie przeciwko ludności, zbrodnie ludobójstwa, odpowiedzialność dowódców za naruszenia prawa wojennego, działanie na rozkaz).

Opis efektów uczenia się:

Rozumienie znaczenia MPHKZ w działaniach wojsk; umiejętność postępowania zgodnie z celem międzynarodowego prawa humanitarnego; znajomość norm humanitarnego postępowania w działaniach zbrojnych i umiejętność egzekwowania takiego zachowania od swoich podwładnych; podejmowanie decyzji w zakresie prowadzenia działań zbrojnych zgodne z MPHKZ.

Przedmiot: A.II.12. WYBRANE ZAGADNIENIA BEZPIECZEŃSTWA NARODOWEGO I MIĘDZYNARODOWEGO

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
VII	8	12				20		20				Zo	O
Ogółem	8	12				20		20				Zo-1	

Celem kształcenia jest znajomość istoty bezpieczeństwa narodowego i międzynarodowego oraz struktur i instytucji zajmujących się bezpieczeństwem narodowym i międzynarodowym.

Treści kształcenia:

Globalne problemy bezpieczeństwa. Narody Zjednoczone i porozumienia regionalne. Procesy rozbrojeniowe i mechanizmy kontroli zbrojeń. Obszary porozumień rozbrojeniowych istotnych dla bezpieczeństwa globalnego. Misje specjalne i operacje wojskowe w systemie bezpieczeństwa. Problemy bezpieczeństwa regionalnego. NATO i UE wobec zagrożeń globalnych i regionalnych. System obrony państwa. Elementy systemu bezpieczeństwa Rzeczypospolitej Polskiej (RP). Przesłanki bezpieczeństwa narodowego RP. Strategia obronności. Prawno - organizacyjne podstawy systemu obronnego RP. Polska w systemie sojuszniczym NATO. Operacje poza granicami Polski. Udział SZ RP w międzynarodowej współpracy wojskowej. Podstawowe pojęcia dotyczące operacji pokojowych i stabilizacyjnych. Typologia operacji pokojowych i stabilizacyjnych. Charakter zadań wykonywanych przez polskie kontyngenty wojskowe podczas udziału w misjach pokojowych i stabilizacyjnych. Zasady użycia siły w działaniach pokojowych i stabilizacyjnych. Podstawowe zasady i sposoby wykonywania zadań mandatowych.

Opis efektów uczenia się:

Rozumienie istoty bezpieczeństwa państw; znajomość podstawowych zasad jego funkcjonowania; rozumienie funkcjonowania systemu obrony państwa; zrozumienie procesów zachodzących w jego systemie politycznym oraz w życiu społeczno-politycznym; zapoznanie z funkcjonowaniem i strukturami współczesnych instytucji europejskich i międzynarodowych w dobie procesów integracyjnych; znajomość podstawowych terminów dotyczących operacji pokojowych i stabilizacyjnych; znajomość typologii operacji pokojowych i stabilizacyjnych; znajomość doświadczeń SZ RP z udziału w operacjach pokojowych i stabilizacyjnych; znajomość sposobów i zasad działania w czasie wykonywania zadań mandatowych.

Przedmiot: A.II.13. PODSTAWY EKSPLOATACJI SPRZĘTU WOJSKOWEGO (SpW)

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
VI	6	8				14		14				Zo	O
Ogółem	6	8				14		14				Zo-1	

Celem kształcenia jest znajomość zasad i bezpieczeństwa eksploatacji sprzętu wojskowego oraz nabycie umiejętności prowadzenia gospodarki materiałowo-technicznej w pododdziale.

Treści kształcenia:

Podstawowy sprzęt wojskowy SZ RP. Podstawowe pojęcia związane z eksploatacją SpW. Bezpieczeństwo eksploatacji SpW (w tym bezpieczeństwo energetyczne, dozorowe metrologiczne, ekologiczne, ppoż. i inne). Przepisy dotyczące użytkowania SpW. Obowiązki osób funkcyjnych w zakresie zapewnienia bezpieczeństwa eksploatacji SpW oraz oszczędnego i racjonalnego zużycia paliw i energii. Obowiązki kierowcy i dysponenta pojazdu. Działalność profilaktyczna w zakresie zapobiegania wypadkom z bronią i amunicją oraz ruchu drogowym z udziałem wojskowych pojazdów mechanicznych. Odpowiedzialność żołnierzy za wyrządzone przez nich szkody w SpW. Zasady prowadzenia gospodarki materiałowo-technicznej w pododdziale. Przyjęcie i przekazanie sprzętu w pododdziale. Podstawowe zadania dowódcy pododdziału w zakresie eksploatacji i użytkowania sprzętu wojskowego. Prowadzenie działalności kontrolno-nadzorczej w pododdziale. Wykorzystanie umiejętności przywódczych.

Opis efektów uczenia się:

Rozumienie zasad eksploatacji SpW; rozumienie przestrzegania przepisów dotyczących bezpieczeństwa eksploatacji SpW; umiejętność identyfikowania przyczyn oraz zapobiegania wypadkom z bronią i amunicją oraz w ruch drogowym; znajomość zasad prowadzenia gospodarki materiałowo-technicznej oraz zasad przyjęcia i przekazania sprzętu w pododdziale; znajomość zadań w zakresie właściwego użytkowania sprzętu, planowania, organizowania i prowadzenia działalności kontrolno-nadzorczej.

Przedmiot: A.II.14. DZIAŁANIA NIEKINETYCZNE

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
VIII	4	6				10		10				Z	O
Ogółem	4	6				10		10				Z-1	

Celem kształcenia jest znajomość podstawowych terminów, zasad i sposobów prowadzenia działań niekinetycznych wykonywanych przez pododdziały i komórki sztabowe w zakresie współpracy cywilno-wojskowej, działań informacyjnych i psychologicznych.

Treści kształcenia:

Założenia współpracy cywilno-wojskowej (CIMIC), cele, funkcje, zasady i zadania. CIMIC jako funkcja połączona. Znajomość efektów i działań współpracy cywilno-wojskowej oraz jej zastosowania w różnych środowiskach i rodzajach działań. Zasady i sposoby oceny

środowiska cywilnego. Cele i zadania organizacji cywilnych (międzynarodowych, rządowych i pozarządowych) w rejonie odpowiedzialności dowódcy oraz ich wpływ na realizację zadań operacyjnych dowódcy. Charakter i zasady kooperacji personelu współpracy cywilno-wojskowej z ludnością lokalną, administracją terenową i organizacjami cywilnymi wpływającymi na realizację zadań i opinię o siłach zbrojnych. Podstawowe pojęcia dotyczące działań informacyjnych i psychologicznych (PSYOPS i INFOOPS). Systematyzacja pojęć i zdefiniowanie obszarów działania w środowisku informacyjnym w relacji z poziomami dowodzenia. Koordynacja działań informacyjnych na poszczególnych szczeblach dowodzenia. Doświadczenia z wykorzystania pododdziałów CIMIC i PSYOPS w działaniach. Rola komórek działań niekinetycznych w procesie planowania działań.

Opis efektów uczenia się:

Znajomość podstawowych terminów dotyczących współpracy cywilno-wojskowej, działań informacyjnych i psychologicznych. Znajomość roli, przeznaczenia i możliwości realizacji zadań w obszarach CIMIC, INFOOPS i PSYOPS zintegrowanych z działaniami bojowymi.

Przedmiot: A.II.15. OCHRONA ŚRODOWISKA

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
V	4	4				8		8				Z	O
Ogółem	4	4				8		8				Z-1	

Celem kształcenia jest opanowanie wiedzy na temat postępowania z zanieczyszczeniami, odpadami, materiałami i substancjami niebezpiecznymi a także zasadami ochrony środowiska podczas realizacji celów i zadań wojskowych.

Treści kształcenia:

Charakterystyka środowisk przyrodniczych i ich elementów chronionych. Zagrożenia dla środowiska wynikające z zagrożeń militarnych i niemilitarnych oraz niekorzystne czynniki oddziaływujące na środowisko. Główne zagrożenia dla środowiska naturalnego związane z techniką motoryzacyjną oraz środkami walki. Postępowanie z odpadami i substancjami niebezpiecznymi. Zagospodarowanie produktów odpadowych powstających w wyniku eksploatacji oraz likwidacji uzbrojenia i sprzętu wojskowego, w tym pojazdów. Ochrona środowiska przez pododdziały na poligonach, ośrodkach ćwiczeń i w działaniach taktycznych.

Opis efektów uczenia się:

Znajomość współczesnych poglądów na ochronę środowiska naturalnego; świadomość i znajomość zagrożeń militarnych i niemilitarnych środowiska naturalnego; znajomość zasad postępowania z zanieczyszczeniami, odpadami, materiałami i substancjami niebezpiecznymi; umiejętność przestrzegania zasad ochrony środowiska podczas realizacji zadań wojskowych.

Przedmiot: A.II.16. OBRONA POWIETRZNA

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
I	4	6				10		10				Zo	O
IV	4	4				8		8				Zo	O
Ogółem	8	10				18		18				Zo-2	

Celem kształcenia jest umiejętność określania istoty, celu, podziału i zasad powszechnej OPL, potencjału bojowego (rodzaj/typ, liczba, prawdopodobne uzbrojenie/wyposażenie) środków napadu powietrznego (ŚNP) oraz ich wpływ na działanie pododdziałów.

Treści kształcenia:

Podział i charakterystyka militarnych zagrożeń powietrznych. Zadania, skład oraz możliwości bojowe lotnictwa taktycznego i śmigłowców bojowych. Działanie samolotów i śmigłowców na polu walki. Rola, zadania, możliwości bojowe oraz struktura organizacyjna oddziałów i pododdziałów wojsk obrony przeciwlotniczej. Zasady ogólne powszechnej obrony przeciwlotniczej. Organizacja systemu powszechnego ostrzegania i alarmowania o zagrożeniu uderzeniami z powietrza. Przedsięwzięcia powszechnej obrony przeciwlotniczej. Zasady organizacji powszechnej obrony przeciwlotniczej w miejscach stałego i czasowego pobytu. Działanie stanu osobowego pododdziału po ogłoszeniu alarmu powietrznego. Realizacja przedsięwzięć POPL w działaniach taktycznych. Bezzałogowe statki powietrzne. Wykorzystanie bezzałogowych statków powietrznych w działaniach taktycznych. Kinetyczne i niekinetyczne sposoby walki z bezzałogowymi statkami powietrznymi.

Opis efektów uczenia się:

Znajomość organizacji oraz możliwości bojowych pododdziałów obrony przeciwlotniczej; znajomość zasad organizacji POPL w warunkach polowych i garnizonowych, w tym odpowiedniego przygotowania infrastruktury; rozumienie znaczenia przedsięwzięć organizowanych w ramach POPL dla zmniejszenia skutków uderzeń z powietrza

wykonywanych przez przeciwnika; umiejętność określania wielkości i charakteru zagrożenia z powietrza oraz jego wpływu na działanie pododdziału; umiejętność organizowania w pododdziałach przedsięwzięć POPL oraz realizowania ich w działaniach bojowych. Znajomość zastosowania bezzałogowych statków powietrznych w działaniach taktycznych oraz prowadzenia z nimi walki.

Przedmiot: A.II.17. OBRONA PRZED BRONIĄ MASOWEGO RAŻENIA

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
I	4	6				10		10				Zo	O
VI	4	16				20		20				Zo	O
Ogółem	8	22				30		30				Zo-2	

Celem kształcenia jest znajomość właściwości rażącego działania broni masowego rażenia i środków zapalających, istoty oraz celu OPBMR, praktycznego działania i wykorzystania środków i sprzętu OPBMR w warunkach zagrożenia skażeniami i skażeń oraz organizacji i prowadzenia szkolenia z OPBMR w pododdziale.

Treści kształcenia:

Wpływ broni masowego rażenia na działania bojowe wojsk. Organizacja OPBMR na szczeblu taktycznym. Wykorzystanie zasad i przedsięwzięć OPBMR w warunkach zagrożenia skażeniami i skażeń. Posługiwanie się indywidualnymi środkami ochrony przed skażeniami. Sprawdzenie szczelności i dopasowania filtracyjnych masek przeciwgazowych w atmosferze skażonej. Sprzęt i środki OPBMR będące na wyposażeniu pododdziału. Poziomy zagrożenia od broni i urządzeń CBRN, stopnie gotowości ISOPS. Działanie po napotkaniu terenu skażonego i w terenie skażonym - prowadzenie natychmiastowej likwidacji skażeń. Ochrona wojsk przed środkami zapalającymi, pokonanie przeszkód na torze napalmowym. Środki dymne, wykonywanie zasłon dymnych z wykorzystaniem ręcznych granatów lub świec dymnych. Szkolenie z ochrony przed bojowymi środkami trującymi i substancjami promieniotwórczymi. Planowanie i rozgrywanie epizodów z OPBMR w ramach prowadzonych zajęć taktycznych. Ochrona środowiska naturalnego i bezpieczeństwo pracy podczas szkolenia z OPBMR.

Opis efektów uczenia się:

Znajomość rażącego działania broni masowego rażenia oraz wykorzystania zasad i przedsięwzięć OPBMR przed, w czasie i po zdarzeniach CBRN (chemical, biological, radiological and nuclear); umiejętność sprawdzania szczelności i dopasowania filtracyjnych

masek przeciwgazowych w atmosferze skażonej; podejmowanie działania na sygnał uprzedzenia o zagrożeniu skażeniami i alarmu o skażeniach oraz umiejętne wykorzystywanie właściwości indywidualnych i zbiorowych środków ochrony przed skażeniami; umiejętność posługiwania się i wykorzystania środków i sprzętu OPBMR będącego na wyposażeniu pododdziału; umiejętność działania po napotkaniu terenu skażonego środkami trującymi i promieniotwórczymi; umiejętność prowadzenia natychmiastowej likwidacji skażeń; umiejętność zachowania się na Punkcie Likwidacji Skażeń; znajomość właściwości środków zapalających; umiejętność stawiania zasłon dymnych za pomocą ręcznych granatów lub świec dymnych; umiejętność zachowania zasad bezpieczeństwa i ochrony środowiska podczas szkolenia z OPBMR.

Przedmiot: A.II.18. POŁĄCZONE WSPARCIE OGNIOWE

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
VI	8	10				18		18				Zo	O
Ogółem	8	10				18		18				Zo-1	

Celem kształcenia jest nabycie ogólnej wiedzy i świadomości w zakresie roli i zasad połączonego wsparcia ogniowego, relacji wsparcia ogniowego wojsk rakietowych i artylerii oraz lotnictwa, możliwości bojowych pododdziałów artylerii oraz roli targetingu w połączonym wsparciu ogniowym.

Treści kształcenia:

Zadania i struktura połączonego wsparcia ogniowego. Rola i zadania artylerii we wsparciu ogniowym. Bliski ogień wspierający. Możliwości i sposoby wykorzystania sił i środków połączonego wsparcia ogniowego na korzyść pododdziałów wojsk walczących. Wezwanie wsparcia ogniowego z pola walki (Call For Fire). Koordynacja wsparcia ogniowego na szczeblu pododdziału. Planowanie i wykonanie bliskiego ognia wspierającego. Rola i zadania Lotnictwa Wojsk Lądowych oraz Lotnictwa Sił Powietrznych we wsparciu ogniowym pododdziałów ogólnowojskowych w różnych rodzajach działań taktycznych. Wywołanie bezpośredniego wsparcia lotniczego (Close Air Suport). Możliwości w połączonym wsparciu ogniowym. Śmigłowcowe wsparcie ogniowe (Close Combat Attack). Rola bezzałogowych statków powietrznych we wsparciu ogniowym wojsk.

Opis efektów uczenia się:

Znajomość przeznaczenia, miejsca i zadań połączonego wsparcia ogniowego oraz jego znaczenia w realizacji zadań przez wojska walczące; rozumienie zasad i sposobów

wykorzystania artylerii w działaniach taktycznych pododdziałów wojsk walczących; znajomość istoty oraz sposobu wykorzystania lotnictwa na korzyść pododdziałów wojsk walczących; znajomość istoty targetingu w połączonym wsparciu ogniowym; znajomość procedury śmigłowcowego wsparcia ogniowego (Close Combat Attack); znajomość procedury wsparcia ogniowego z pola walki (Call For Fire).

Przedmiot: A.II.19. ZABEZPIECZENIE INŻYNIERYJNE

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
II	6	4				10		10				Zo	O
III		10				10		10				Zo	O
Ogółem	6	14				20		20				Zo-2	

Celem kształcenia jest nabycie wiedzy w zakresie przeznaczenia i zadań zabezpieczenia inżynieryjnego realizowanego w pododdziale oraz umiejętności realizacji podstawowych zadań zabezpieczenia inżynieryjnego.

Treści kształcenia:

Cel i zadania zabezpieczenia i wsparcia inżynieryjnego pododdziałów. Struktury, przeznaczenie i zasady użycia pododdziałów wojsk inżynieryjnych. Koordynacja działań pododdziałów wojsk inżynieryjnych z pododdziałami wspieranymi. Sposoby organizacji i realizacji podstawowych zadań inżynieryjnych na szczeblu pododdziału: rozpoznanie inżynieryjne przeciwnika i terenu, budowa obiektów fortyfikacyjnych, budowa zapór inżynieryjnych i wykonywanie niszczeń, przygotowanie i utrzymanie dróg, wykonywanie przejść (torowanie) w zaporach, przez przeszkody naturalne i rejony zniszczeń oraz rozminowanie terenu i obiektu, urządzanie i utrzymanie przepraw, realizacja przedsięwzięć w ramach maskowania, udział w likwidacji skutków uderzeń przeciwnika oraz klęsk żywiołowych i ekologicznych, wydobywanie i oczyszczanie wody, usuwanie i niszczenie niewybuchów i niewypałów, w tym improwizowanych ładunków wybuchowych. Dowodzenie podczas realizacji procedury 5-25 oraz 5xC. Inżynieryjne systemy bezzałogowe.

Opis efektów uczenia się:

Znajomość: celów, zadań i zasad zabezpieczenia i wsparcia inżynieryjnego działań taktycznych; znajomość sposobów wykonywania podstawowych zadań inżynieryjnych na szczeblu pododdziału; celów i zadań wsparcia inżynieryjnego pododdziałów rodzajów

wojsk; znajomość struktur, przeznaczenia i zasad użycia pododdziałów wojsk inżynieryjnych; znajomość min oraz materiałów wybuchowych i środków zapalających stosowanych w SZ RP; umiejętność sporządzania zapalnika lontowego i wysadzanie pojedynczego ładunku materiału wybuchowego; umiejętność zachowania się w rejonach zagrożenia minami oraz IED (Improvised Explosive Device); umiejętność realizacji procedur 5-25 oraz 5xC.

Przedmiot: A.II.20. ZABEZPIECZENIE MEDYCZNE

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
II	6	4				10		10				Zo	O
V	2	18				20		20				E	O
Ogółem	8	22				30		30				Zo-1 E-1	

Celem kształcenia jest uzyskanie wiedzy i umiejętności w zakresie organizacji zabezpieczenia medycznego pododdziału.

Treści kształcenia:

Ogólna charakterystyka zabezpieczenia medycznego SZ RP. Zabezpieczenie medyczne pododdziału do szczebla batalionu. Założenia taktyczno-medyczne opieki nad poszkodowanym w warunkach pola walki (Tactical Combat Casualty Care – TCCC). Posługiwanie się indywidualnym wyposażeniem medycznym żołnierza (Indywidualny Pakiet Medyczny – IPMEd) podczas udzielania samopomocy i pomocy koleżeńskiej na polu walki. Sposoby ewakuacji poszkodowanych. Zasady prowadzenia ewakuacji medycznej – MEDEVAC. Procedury CASEVAC. Improwizowane sposoby wynoszenia rannych z pola walki. Postępowanie w przypadku wystąpienia masowych strat sanitarnych MASCAL. Zabezpieczenie medyczne działań taktycznych przez pododdziały rodzajów wojsk w różnorodnych środowiskach pola walki. Systemy bezzałogowe w ewakuacji medycznej.

Opis efektów uczenia się:

Znajomość zasad zabezpieczenia medycznego pododdziału. Założeń taktyczno-medycznych i standardów medycznych TCCC, faz i celów udzielania taktycznej pomocy medycznej. Znajomość czynności wykonywanych w ramach samopomocy i pomocy koleżeńskiej na polu walki w poszczególnych fazach TCCC; znajomość IPMed oraz umiejętność posługiwania się nim; umiejętność oceny obrażeń i stanu rannego; umiejętność

udrażniania dróg oddechowych oraz oceny i kontroli oddechu poszkodowanego; umiejętność rozpoznawania, tamowania i zaopatrywania krwotoków z użyciem dostępnych opatrunków, zaopatrywania amputacji urazowych kończyn; znajomość zasad i umiejętność rozpoznania oraz postępowania z ranami klatki piersiowej, unieruchamiania złamań; umiejętność zgłoszenia potrzeby ewakuacji medycznej; znajomość sposobów ewakuacji poszkodowanych przy użyciu sprzętu medycznego oraz środków improwizowanych.

Przedmiot: A.II.21. REGULAMINY SZ RP

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
I	4	6				10		10				Zo	O
II	2	8				10		10				Zo	O
VII		6				6		6				Z	O
VIII		8				8		8				Zo	O
Ogółem	6	28				34		34				Z-1 Zo-3	

Celem kształcenia jest opanowanie postanowień i zarządzeń regulujących tok życia i służby w jednostce wojskowej oraz umiejętności stosowania regulaminów w codziennym toku służby, a także przygotowanie do planowania, organizacji i prowadzenia szkolenia z regulaminów.

Treść kształcenia:

Podstawowe uwarunkowania służby wojskowej. Organizacja życia żołnierskiego w jednostce wojskowej. Działalność służbowa w jednostce wojskowej i garnizonie. Wzory dokumentów. Służba wewnętrzna jednostki wojskowej. Musztra indywidualna i zespołowa piesza. Musztra z pojazdami. Sygnały dowodzenia stosowane w musztrze. Dowodzenie pododdziałem podczas wystąpień służbowych i uroczystości wojskowych. Opracowanie dokumentacji szkoleniowej do zajęć z regulaminów w roli instruktora i kierownika zajęć. Udział w instruktażu kierownika zajęć. Organizacja i prowadzenie instruktażu. Przygotowanie i prowadzenie szkolenia w roli dowódcy drużyny – instruktora. Planowanie, organizowanie i prowadzenie zajęć z regulaminów w roli kierownika zajęć. Działalność służbowa w jednostce wojskowej. Wybrane zagadnienia z Ceremoniału Wojskowego SZ RP. Przegląd musztry pododdziału.

Opis efektów uczenia się:

Umiejętność stosowania zapisów regulaminów w codziennym toku służby; opanowanie zasad żołnierskiego zachowania się w różnych sytuacjach; znajomość postępowania służbowego, codziennego toku służby, zabezpieczenia logistycznego, ochrony ppoż i zdrowia; znajomość służb wewnętrznych i służb garnizonowych, dokumentacji służb wewnętrznych, organizacji i pełnienia służby wartowniczej, patrolowej i konwojowej; umiejętność zdawania i obejmowania obowiązków na stanowiskach służbowych; opanowanie czynności wchodzących w zakres musztry indywidualnej i zespołowej pieszej do szczebla plutonu oraz z pojazdami; umiejętność dowodzenia pododdziałem podczas wystąpień służbowych i uroczystości wojskowych; wydawania komend i zachowania się w szyku, planowania, organizowania i prowadzenia zajęć z regulaminów w roli instruktora i kierownika zajęć; umiejętność przygotowania i realizacji przeglądu musztry plutonu; znajomość zadań stojących przed służbami w jednostce wojskowej i garnizonie.

8.1.3. B.I. GRUPA TREŚCI KSZTAŁCENIA SPORTOWO-JĘZYKOWEGO

Ramowy opis przedmiotów

Przedmiot: B.I.1. JĘZYK ANGIELSKI

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
I		60				60	15	60	2,4	0,6	3	Zo	O
II		60				60	15	60	2,4	0,6	3	Zo	O
III		60				60	15	60	2,4	0,6	3	Zo	O
IV		60				60	15	60	2,4	0,6	3	Zo	O
V		60				60	15	60	2,4	0,6	3	Zo	O
VI		60				60	15	60	2,4	0,6	3	E-B2 Stanag 2222	O
VII		60				60	15	60	2,4	0,6	3	Zo	O
VIII		60				60	15	60	2,4	0,6	3	Zo	O
Ogółem		480				480	120	600	19,2	4,8	24	Zo-7 E-1	

Celem kształcenia jest udoskonalenie umiejętności receptywnych (czytanie, słuchanie) zgodnie z porozumieniem standaryzacyjnym NATO STANAG 6001 i osiągnięcie kwalifikacji językowych potwierdzonych Standardowym Profilem Językowym

(SPJ 3 2 3 2) z egzaminu zgodnego z porozumieniem standaryzacyjnym NATO STANAG 6001.

Treści kształcenia:

I. Tematyka wojskowa
Stopnie wojskowe i podstawowe systemy broni wszystkich rodzajów sił zbrojnych.

2. Rodzaje sił zbrojnych i służb:
   - podstawowa organizacja wybranego rodzaju sił zbrojnych/rodzajów sił zbrojnych;
   - wyposażenie i uzbrojenie żołnierzy wybranego rodzaju wojsk i służb;
   - systemy uzbrojenia wybranego rodzaju wojsk i służb.

- Służba wojskowa:
  - kształcenie i szkolenie w siłach zbrojnych;
  - kariera zawodowa w wojsku;
  - instrukcje i dokumenty.
- Ćwiczenia wojskowe:
  - działania bojowe i szkolno-bojowe;
  - ćwiczenia międzynarodowe;
  - C4I – Command, Control, Communication, Computers, Inteligence;
  - elementy rozkazu.
- Międzynarodowa współpraca wojskowa:
  - NATO i praca poza granicami państwa;
  - międzynarodowe jednostki wojskowe;
  - misje pokojowe i humanitarne;
  - działania w ramach porozumień rozbrojeniowych.
- Bron masowego rażenia:
  - działanie broni masowego rażenia;
  - umowy międzynarodowe;
  - bieżące wydarzenia wojskowo-polityczne.
- Podstawowe skróty w dokumentach wojskowych.
- Korespondencja służbowa – w formie pisanej i przez techniczne środki łączności.
- Bieżące wydarzenia polityczne i militarne na świecie.

II. Tematyka ogólna
1. Stosunki międzyludzkie i społeczeństwo
2. Środowisko
3. Polityka wewnętrzna i międzynarodowa
4. Kultura oraz kultura anglosaskiego obszaru kulturowego

Opis efektów uczenia się:

Po zrealizowaniu programu uczący się powinni osiągnąć następujące kwalifikacje językowe:
1. w zakresie sprawności receptywnych uczący się powinni:
a. Rozumieć rozmowy użytkowników języka angielskiego mówiących językiem ludzi wykształconych, charakteryzujące się występowaniem złożonych struktur języka i obszernym zakresem słownictwa ogólnego oraz słownictwa specjalistycznego;
b. Czytać ze zrozumieniem teksty nie adaptowane, dotyczące różnych dziedzin życia społecznego oraz specjalistyczne, w tym korespondencje, instrukcje i zarządzenia wojskowe;

c. Poprawnie rozpoznawać ładunek emocjonalny wypowiedzi.
2. w zakresie sprawności produktywnych uczący się powinni:
a. Wypowiadać się płynnie i spójnie w odniesieniu do spraw ogólnych, ogólnowojskowych oraz specjalistycznych, związanych z własna specjalnością zawodową;
b. Wypowiadać się pisemnie na znane tematy ogólne i zawodowe, precyzyjnie przekazując zamierzone treści oraz tworzyć podstawową korespondencję specjalistyczną.

Przedmiot: B.I.2. WYCHOWANIE FIZYCZNE

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
I		60				60		60				Zo	O
II		60				60		60				Zo	O
III		60				60		60				Zo	O
IV		60				60		60				Zo	O
V		60				60		60				Zo	O
VI		60				60		60				Zo	O
VII	10	60				70		70				Zo	O
VIII		60				60		60				Zo	O
IX		60				60		60				Zo	O
X		10				10		10				E	O
Ogółem	10	550				560		560				Zo-9 E-1	

Celem przedmiotu jest przygotowanie kandydatów do wykonywania zawodu oficera, zapewniające skuteczne ich działanie w warunkach bojowych i podczas pokojowego funkcjonowania Sił Zbrojnych RP. Ponadto, realizacja programu zapewni kandydatom na oficerów nabycie specyficznej, dla wychowania fizycznego, wiedzy i umiejętności związanych ze służbą wojskową, wpłynie na kształtowanie podstawowych zdolności motorycznych oraz kompetencji społecznych niezbędnych do objęcia pierwszego stanowiska służbowego. Treści programowe obejmują realizację szkolenia specjalistycznego z wychowania fizycznego i sportu dla żołnierzy dobrowolnej zasadniczej służby wojskowej oraz żołnierzy zawodowych w trakcie kształcenia na jednolitych studiach magisterskich, zgodnie z wytycznymi zawartymi w *„Decyzji nr 158/MON Ministra obrony narodowej z dnia 11 maja 2015 r. w sprawie realizacji szkolenia specjalistycznego z wychowania fizycznego i sportu w resorcie obrony narodowej.”* Ukończenie szkolenia specjalistycznego zapewni uczestnikom nabycie odpowiedniej wiedzy oraz właściwych

umiejętności niezbędnych do uzyskania uprawnień do prowadzenia zajęć z wychowania fizycznego i sportu w resorcie obrony narodowej pod nadzorem merytorycznym żołnierza zawodowego lub pracownika wojska zajmującego etatowe stanowisko służbowe związane z wykonywaniem zadań z zakresu wychowania fizycznego i sportu.

Treści kształcenia:

Teoria wychowania fizycznego i sportu, atletyka terenowa i specjalistyczne ćwiczenia na torach przeszkód, gimnastyka i ćwiczenia siłowe, walka wręcz, pływanie i ratownictwo wodne, piłka siatkowa, piłka koszykowa, piłka nożna, zajęcia sportowe z różnych dyscyplin sportu i rekreacji ruchowej.

Opis efektów uczenia się:

W wyniku opanowania treści programowych przedmiotu kandydat powinien uzyskać następujące kompetencje - efekty kształcenia w zakresie:

1. wiedzy:
- definiuje pojęcia z zakresu nauk o kulturze fizycznej, w szczególności w zakresie wychowania fizycznego i sportu,
- opisuje budowę i funkcje organizmu człowieka,
- wyjaśnia metody oceny stanu sprawności fizycznej,
- charakteryzuje zasady promocji zdrowia i zdrowego trybu życia,
- opisuje mechanizm działania i wpływ aktywności ruchowej na człowieka,
- rozpoznaje prawne, organizacyjne i etyczne uwarunkowania wykonywania działalności służbowej z wychowania fizycznego i sportu,
- wyjaśnia metodykę prowadzenia zajęć z walki wręcz, ćwiczeń na torach przeszkód, ćwiczeń siłowych, atletyki terenowej,
- zna obowiązujące normy sprawności fizycznej przewidziane dla żołnierzy zawodowych,
- charakteryzuje organizację i sposoby przeprowadzenia zawodów sportowych,
- wyjaśnia zasady zapobiegania urazom i wypadkom podczas zajęć z wychowania fizycznego.

2. umiejętności:
- posługiwania się techniczną, manualną i ruchową sprawnością związaną ze specyfiką służby wojskowej,
- posługiwania się podstawowym sprzętem i aparaturą stosowaną w czasie zajęć programowych i sportowych, treningów sportowych oraz zawodów sportowo-rekreacyjnych,
- komunikowania się z grupą szkoleniową podczas realizacji zajęć z wychowania fizycznego i sportu,
- wykorzystywania technik informacyjnych w celu pozyskiwania i przechowywania danych,
- korygowania błędów i zaniedbań w praktyce szkoleniowej,
- prowadzenia dokumentacji szkoleniowej z wychowania fizycznego i sportu,
- planowania, projektowania i realizacji działania z zakresu wychowania fizycznego i sportu, z uwzględnieniem obowiązujących norm oraz dostępnych warunków,
- posługiwania się specjalistyczną sprawnością ruchową z zakresu wybranych form aktywności fizycznej w zależności od wymogów określonych na zajmowanym stanowisku służbowym,
- posługiwania się sprawnością fizyczną umożliwiającą wykonanie norm szkoleniowych z wychowania fizycznego,
- rozwiązywania najczęstszych problemów związanych z procesem dydaktycznym

i treningowym,
- formułowania opinii i ocen dotyczących ćwiczących i grup szkoleniowych w kontekście związanym z wychowaniem fizycznym i sportem,
- realizowania zadania w sposób zapewniający bezpieczeństwo własne i szkolonych, w tym przestrzega zasady bezpieczeństwa służby i pracy.

3. kompetencji społecznych:
- rozumie potrzebę kształcenia się przez całe życie,
- współdziała i pracuje w grupie, przyjmując w niej różne role,
- określa priorytety służące realizacji określonego przez siebie lub innych zadania,
- rozwiązuje najczęstsze problemy związane z procesem dydaktycznym i treningowym,
- realizuje zadania w sposób zapewniający bezpieczeństwo własne i otoczenia, w tym przestrzega zasad bezpieczeństwa służby i pracy,
- formułuje opinie i oceny dotyczące ćwiczących i grup szkoleniowych w kontekście związanym z wychowaniem fizycznym i sportem,
- dba o sprawność fizyczną niezbędną dla wykonywania zadań właściwych dla działalności zawodowej związanej z pełnioną funkcją w środowisku wojskowym.

Przedmiot: B.I.3. OBÓZ JĘZYKOWY - JĘZYK ANGIELSKI

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	symulator	seminarium	łącznie							
IV		**30**				**30**		**30**				**Z**	**O**
Ogółem		**30**				**30**		**30**				**Z-1**	

Celem kształcenia jest udoskonalenie umiejętności receptywnych (czytanie, słuchanie) i produktywnych (pisanie, mówienie) zgodnie z porozumieniem standaryzacyjnym NATO STANAG 6001 i osiągnięcie Standardowego Profilu Językowego 2 2 2 2 z egzaminu zgodnego z porozumieniem standaryzacyjnym NATO STANAG 6001.

Treści kształcenia:

Służba wojskowa:
- kształcenie i szkolenie w siłach zbrojnych;
- kariera zawodowa w wojsku;
- operacje połączonych rodzajów sił zbrojnych.

Strategie pisania: notatka: służbowa, instruująca, decyzyjna; raport; list z zapytaniem o informację.

Doskonalenie formalnych i nieformalnych sposobów komunikowania się.
Opis efektów uczenia się:

Utrwalenie umiejętności słuchania i czytania na poziomie 2. zgodnie z porozumieniem standaryzacyjnym NATO STANAG 6001.
Rozwinięcie umiejętności mówienia i pisania na poziomie 2. zgodnie z porozumieniem standaryzacyjnym NATO STANAG 6001.

8.2. Przedmioty modułu kierunkowego

8.2.1. GRUPA TREŚCI PRZEDMIOTÓW KSZTAŁCENIA OGÓLNEGO C.I.

Ramowy opis przedmiotów

Przedmiot: C.I.1. WPROWADZENIE DO STUDIOWANIA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						Niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
I	6					6	8	14	0,2	0,3	0,5	Zo	O
Ogółem	6					6	8	14	0,2	0,3	0,5	Zo-1	

Cele kształcenia: Zapoznanie studenta z nowoczesnymi metodami studiowania, a także umożliwienie mu zdobycia umiejętności niezbędnych w studiowaniu, takich jak: umiejętność samodzielnego uczenia się, autoprezentacji, wystąpień publicznych, naukowej dyskusji, odpowiedzialnej pracy w zespole, studiowania literatury naukowej, tworzenia sprawozdań z badań, inicjowania zagadnień do studiowania, rozwijania postawy badawczej i twórczej, a także zarządzania swoim czasem oraz radzenia sobie ze stresem – zatem tych wszystkich elementów wiedzy oraz umiejętności i kompetencji, które wymagane są w trakcie realizacji innych przedmiotów.

Treści kształcenia: Przedmiot ma ułatwić studentowi pokonanie trudności, pojawiających się na początku studiów w związku z koniecznością zmiany szkolnego stylu uczenia się na akademicki styl samodzielnego zdobywania wiedzy oraz nabywania umiejętności i kompetencji. Treści kształcenia obejmują metodykę nowoczesnego studiowania, metody i techniki efektywnego uczenia się oraz nowoczesne techniki wspomagające proces studiowania.

Efekty uczenia się: Zna i rozumie istotę i charakter studiowania oraz profesjonalizmu zawodowego w zakresie wybranego kierunku studiów. Zna i rozumie podstawowe pojęcia

związane ze studiami w szkole wyższej. Zna podstawowe zasady indywidualnej i zespołowej pracy naukowej oraz przedstawiania jej efektów. Zna podstawowe metody i techniki efektywnego uczenia się. Potrafi diagnozować uwarunkowania przebiegu procesu studiowania. Potrafi planować własną ścieżkę rozwoju oraz stosować wiedzę w zakresie zarządzania czasem i radzenia sobie ze stresem. Potrafi prezentować osiągnięte efekty kształcenia i wyniki własnej pracy badawczej. Jest świadomy rangi i znaczenia studiów dla osobistego rozwoju i indywidualnej ścieżki kariery. Jest świadomy potrzeby rozwijania umiejętności uczenia się, planowania własnej pracy, prezentowania jej rezultatów. Jest świadomy potrzeby uczenia się przez całe życie.

Przedmiot: C.I.2. OCHRONA WŁASNOŚCI INTELEKTUALNYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
I	12	2				14	13	27	0,5	0,5	1	Zo	O
Ogółem	12	2				14	13	27	0,5	0,5	1	Zo-1	

Cele kształcenia: Wprowadzenie do problematyki ochrony własności intelektualnej.

Treści kształcenia: Historia ochrony własności przemysłowej w Polsce i na świecie. Międzynarodowe organizacje ochrony własności intelektualnych. Ochrona patentowa, wzory użytkowe i wzory przemysłowe. Znaki towarowe, oznaczenia geograficzne, znaki handlowe i usługowe. Topografie układów scalonych. Postępowanie przed Urzędem Patentowym RP. Procedury, opłaty, rejestry. Prawo autorskie i prawa pokrewne – Copyright.

Efekty uczenia się: Zna i rozumie podstawowe pojęcia i zasady z zakresu ochrony własności przemysłowej i prawa autorskiego, potrafi korzystać z zasobów informacji patentowej. Ma wiedzę ogólną niezbędną do rozumienia społecznych, ekonomicznych, prawnych, finansowych, marketingowych i innych pozatechnicznych uwarunkowań działalności inżyniera logistyka. Potrafi – przy formułowaniu i rozwiązywaniu zadań obejmujących projektowanie systemów i procesów logistycznych – dostrzegać ich aspekty pozatechniczne, w tym środowiskowe, organizacyjne, ekonomiczne i prawne. Potrafi dokonać krytycznej oceny posiadanej wiedzy, a także dostrzega jej znaczenie w rozwiązywaniu problemów poznawczych i praktycznych.

Przedmiot: C.I.3. WPROWADZENIE DO INFORMATYKI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						Niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
I	16		22			38	38	76	1,5	1,5	3	Zo	O
Ogółem	16		22			38	38	76	1,5	1,5	3	Zo-1	

Cele kształcenia: Przedstawienie oraz nauczenie studenta przygotowania i wykorzystania komputerów oraz oprogramowania w dydaktyce i pracy. Wykłady prezentują zagadnienia zarówno ogólne teoretyczne, jak również praktyczne szczegóły w wybranych zagadnieniach. W ramach zajęć laboratoryjnych w wybranym środowisku operacyjnym, na określonym przez prowadzącego pakiecie biurowym i środowisku programowania realizowane są zadania ilustrujące treści wykładu.

Treści kształcenia: Wprowadzenie do architektury i funkcjonowania współczesnych komputerów. Podstawy sieci komputerowych oraz sieci Internet. Systemy operacyjne z rodzin Windows oraz Linux – funkcje i zadania. Standardy, formaty i programy komputerowe dla elektronicznych dokumentów biurowych. Edytory tekstu – wybrane funkcje oraz zastosowania. Arkusze kalkulacyjne. Oprogramowanie do prezentacji multimedialnych. Pakiety obróbki grafiki. Wprowadzenie do baz danych. Modele i standardy gromadzenia oraz przetwarzania danych. Podstawy programowania w językach wysokiego poziomu. Wprowadzenie w semantykę i syntaktykę wybranego języka programowania wysokiego poziomu.

Efekty uczenia się: Zna i rozumie podstawowe pojęcia z zakresu podstaw informatyki. Zna możliwości i zasady praktycznego wykorzystania technologii informatycznych w nauce, badaniach i gospodarce. Ma podstawową wiedzę z zakresu języków programowania komputerów. Umie wykorzystywać podstawowe narzędzia i oprogramowanie do komunikowania się, gromadzenia i przetwarzania danych. Ma kompetencje z zakresu wykorzystywania podstawowych narzędzi informatycznych wspomagających procesy gromadzenia, dokumentowania i prezentacji informacji.

Przedmiot: C.I.4. PODSTAWY ZARZĄDZANIA I PRZEDSIĘBIORCZOŚCI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
V	18	16				34	30	64	1,3	1,2	2,5	Zo	O
Ogółem	18	16				34	30	64	1,3	1,2	2,5	Zo-1	

Cele kształcenia: Przekazanie wiedzy teoretycznej i praktycznej w zakresie podstaw zarządzania we współczesnych przedsiębiorstwach; wprowadzenie studentów w podstawowe zagadnienia problematyki współczesnego zarządzania oraz zapoznanie z mechanizmami funkcjonowania organizacji; przedstawienie najważniejszych metod i narzędzi wsparcia przedsiębiorczości w Polsce.

Treści kształcenia: Przedmiot oraz kierunki rozwoju nauki o organizacji i zarządzania. Aktualne wyzwania teorii i praktyki zarządzania. Organizacja jako system. Zarządzanie i jego funkcje. Współczesny menedżer i warunki jego sukcesu. Organizacja pracy własnej menedżera. Planowanie jako funkcja menedżerska. Podejmowanie decyzji. Rutynowe i twórcze metody rozwiązywania problemów. Organizowanie działań. Tradycyjne i nowoczesne struktury organizacyjne Techniki organizatorskie. Zarządzanie personelem. Przywództwo kierownicze. Style kierowania. System motywowania w organizacji i techniki motywacyjne. Zarządzanie zmianami organizacyjnymi. Zarządzanie informacją. Komunikowanie się w organizacji. Zarządzanie wiedzą w organizacji. Techniki negocjacji. Nowoczesne metody i techniki zarządzania. Kontrola jako funkcja menedżerska.

Efekty uczenia się: Student ma podstawową wiedzę teoretyczną dotyczącą nauki o zarządzaniu i jej interdyscyplinarnym charakterze. Ma teoretyczną wiedzę o istocie, działaniu i przekształceniach różnych struktur i instytucji społecznych, w szczególności przedsiębiorstw i organizacji publicznych oraz identyfikuje i wyjaśnia różnice między poszczególnymi typami organizacji. Ma podstawową wiedzę dotyczącą uwarunkowań współczesnego zarządzania, w szczególności o: globalizacji, postępie technologicznym, nowych wymiarach konkurencyjności, znaczeniu środowiska naturalnego, przekształceniach społeczno-kulturowych oraz o przedsiębiorczości. Zna istotę zarządzania oraz zasady realizowania głównych funkcji procesu zarządzania organizacjami: planowania, organizowania, zarządzania zasobami ludzkimi oraz kontrolowania. Potrafi dokonać obserwacji i interpretacji otaczających go zjawisk humanistycznych, prawnych i społecznych. Potrafi przeprowadzić analizę otoczenia organizacji i sformułować na jej podstawie adekwatne rekomendacje do działania. Student potrafi realizować podstawowe

przedsięwzięcia menedżerskie z zakresu planowania, organizowania, kierowania ludźmi i kontrolowania. Ma świadomość znaczenia społecznych skutków działań prowadzonych przez rożnego typu organizacje oraz posiada świadomość odpowiedzialności za kształtowanie relacji z innymi. Rozumie wagę decyzji menedżerskich w stosunku do pracowników, podmiotów współpracujących z organizacją oraz klientów. Student rozumie potrzebę kształcenia ustawicznego. Potrafi wyrażać własne opinie dotyczące problemów z zakresu zarządzania oraz przekonywać do własnych racji poprzez odpowiednie merytoryczne argumentowanie.

8.2.2. GRUPA TREŚCI PRZEDMIOTÓW KSZTAŁCENIA PODSTAWOWEGO C.II.

Ramowy opis przedmiotów

Przedmiot: C.II.1. WPROWADZENIE DO METROLOGII

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						Niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
I	18	20				38	38	76	1,5	1,5	3	Zo	O
Ogółem	18	20				38	38	76	1,5	1,5	3	Zo-1	

Cele kształcenia: Zapoznanie studentów z podstawami metrologii, posługiwaniem się przyrządami kontrolno-pomiarowymi oraz zasadami ich nadzoru.

Treści kształcenia: Miejsce i rola metrologii jako interdyscyplinarnego obszaru wiedzy we współczesnym społeczeństwie. Definicje podstawowych pojęć z zakresu metrologii. Istota podstawowych metod pomiarowych. Budowa oraz przeznaczenie podstawowych wzorców i przyrządów pomiarowych wielkości fizycznych. Błędy i niepewność pomiaru.

Efekty uczenia się: Student zna podstawy metrologii, podstawowe przyrządy pomiarowe i metody pomiarów wielkości fizycznych, zna metody rachunku błędów i zasady opracowania wyników pomiarów oraz szacowania niepewności. Student ma podstawową wiedzę dotyczącą nadzorowania przyrządów pomiarowych w systemach zarządzania jakością. Student potrafi interpretować uzyskane wyniki pomiarów, z uwzględnieniem rachunku błędów, jak też formułować wnioski na podstawie tak przeprowadzonej analizy. Student potrafi – zgodnie z zadaną specyfikacją - zaprojektować oraz zrealizować prosty proces

pomiarowy, używając właściwych metod, technik i narzędzi. Student dostrzega potrzebę ciągłego dokształcania się w kierunku podnoszenia kompetencji zawodowych. Student

dostrzega i prawidłowo identyfikuje oraz rozstrzyga dylematy związane z wykonywaniem zawodu, z badaniami i działalnością inżynierską.

Przedmiot: C.II.2. PODSTAWY GRAFIKI INŻYNIERSKIEJ

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
I	14		24			38	38	76	1,5	1,5	3	Zo	O
Ogółem	14		24			38	38	76	1,5	1,5	3	Zo-1	

Cele kształcenia: Nabycie umiejętności odwzorowania układów przestrzennych, w tym elementów maszyn, urządzeń i konstrukcji oraz innych układów technicznych za pomocą graficznej reprezentacji na płaszczyźnie; znajomość oprogramowania do wspomagania tworzenia dokumentacji technicznej.

Treści kształcenia: Podstawy wykonania i umiejętność odczytywania inżynierskiej dokumentacji technicznej. Metody odwzorowań figur geometrycznych na płaszczyźnie, oparte na rzutowaniu równoległym i środkowym. Normalizacja w zakresie dokumentacji technicznej. Zapoznanie się z podstawowym oprogramowaniem wspomagającym proces tworzenia dokumentacji technicznej.

Efekty uczenia się: Student zna i rozumie podstawowe zasady odwzorowania układów przestrzennych, w tym elementów maszyn, urządzeń i konstrukcji oraz innych układów technicznych za pomocą graficznej reprezentacji na płaszczyźnie. Student zna podstawowe zasady tworzenia rysunkowej dokumentacji technicznej układów technicznych oraz elementów konstrukcyjnych w oparciu o normatywy. Student zna podstawowe oprogramowanie do wspomagania wykonywania rysunkowej dokumentacji technicznej. Student potrafi wykorzystać poznane metody odwzorowania graficznego i restytucji do stworzenia zapisu graficznego elementów maszyn, urządzeń i konstrukcji oraz innych układów technicznych. Student potrafi posłużyć się właściwym sposobem odwzorowania graficznego do wykonania dokumentacji techniczno-wykonawczej pojedynczego elementu lub grupy elementów w postaci złożenia podzespołu lub zespołu. Student potrafi odczytać

oraz określić rodzaj i dokonać klasyfikacji elementów odwzorowanych za pomocą rysunku wykonawczego złożeniowego lub zestawieniowego. Student zna podstawy posługiwania się oprogramowaniem komputerowym do wspomagania tworzenia dokumentacji technicznej. Student ma świadomość odpowiedzialności za pracę własną. Rozumie potrzebę i zna możliwości ciągłego dokształcania się.

Przedmiot: C.II.3. MATEMATYKA 1

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
I	30	38				68	83	151	2,7	3,3	6	E	O
Ogółem	30	38				68	83	151	2,7	3,3	6	E-1	

Cele kształcenia: Uzyskanie na koniec realizacji przedmiotu wiedzy, umiejętności i kompetencji zgodnych z niżej wykazanymi efektami uczenia się.

Treści kształcenia: Elementy teorii zbiorów. Zbiory liczbowe. Działania na zbiorach. Odwzorowania i ich właściwości. Relacje. Przeliczalność zbioru. Funkcje elementarne. Określenie i właściwości funkcji. Funkcje trygonometryczne. Tożsamości trygonometryczne. Funkcje cyklometryczne. Funkcje wykładnicze i logarytmiczne, funkcje hiperboliczne. Struktury algebraiczne. Zbiory liczbowe. Działania arytmetyczne. Grupa. Ciało. Ciało liczb rzeczywistych. Liczby zespolone. Ciało liczb zespolonych. Postacie liczb zespolonych: algebraiczna, trygonometryczna, wykładnicza. Potęga i pierwiastek liczby zespolonej. Zbiory na płaszczyźnie zespolonej. Wielomiany nad ciałem liczb zespolonych. Zasadnicze twierdzenie algebry. Rozkład wielomianu zespolonego lub rzeczywistego na czynniki. Macierze i wyznaczniki. Macierze. Rachunek macierzowy. Wyznaczniki i ich właściwości. Macierz odwrotna. Rząd macierzy. Układy liniowych równań algebraicznych. Metoda eliminacji Gaussa. Wzory Cramera. Twierdzenie Kroneckera-Capelliego. Równania macierzowe. Przestrzenie wektorowe. Określenie przestrzeni wektorowej. Kombinacja liniowa wektorów. Układ liniowo niezależny wektorów. Baza i wymiar przestrzeni liniowej. Podprzestrzeń. Przekształcenie liniowe. Macierz przekształcenia. Wektory i wartości własne macierzy. Geometria analityczna. Wektory swobodne. Iloczyny: skalarny, wektorowy, mieszany. Norma wektora, kąt między wektorami. Afiniczna przestrzeń euklidesowa. Prosta i płaszczyzna w przestrzeni trójwymiarowej. Zagadnienia geometryczne: proste, płaszczyzny, rzuty prostokątne i symetrie. Proste konstrukcje geometryczne. Krzywe płaskie drugiego stopnia. Powierzchnie drugiego stopnia w przestrzeni trójwymiarowej.

Efekty uczenia się: Posiada podstawową wiedzę, stanowiącą bazę dla zrozumienia i studiowania przedmiotów kierunkowych, w zakresie algebry z geometrią. Zna symbole i elementarne pojęcia logiki i teorii mnogości. Zna funkcje elementarne. Zna liczby rzeczywiste i zespolone. Poznał i rozumie zasadnicze twierdzenie algebry. Opanował rachunek wektorowy i macierzowy, zna właściwości skończenie wymiarowych przestrzeni wektorowych, rozumie pojęcia bazy przestrzeni wektorowej i niezależności układu wektorów. Zna określenie układu liniowych równań algebraicznych i rozumie pojęcie jego rozwiązania. W zakresie geometrii zna podstawy geometrii analitycznej, równania prostej, płaszczyzny oraz wybranych krzywych płaskich i powierzchni drugiego stopnia w przestrzeni trójwymiarowej. Umie posługiwać się w elementarnym zakresie językiem algebry i geometrii analitycznej, wykorzystując właściwe symbole i odpowiednie twierdzenia. Umie obliczać wyznaczniki macierzy. Umie wyznaczać macierze odwrotne. Umie rozwiązywać proste układy liniowych równań algebraicznych. Umie rozkładać wektory w bazie przestrzeni wektorowej. Umie wykonywać analitycznie proste konstrukcje geometryczne z użyciem prostych i płaszczyzn. Umie formułować i rozwiązywać proste problemy z wykorzystaniem rachunku wektorowego, rachunku macierzowego, układów liniowych równań algebraicznych i geometrii analitycznej. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł (także anglojęzycznych); potrafi interpretować uzyskane informacje i formułować wnioski. Ma wyrobioną wewnętrzną potrzebę i umiejętność ustawicznego uzupełniania i nowelizacji nabytej wiedzy poprzez samokształcenie. Rozumie potrzebę ciągłego dokształcania się i odświeżania wiedzy, w szczególności związanej ze złożoną strukturą matematyki.

Przedmiot: C.II.4. MATEMATYKA 2

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
I	34	34				68	83	151	2,7	3,3	6	E	O
Ogółem	34	34				68	83	151	2,7	3,3	6	E-1	

Cele kształcenia: Uzyskanie na koniec realizacji przedmiotu wiedzy, umiejętności i kompetencji zgodnych z niżej wykazanymi efektami uczenia się.

Treści kształcenia: Ciągi liczbowe. Twierdzenia o ciągach liczbowych. Granica ciągu liczbowego. Granice niewłaściwe. Symbole oznaczone i nieoznaczone. Przykłady ciągów, liczba e. Szeregi liczbowe. Określenie i kryteria zbieżności szeregów. Zbieżność warunkowa i bezwzględna szeregu liczbowego. Szeregi przemienne. Przykłady; liczby e i π. Granica

i ciągłość odwzorowania. Przestrzeń metryczna skończenie wymiarowa z metryką euklidesową. Gęstość i ciągłość przestrzeni liczb rzeczywistych. Określenia granicy i ciągłości odwzorowania z przykładami. Granica i ciągłość odwzorowania. Ciągłość funkcji jednej zmiennej. Twierdzenia o granicach funkcji. Asymptoty. Pochodna funkcji jednej zmiennej. Różniczka i pochodna funkcji jednej zmiennej. Podstawowe twierdzenia o pochodnych. Pochodne funkcji elementarnych. Ekstrema. Wypukłość i wklęsłość funkcji. Punkt przegięcia. Zastosowania pochodnej. Całka nieoznaczona. Określenie całki nieoznaczonej. Całkowanie przez części. Całkowanie przez podstawienie. Całkowanie funkcji wymiernych i trygonometrycznych. Całka oznaczona. Określenie całki oznaczonej. Właściwości całki oznaczonej. Związek między całką oznaczoną i nieoznaczoną. Całki niewłaściwe pierwszego i drugiego rodzaju. Zastosowania całek oznaczonych. Pochodna funkcji wielu zmiennych. Granica i ciągłość skalarnej i wektorowej funkcji wielu zmiennych. Pochodne cząstkowe. Różniczka i pochodna skalarnej i wektorowej funkcji wielu zmiennych. Pochodna w kierunku wektora. Wzór Taylora z pierwszą pochodną. Ekstrema lokalne i ekstrema na zbiorze skalarnej funkcji dwu lub trzech zmiennych.

Efekty uczenia się: Posiada podstawową wiedzę, stanowiącą bazę dla zrozumienia i studiowania przedmiotów kierunkowych, w zakresie analizy matematycznej. Zna symbole, podstawowe pojęcia i twierdzenia rachunku różniczkowego i całkowego funkcji jednej zmiennej rzeczywistej oraz rachunku różniczkowego funkcji wielu zmiennych rzeczywistych. Rozumie pojęcia granicy i ciągłości funkcji, funkcji pochodnej, całki oznaczonej i nieoznaczonej. Zna podstawowe sposoby i wzory znajdowania pochodnych oraz całek oznaczonych i nieoznaczonych. Rozumie pojęcia granicy, ciągłości i różniczkowalności funkcji wielu zmiennych. Zna podstawowe sposoby i wzory znajdowania pochodnych cząstkowych. Umie posługiwać się w podstawowym zakresie językiem analizy matematycznej, wykorzystując właściwe symbole i odpowiednie twierdzenia. Umie obliczać granice ciągów, także wyrażeń nieoznaczonych, wykorzystując wzory i twierdzenia. Umie zbadać zbieżność prostych szeregów liczbowych, stosując odpowiednie twierdzenia. Umie obliczać granice i badać ciągłość funkcji jednej zmiennej. Umie znajdować pochodne według określenia i z wykorzystaniem wzorów i twierdzeń. Umie obliczać proste całki nieoznaczone, stosując odpowiednie twierdzenia i wzory, w tym całki funkcji wymiernych. Umie obliczać proste całki oznaczone. Umie obliczać pochodne cząstkowe. Umie formułować i rozwiązywać proste problemy z wykorzystaniem rachunku różniczkowego i całkowego funkcji jednej zmiennej oraz rachunku różniczkowego funkcji wielu zmiennych. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł (także anglojęzycznych); potrafi interpretować uzyskane informacje i formułować wnioski. Ma wyrobioną wewnętrzną potrzebę i umiejętność ustawicznego uzupełniania i nowelizacji nabytej wiedzy poprzez samokształcenie. Rozumie potrzebę ciągłego dokształcania się i odświeżania wiedzy, w szczególności związanej ze złożoną strukturą matematyki.

Przedmiot: C.II.5. MATEMATYKA DYSKRETNA 1

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
I	16	14				30	33	63	1,2	2,3	2,5	Zo	O
Ogółem	16	14				30	33	63	1,2	2,3	2,5	Zo-1	

Cele kształcenia: Uzyskanie na koniec realizacji przedmiotu wiedzy, umiejętności i kompetencji zgodnych z niżej wykazanymi efektami uczenia się.

Treści kształcenia: Rachunek zdań i kwantyfikatorów. Metody wnioskowania. Indukcja matematyczna. Rachunek zbiorów. Relacje. Funkcje. Działania uogólnione na zbiorach. Elementy teorii mocy. Rekurencje. Drzewa binarne i wielomianowe. Asymptotyka funkcji liczbowych. Permutacje.

Efekty uczenia się: Ma wiedzę w zakresie podstaw logiki matematycznej, rachunku predykatów oraz teorii mnogości i teorii mocy. Ma wiedzę w zakresie relacji oraz funkcji, w tym permutacji. Ma wiedzę w zakresie definicji rekurencyjnych ciągów liczbowych, zbiorów i funkcji. Ma wiedzę w zakresie podstaw analizy złożoności obliczeniowej podstawowych funkcji liczbowych. Umie posługiwać się terminologią logiki, teorii mnogości, relacji i funkcji do interpretowania pojęć z zakresu informatyki. Potrafi opisywać w postaci zależności rekurencyjnych wyrażenia opisujące procesy występujące w systemach informatycznych, w szczególności w opisach algorytmicznych tych procesów. Potrafi posługiwać się podstawowymi narzędziami do analizy złożoności problemów występujących w systemach inżynierskich, w tym informatycznych.

Przedmiot: C.II.6. ANALIZA MATEMATYCZNA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
II	20	24				44	58	102	1,7	2,3	4	E	O
Ogółem	20	24				44	58	102	1,7	2,3	4	E-1	

Cele kształcenia: Uzyskanie na koniec realizacji przedmiotu wiedzy, umiejętności i kompetencji zgodnych z niżej wykazanymi efektami uczenia się.

Treści kształcenia: Równania różniczkowe zwyczajne. Określenie równania różniczkowego zwyczajnego rzędów pierwszego i wyższych. Zagadnienie Cauchy'ego. Twierdzenia o istnieniu i jednoznaczności rozwiązań. Równania pierwszego rzędu o zmiennych rozdzielonych. Wybrane typy równań pierwszego i drugiego rzędu. Równania liniowe pierwszego rzędu. Równania liniowe drugiego rzędu, w tym o stałych współczynnikach. Całki wielokrotne. Określenie całki wielokrotnej. Całki iterowane. Całka podwójna i całka potrójna po dowolnym obszarze. Zamiana zmiennych w całce wielokrotnej. Współrzędne prostokątne, biegunowe, walcowe i kuliste. Zastosowania całek wielokrotnych. Zastosowania całek oznaczonych i wielokrotnych. Obliczanie długości krzywych i pól powierzchni. Zastosowania całek wielokrotnych. Obliczanie objętości brył. Ciągi i szeregi funkcyjne. Zbieżność punktowa i jednostajna ciągu i szeregu funkcyjnego. Twierdzenia o ciągach i szeregach zbieżnych jednostajnie. Szereg potęgowy. Promień i przedział zbieżności szeregu potęgowego. Twierdzenia o różniczkowaniu i całkowaniu szeregu potęgowego. Szereg Taylora. Rozwijanie funkcji w szereg potęgowy. Wykład z możliwym wykorzystaniem technik audiowizualnych; podanie zadań do samodzielnego rozwiązania i tematów do studiowania.

Efekty uczenia się: Posiada podstawową wiedzę, stanowiącą bazę dla zrozumienia i studiowania przedmiotów kierunkowych, w zakresie analizy matematycznej. Zna symbole, podstawowe pojęcia i twierdzenia rachunku różniczkowego i całkowego funkcji wielu zmiennych rzeczywistych oraz podstawowe pojęcia, określenia i twierdzenia teorii równań różniczkowych zwyczajnych pierwszego i drugiego rzędu. Zna podstawowe pojęcia, określenia, twierdzenia i przykłady dla szeregów potęgowych. Zna podstawowe sposoby i wzory znajdowania całek podwójnych i potrójnych oraz podstawowe sposoby rozwiązywania równań różniczkowych zwyczajnych pierwszego i drugiego rzędu. Zna podstawowe metody rozwijania funkcji w szeregi potęgowe. Umie posługiwać się w podstawowym zakresie językiem analizy matematycznej, wykorzystując właściwe

symbole, określenia i odpowiednie twierdzenia. Umie stosować rachunek różniczkowy i całkowy funkcji wielu zmiennych do rozwiązywania zadań. Umie rozwiązywać równania różniczkowe zwyczajne pierwszego rzędu o zmiennych rozdzielonych i liniowe oraz drugiego rzędu liniowe o stałych współczynnikach. Umie rozwijać funkcje w szeregi potęgowe. Umie formułować i rozwiązywać proste problemy z wykorzystaniem rachunku różniczkowego i całkowego funkcji wielu zmiennych, równań różniczkowych zwyczajnych oraz szeregów potęgowych. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł (także anglojęzycznych); potrafi interpretować uzyskane informacje i formułować wnioski. Ma wyrobioną wewnętrzną potrzebę i umiejętność ustawicznego uzupełniania i nowelizacji nabytej wiedzy poprzez samokształcenie. Rozumie potrzebę ciągłego dokształcania się i odświeżania wiedzy, w szczególności związanej ze złożoną strukturą matematyki.

Przedmiot: C.II.7. FIZYKA 1

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
II	40	30	10			80	70	150	3,2	2,8	6	E	O
Ogółem	40	30	10			80	70	150	3,2	2,8	6	E-1	

Cele kształcenia: Uzyskanie na koniec realizacji przedmiotu wiedzy, umiejętności i kompetencji zgodnych z niżej wykazanymi efektami uczenia się.

Treści kształcenia: Kinematyka punktu materialnego. Dynamika punktu materialnego. Mechanika ciała sztywnego. Podstawy szczególnej teorii względności. Elementy mechaniki relatywistyczne. Pole elektryczne. Pole magnetyczne. Zmienne pola elektromagnetyczne, równania Maxwella.

Efekty uczenia się: Ma podstawową wiedzę na temat ogólnych zasad fizyki, wielkości fizycznych, oddziaływań fundamentalnych. Ma wiedzę w zakresie fizyki klasycznej oraz podstaw fizyki relatywistycznej. Ma wiedzę na temat zasad przeprowadzania i opracowania wyników pomiarów fizycznych, rodzajów niepewności pomiarowych i sposobów ich wyznaczania. Potrafi wykorzystać poznane zasady i metody fizyki oraz odpowiednie narzędzia matematyczne do opisu właściwości fizycznych oraz związanych z nimi efektów przyczynowo skutkowych pod wpływem oddziaływań zewnętrznych. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł, potrafi integrować uzyskane informacje, dokonywać ich interpretacji oraz prawidłowo wyciągać wnioski. Umie przeprowadzić pomiary wybranych wielkości fizycznych i je opracować, a także zinterpretować w

kontekście posiadanej wiedzy z fizyki. Potrafi myśleć i działać w twórczy sposób. Potrafi pracować i współdziałać w grupie.

Przedmiot: C.II.8. MATEMATYKA DYSKRETNA 2

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
II	16	14				30	45	75	1,2	1,8	3	E	O
Ogółem	16	14				30	45	75	1,2	1,8	3	E-1	

Cele kształcenia: Uzyskanie na koniec realizacji przedmiotu wiedzy, umiejętności i kompetencji zgodnych z niżej wykazanymi efektami uczenia się.

Treści kształcenia: Techniki zliczania. Zliczanie zbiorów i funkcji. Funkcje tworzące i ich zastosowania. Podzielność liczb całkowitych. Działanie modulo. Podstawowe twierdzenie arytmetyki. Kongruencje.

Efekty uczenia się: Ma wiedzę w zakresie technik zliczania. Ma wiedzę w zakresie funkcji tworzących i ich zastosowań. Ma wiedzę w zakresie zagadnień podzielności liczb całkowitych. Umie zliczać zbiory elementów występujących w problemach inżynierskich w tym problemach z zakresu informatyki. Potrafi konstruować funkcje tworzące dla wybranych ciągów liczbowych oraz stosować je do rozwiązywania równań rekurencyjnych występujących w zagadnieniach inżynierskich. Potrafi rozwiązywać kongruencje odpowiadających problemom inżynierskim.

Przedmiot: C.II.9 RACHUNEK PRAWDOPODOBIEŃSTWA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
II	18	4	10			32	45	77	1,2	1,8	3	Zo	O
Ogółem	18	4	10			32	45	77	1,2	1,8	3	Zo-1	

Cele kształcenia: Poznanie i zrozumienie przez studentów podstawowych pojęć i twierdzeń rachunku prawdopodobieństwa, oraz opanowania elementarnych umiejętności rachunkowych z zakresem wiedzy obejmującym: prawdopodobieństwo, zmienne losowe, parametry zmiennych losowych, podstawowe rozkłady prawdopodobieństwa twierdzenia graniczne.

Treści kształcenia: Pojęcie i właściwości prawdopodobieństwa. Pojęcie prawdopodobieństwa. Przestrzeń probabilistyczna. Pojęcie i właściwości prawdopodobieństwa. Prawdopodobieństwo warunkowe. Niezależność zdarzeń. Zmienne losowe. Zmienna losowa jednowymiarowa. Parametry rozkładu zmiennych losowych. Funkcja charakterystyczna zmiennej losowej. Podstawowe rozkłady prawdopodobieństwa. Rozkłady: dwumianowy, Poissona, geometryczny, jednostajny, wykładniczy. Normalny (Gaussa). Zmienna losowa wielowymiarowa. Zmienna losowa dwuwymiarowa; parametry rozkładu. Rozkłady brzegowe i warunkowe. Twierdzenia graniczne rachunku prawdopodobieństwa.

Efekty uczenia się: Posiada podstawową wiedzę, stanowiącą bazę dla zrozumienia i studiowania przedmiotów kierunkowych, w zakresie rachunku prawdopodobieństwa. Zna podstawowe pojęcia, określenia, rozkłady prawdopodobieństwa i twierdzenia rachunku prawdopodobieństwa. Zna podstawowe metody obliczania prawdopodobieństw zdarzeń losowych. Zna interpretacje i sposoby obliczania najważniejszych parametrów zmiennych losowych oraz stosuje twierdzenia graniczne. Umie korzystać z najważniejszych rozkładów prawdopodobieństwa. Umie formułować i rozwiązywać proste problemy z wykorzystaniem pojęć rachunku prawdopodobieństwa, rozkładów prawdopodobieństwa i twierdzeń granicznych. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł (także anglojęzycznych); potrafi interpretować uzyskane informacje i formułować wnioski. Ma wyrobioną wewnętrzną potrzebę i umiejętność ustawicznego uzupełniania i nowelizacji nabytej wiedzy poprzez samokształcenie.

Przedmiot: C.II.10. TEORETYCZNE PODSTAWY INFORMATYKI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
II	14	12	4			30	45	75	1,2	1,8	3	Zo	O
Ogółem	14	12	4			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Uzyskanie na koniec realizacji przedmiotu wiedzy, umiejętności i kompetencji zgodnych z niżej wykazanymi efektami uczenia się.

Treści kształcenia: Reprezentacja algorytmu i charakterystyki algorytmu. Modele obliczeń, deterministyczne i niedeterministyczne maszyny Turinga jednotaśmowe i wielotaśmowe. Modele obliczeń niejednostajnych. Złożoność algorytmów i problemów oraz metody jej szacowania. Transformacje problemów, funkcje obliczalne. Klasy złożoności problemów. NP.-zupełność. Hierarchie złożoności. Czas działania algorytmów i programów. Modele definiowania i rozpoznawania wzorców znakowych. Alfabet, język. Automaty deterministyczne skończone, automaty niedeterministyczne, języki akceptowane przez automaty. Wyrażenia regularne, Gramatyki bezkontekstowe. i kontekstowe, języki gramatyk. Architektury równoległe. Modele obliczeń równoległych.

Efekty uczenia się: Ma wiedzę dotyczącą modeli obliczeniowych, reprezentacji i charakterystyk algorytmów, w tym dokładności i złożoności obliczeniowej. Ma podstawową wiedzę w zakresie obliczeń niejednostajnych, architektur i modeli obliczeń równoległych. Ma wiedzę z podstaw informatyki dotyczącą wyrażeń regularnych, automatów skończonych i gramatyk formalnych. Umie szacować złożoność algorytmów i problemów i oceniać oraz klasyfikować problemy decyzyjne. Umie: zbudować diagram automatu skończonego, dokonać przekształceń wyrażeń regularnych i wyznaczyć ich wartość (język), dokonywać równoważnych przekształceń gramatyk formalnych i określać języki gramatyk.

Przedmiot: C.II.11. FIZYKA 2

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
III	30	20	10			60	40	100	2,4	1,6	4	E	O
Ogółem	30	20	10			60	40	100	2,4	1,6	4	E-1	

Cele kształcenia: Uzyskanie na koniec realizacji przedmiotu wiedzy, umiejętności i kompetencji zgodnych z niżej wykazanymi efektami uczenia się.

Treści kształcenia: Drgania i fale mechaniczne i elektromagnetyczne. Elementy akustyki. Elementy optyki. Dualizm korpuskularno–falowy promieniowania elektromagnetycznego i mikrocząstek. Budowa atomu. Podstawy krystalografii. Metale i półprzewodniki.

Efekty uczenia się: Ma podstawową wiedzę na temat ogólnych zasad fizyki, wielkości fizycznych, oddziaływań fundamentalnych. Ma wiedzę w zakresie optyki, podstaw fizyki kwantowej, podstaw fizyki ciała stałego i fizyki jądrowej. Ma wiedzę na temat zasad przeprowadzania i opracowania wyników pomiarów fizycznych, rodzajów niepewności pomiarowych i sposobów ich wyznaczania. Potrafi wykorzystać poznane zasady i metody fizyki oraz odpowiednie narzędzia matematyczne do opisu właściwości fizycznych oraz związanych z nimi efektów przyczynowo-skutkowych pod wpływem oddziaływań zewnętrznych. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł, potrafi integrować uzyskane informacje, dokonywać ich interpretacji oraz prawidłowo wyciągać wnioski. Umie przeprowadzić pomiary wybranych wielkości fizycznych i je opracować, a także zinterpretować w kontekście posiadanej wiedzy z fizyki. Potrafi myśleć i działać w twórczy sposób. Potrafi pracować i współdziałać w grupie.

Przedmiot: C.II.12. TEORIA GRAFÓW I SIECI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
III	16	14				30	20	50	1,2	0,8	2	Zo	O
Ogółem	16	14				30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Uzyskanie na koniec realizacji przedmiotu wiedzy, umiejętności i kompetencji zgodnych z niżej wykazanymi efektami uczenia się.

Treści kształcenia: Definicja grafu. Rodzaje i części grafów (Graf jako model systemu. Charakterystyki grafu i elementów jego struktury. Podgrafy i grafy częściowe). Kolorowanie grafów (Stabilne podzbiory wierzchołków grafu. Bazy grafu. Chromatyka grafów. Modele kolorowania grafów. Algorytmy dokładne i przybliżone kolorowania grafów. Złożoność obliczeniowa omawianych algorytmów). Marszruty, łańcuchy i drogi w grafach (Definicje marszruty, łańcucha, drogi. Spójność i silna spójność grafu. Cyklomatyka i karkasy grafów. Złożoność obliczeniowa omawianych algorytmów). Grafy Berge'a (Definicja i rodzaje. Składowe silnej spójności digrafów. Algorytm Leifmana. Drogi w digrafach. Warstwowa reprezentacja digrafu. Drogi Eulera i Hamiltona w grafie. Złożoność obliczeniowa omawianych algorytmów). Sieci (Definicja sieci. Karkasy ekonomiczne. Drogi ekstremalne w sieciach cyklicznych i acyklicznych w sensie dróg. Sieciowe metody analizy złożonych przedsięwzięć. Sieci stochastyczne i podstawowe problemy definiowane w nich. Złożoność obliczeniowa omawianych algorytmów). Przepływy w sieciach (Przepływ w sieci standardowej. Przekrój rozdzielający i jego przepustowość. Algorytm wyznaczania przepływu maksymalnego. Spójność krawędziowa i wierzchołkowa. Drogi rozłączne wierzchołkowo i krawędziowo. Twierdzenie Mengera. Przepływ zaspokajający o minimalnym koszcie. Złożoność obliczeniowa omawianych algorytmów). Przydziały optymalne (Określenie przydziału jako skojarzenia sieci dwudzielnej. Twierdzenie Halla. Algorytm wyznaczania przydziału najliczniejszego, przydziału najliczniejszego o minimalnym koszcie. Złożoność obliczeniowa algorytmów).

Efekty uczenia się: Znajomość zasad modelowania systemów z wykorzystaniem grafów i sieci. Znajomość różnych modeli teorii grafów i sieci. Znajomość metod rozwiązywania problemów modelowanych za pomocą grafów i sieci. Umiejętność modelowania obiektów rzeczywistych za pomocą modeli grafowych i sieciowych. Umiejętność rozróżnienia problemu grafowego od sieciowego. Umiejętność wykorzystania specjalizowanych metod grafowo-sieciowych do rozwiązywania praktycznych problemów inżynierskich.

Przedmiot: C.II.13. PODSTAWY OPTYMALIZACJI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
III	14	16				30	45	75	1,2	1,8	3	Zo	O
Ogółem	14	16				30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Poznanie i zrozumienie metod rozwiązywania zadań dyskretnych, liniowych i nieliniowych oraz wykorzystywania metody optymalizacji do rozwiązywania zadań praktycznych.

Treści kształcenia: Ogólne zadanie optymalizacji, klasy zadań, własności zadań. Elementy analizy wypukłe i zadania wypukłe. Postaci zadania liniowego, zadania dualne. Algorytm prymalny i dualny simpleks. Programowanie dyskretne: zadania unimodularne, metoda podziału i oszacowań, metody rozwiązywania zadań PLB. Programowanie nieliniowe: metody rozwiązywania zadań bez ograniczeń, metody rozwiązywania zadań z ograniczeniami, a w tym warunki różniczkowe Kuhna-Tuckera, metody kierunków dopuszczalnych, metoda rozwiązywania zadań kwadratowych.

Efekty uczenia się: Ma wiedzę dotyczącą własności i metod rozwiązywania zadań liniowych. Ma wiedzę dotyczącą własności i metod rozwiązywania zadań dyskretnych. Ma wiedzę dotyczącą własności i metod rozwiązywania zadań nieliniowych. Umie badać własności i klasyfikować zadania optymalizacji z punktu widzenia ich zastosowań. Umie wykorzystywać metody optymalizacji do rozwiązywania zadań praktycznych.

Przedmiot: C.II.14. STATYSTYKA MATEMATYCZNA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
III	16		14			30	20	50	1,2	0,8	2	Zo	O
Ogółem	16		14			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Poznanie i zrozumienie przez studentów podstawowych pojęć i twierdzeń statystyki matematycznej oraz opanowanie elementarnych umiejętności rachunkowych z zakresem wiedzy obejmującym: podstawowe statystyki i ich rozkłady, estymację punktową i przedziałową, weryfikację hipotez parametrycznych i nieparametrycznych, analizę korelacji i regresji.

Treści kształcenia: Podstawy statystyki matematycznej. Podstawowe statystyki. Rozkłady wybranych statystyk. Estymacja punktowa. Estymatory parametrów rozkładów zmiennych losowych. Estymacja przedziałowa. Przedziały ufności dla parametrów rozkładów zmiennych losowych. Weryfikacja hipotez parametrycznych. Testy dla parametrów rozkładów zmiennych losowych. Moc testu. Weryfikacja hipotez nieparametrycznych. Testy zgodności i niezależności. Analiza korelacji. Kowariancja. Charakterystyki korelacji zmiennych losowych. Wnioskowanie dotyczące korelacji. Analiza regresji. Rodzaje regresji. Regresja liniowa. Wnioskowanie dotyczące regresji.

Efekty uczenia się: Posiada podstawową wiedzę, stanowiącą bazę dla zrozumienia i studiowania przedmiotów kierunkowych, w zakresie statystyki matematycznej. Zna podstawowe pojęcia, określenia i twierdzenia dotyczące estymacji punktowej i przedziałowej, weryfikacji hipotez parametrycznych i nieparametrycznych, badania korelacji i regresji. Zna podstawowe konstrukcje estymatorów punktowych, przedziałów ufności, testów statystycznych i linii regresji. Zna sposoby wnioskowania o parametrach rozkładów, postaciach dystrybuant, niezależności, korelacji i regresji zmiennych losowych na podstawie danych statystycznych. Umie estymować parametry rozkładów zmiennych losowych, weryfikować hipotezy statystyczne i znajdować charakterystyki korelacji i regresji zmiennych losowych. Umie formułować i rozwiązywać proste problemy z wykorzystaniem pojęć i metod wnioskowania statystyki matematycznej. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł (także anglojęzycznych); potrafi interpretować uzyskane informacje i formułować wnioski. Ma wyrobioną wewnętrzną potrzebę i umiejętność ustawicznego uzupełniania i nowelizacji nabytej wiedzy poprzez samokształcenie.

Przedmiot: C.II.15. MODELOWANIE MATEMATYCZNE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IV	14	16				30	45	75	1,2	1,8	3	Zo	O
Ogółem	14	16				30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Umiejętność konstruowania modeli matematycznych oraz formułowania zadań optymalizacyjnych oraz dobierania narzędzi do formalnego opisu sytuacji decyzyjnych w warunkach wielokryterialnych, growych, ryzyka, niepewności, rozmytości oraz przybliżoności.

Treści kształcenia: Zasady modelowania matematycznego. Model matematyczny. Dane, zmienne decyzyjne, kryteria oraz zbiory ich wartości. Analiza informacyjna. Funkcja oceny osiągnięcia celu. Sformułowanie zadania optymalizacyjnego. Modele deterministyczne. Modele growe. Modele probabilistyczne. Modele wykorzystujące teorię zbiorów rozmytych. Modele uwzględniające niepewność danych. Modele wykorzystujące teorię zbiorów przybliżonych.

Efekty uczenia się: Ma wiedzę w zakresie zasad konstruowania modeli matematycznych oraz formułowania zadań optymalizacyjnych, w tym przy niepewnej i niekompletnej informacji. Umie konstruować modele matematyczne oraz formułować zadania optymalizacyjne dla problemów praktycznych w tym problemów z zakresu informatyki. Potrafi dobierać narzędzia do formalnego opisu sytuacji decyzyjnych w warunkach wielokryterialnych, growych, ryzyka, niepewności, rozmytości oraz przybliżoności.

Przedmiot: C.II.16. BEZPIECZEŃSTWO PRACY I ERGONOMIA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IV	12		8			20	5	25	0,8	0,2	1	Zo	O
Ogółem	12		8			20	5	25	0,8	0,2	1	Zo-1	

Cele kształcenia: Nabycie wiedzy w zakresie odbioru informacji przez użytkownika, wymagań na warunki pracy oraz zagrożeń dla zdrowia użytkownika występujących na stacjonarnym stanowisku pracy z monitorem ekranowym; umiejętność organizacji stacjonarnego stanowiska pracy z monitorem ekranowym.

Treści kształcenia: Odbiór informacji przez użytkownika systemu komputerowego. Organizacja stacjonarnego stanowiska pracy z monitorem ekranowym. Wymagania na warunki pracy na stanowisku wyposażonym w monitor ekranowy. Zagrożenia dla zdrowia pracownika występujące na stanowisku pracy wyposażonym w monitor ekranowy. Obowiązki oraz prawa pracownika i pracodawcy w zakresie bezpieczeństwa i higieny pracy w informatyce. Metody oceny ryzyka zawodowego na stanowisku pracy. Ergonomiczne wymagania na interfejs człowiek-komputer.

Efekty uczenia się: Ma wiedzę w zakresie wymagań na warunki pracy na stanowisku i podstawowych zagrożeń dla zdrowia pracownika występujących na stanowisku pracy wyposażonym w monitor ekranowy. Ma wiedzę w zakresie podstawowych przepisów dotyczących bezpieczeństwa i higieny pracy w informatyce. Potrafi zorganizować stanowisko pracy z monitorem ekranowym oraz ocenić ryzyko zawodowe na takim stanowisku.

Przedmiot: C.II.17. PODSTAWY BEZPIECZEŃSTWA INFORMACJI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
V	20		10			30	20	50	1,2	0,8	2	Zo	O
Ogółem	20		10			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: nabycie wiedzy w zakresie odbioru informacji przez użytkownika, wymagań na warunki pracy oraz zagrożeń dla zdrowia użytkownika występujących na stacjonarnym stanowisku pracy z monitorem ekranowym; umiejętność organizacji stacjonarnego stanowiska pracy z monitorem ekranowym.

Treści kształcenia: Odbiór informacji przez użytkownika systemu komputerowego. Organizacja stacjonarnego stanowiska pracy z monitorem ekranowym. Wymagania na warunki pracy na stanowisku wyposażonym w monitor ekranowy. Zagrożenia dla zdrowia pracownika występujące na stanowisku pracy wyposażonym w monitor ekranowy. Obowiązki oraz prawa pracownika i pracodawcy w zakresie bezpieczeństwa i higieny pracy w informatyce. Metody oceny ryzyka zawodowego na stanowisku pracy. Ergonomiczne wymagania na interfejs człowiek-komputer.

Efekty uczenia się: Ma wiedzę w zakresie wymagań na warunki pracy na stanowisku i podstawowych zagrożeń dla zdrowia pracownika występujących na stanowisku pracy wyposażonym w monitor ekranowy. Ma wiedzę w zakresie podstawowych przepisów dotyczących bezpieczeństwa i higieny pracy w informatyce. Potrafi zorganizować stanowisko pracy z monitorem ekranowym oraz ocenić ryzyko zawodowe na takim stanowisku.

8.2.3. GRUPA TREŚCI PRZEDMIOTÓW KSZTAŁCENIA KIERUNKOWEGO C.III

Ramowy opis przedmiotów

Przedmiot: C.III.1. WPROWADZENIE DO PROGRAMOWANIA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	Łącznie							
II	10		20			30	45	75	1,2	1,8	3	E	O
Ogółem	10		20			30	45	75	1,2	1,8	3	E-1	

Cele kształcenia: Nabycie wiedzy w zakresie: różnych metod i technik programowania strukturalnego w języku C oraz umiejętność konstruowania algorytmów będących rozwiązaniami typowych zadań programistycznych; programowania strukturalnego; podstaw algorytmiki i struktur danych

Treści kształcenia: Pojęcia podstawowe technik programowania. Elementarny wstęp do algorytmiki. Typy danych w języku C. Operatory i instrukcje języka C. Liniowe struktury danych. Funkcje. Rekurencja. Wskaźniki. Dynamiczne struktury danych – listy. Pliki.

Efekty uczenia się: Ma uporządkowaną, podbudowaną teoretycznie, wiedzę w zakresie różnych metod i technik programowania strukturalnego w języku C oraz umiejętność konstruowania algorytmów będących rozwiązaniami typowych zadań programistycznych. Ma uporządkowaną, podbudowaną teoretycznie, wiedzę w zakresie programowania strukturalnego. Ma uporządkowaną, podbudowaną teoretycznie, wiedzę z zakresu podstaw algorytmiki i struktur danych. Ma wiedzę i umiejętności samokształcenia się w zakresie programowania strukturalnego i podstaw algorytmiki. Ma podstawowe umiejętności z zakresu programowania strukturalnego pozwalające na samodzielne rozwiązywanie dobrze i słabo określonych zadań programowania.

Przedmiot: C.III.2. PODSTAWY TECHNIKI KOMPUTERÓW

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						Niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
II	28	8	16			52	75	127	2	3	5	Zo	O
Ogółem	28	8	16			52	75	127	2	3	5	Zo-1	

Cele kształcenia: Nabycie wiedzy w zakresie zasad działania elementów elektronicznych i cyfrowych układów elektronicznych, umiejętność projektowania prostych układów logicznych dla systemów komputerowych oraz dokonania krytycznej analizy sposobu funkcjonowania i oceny technicznych rozwiązań współczesnych komputerów a także programowania sterowników logicznych.

Treści kształcenia: Podstawowe elementy elektroniczne. Diody, tranzystory bipolarne i unipolarne Bramki logiczne diodowe, DTL i inwertor CMOS. Bramki logiczne TTL. Skale scalenia układów elektronicznych (SSI, MSI, LSI, VLSI, GLSI). Układy logiczne CMOS (bramki logiczne, koder/dekoder, multiplekser, sumator 1-bitowy). Przerzutniki (rodzaje) i ich zastosowania (rejestry, liczniki, pamięci statyczne).

Efekty uczenia się: Ma elementarną wiedzę w zakresie zasad działania elementów elektronicznych i cyfrowych układów elektronicznych. Potrafi projektować proste układy logiczne dla systemów komputerowych; potrafi dokonać krytycznej analizy sposobu funkcjonowania i ocenić techniczne rozwiązania współczesnych komputerów; potrafi programować sterowniki logiczne.

Przedmiot: C.III.3. ARCHITEKTURA I ORGANIZACJA KOMPUTERÓW

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
III	20		32			52	75	127	2	3	5	E	O
Ogółem	20		32			52	75	127	2	3	5	E-1	

Cele kształcenia: Znajomość elementów składowych komputera oraz budowy i działania podstawowych układów kombinacyjnych i sekwencyjnych; znajomość cyklu rozkazowego, sposobów realizacji sterowania centralnego w procesorze; umiejętność zapisu liczb w kodach dwójkowych, w kodzie ósemkowym, szesnastkowych, oraz wg normy IEEE 754; umiejętność wykonywania operacji arytmetycznych i logicznych na liczbach w różnych kodach.

Treści kształcenia: Cyfrowy zapis informacji. Funkcje logiczne. Algebra Boole'a. Metody minimalizacji funkcji logicznych. Układy arytmetyczne. Układy konwersji kodów. Multipleksery i demultipleksery. Przerzutniki. Maszynowa reprezentacja danych. Kodowanie liczb. Realizacja podstawowych operacji arytmetycznych i logicznych. Schemat blokowy komputera. Model von Neumanna. Pojęcie architektury i organizacji. Architektura języka wewnętrznego. Lista rozkazów, formaty rozkazów i danych, typy operacji, tryby adresacji. Organizacja komputera na poziomie asemblera. Organizacja jednostki centralnej. Sterowanie sprzętowe i mikroprogramowane. Cykl rozkazowy. Przerwania i wyjątki. Systemy przerwań. Wprowadzenie do komputera LABZSK. Pamięć główna. Typy i hierarchia pamięci. Organizacja i architektura systemów pamięci. Interfejsy i komunikacja. Przetwarzanie potokowe. Architektura procesora DLX – formaty danych, formaty rozkazów. Organizacja procesora DLX – wersja sekwencyjna i potokowa. Opis działania procesora w notacji przesłań międzyrejestrowych. Hazardy strukturalne. Zależności danych: true dependency, anti-dependency, output dependency. Hazardy danych – wprowadzenie. Przykłady hazardów danych RAW, WAR, WAW. Forwarding, scheduling. Analiza wybranych przykładów programów na poziomie asemblera z użyciem instrukcji warunkowych, pętli, operacji na liczbach całkowitych i zmiennoprzecinkowych, tablic. Hazardy sterowania. Statyczne i dynamiczne przewidywanie skoków. Rozwijanie pętli. Analiza i projektowanie programów na poziomie asemblera. Pamięć podręczna. Zasada lokalności odwołań. Typy odwzorowań pamięci cache. Współpraca cache – pamięć główna przy odczycie i przy zapisie. Ocena efektywności pamięci podręcznej. Przykłady rzeczywistych rozwiązań. Pamięć wirtualna. Sprzętowe i programowe mechanizmy

wspomagające efektywność działania pamięci wirtualnych. Porównanie architektur CISC, RISC i VLIW. Taksonomie systemów komputerowych: Flynna, Treleavena. Tendencje rozwojowe architektur współczesnych komputerów.

Efekty uczenia się: Znajomość maszynowej reprezentacji danych i liczb oraz operacji arytmetycznych i logicznych realizowanych przez komputer. Znajomość elementów składowych komputera oraz budowy i działania podstawowych układów kombinacyjnych i sekwencyjnych, model von Neumanna. Znajomość cyklu rozkazowego, sposobów realizacji sterowania centralnego w procesorze, znajomość pojęć: architektura i organizacja komputera, trybów adresowania, formatów i typów rozkazów na poziomie asemblera. Umiejętność zapisu liczb w kodach dwójkowych, w kodzie ósemkowym, szesnastkowych oraz wg normy IEEE 754. Umiejętność wykonywania operacji arytmetycznych i logicznych na liczbach w różnych kodach. Umiejętność projektowania sterowania centralnego procesora i budowania rozkazów z wykorzystaniem mikroprogramowania oraz sterowania sprzętowego. Znajomość metody przetwarzania potokowego. Znajomość przeznaczenia, organizacji i działania pamięci podręcznej i pamięci wirtualnej. Znajomość cech architektur oraz tendencji rozwojowych współczesnych systemów komputerowych. Umiejętność implementacji prostych programów w języku asembler. Umiejętność optymalizacji kodu programu, w języku asemblera, dla procesora o znanej architekturze.

Przedmiot: C.III.4. PODSTAWY PODZESPOŁÓW KOMPUTERÓW

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
III	14		16			30	20	50	1,2	0,8	2	Zo	O
Ogółem	14		16			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Umiejętności wykorzystania aparatu matematycznego w procesie projektowania prostych układów logicznych dla systemów cyfrowych.

Treści kształcenia: Układy kombinacyjne - pojęcia podstawowe. Algebra Boole'a, arytmetyka dwójkowa. Metody opisu układów kombinacyjnych. Podstawowe układy kombinacyjne. Minimalizacja funkcjilogicznych za pomocą przekształceń algebry Boole'a, graficzne metody minimalizacji za pomocą tablic Karnaugh'a, zjawisko hazardu. Metody syntezy układów kombinacyjnych. Projektowanie układów realizujących założoną funkcję logiczną. Projektowanie układów konwersji kodów (enkoderów, dekoderów, translatorów kodów). Projektowanie prostych układów arytmetycznych. Wykorzystanie układów

multiplekserów do realizacji funkcji logiczny n-zmiennych. Weryfikacja poprawności działania zaprojektowanego układu.

Układy sekwencyjne - pojęcia podstawowe. Podział układów sekwencyjnych, metody opisu układów sekwencyjnych, zjawisko wyścigu, przerzutnik jako podstawowy układ sekwencyjny. Automaty Meale'a i Moore'a jako modele układów sekwencyjnych, metody konwersji z jednego modelu w drugi. Metody syntezy układów sekwencyjnych. Projektowanie: układu asynchronicznego i synchronicznego działającego zgodnie z zadanym grafem przejść i wyjść, liczników oraz rejestrów. Weryfikacja poprawności działania zaprojektowanego układu sekwencyjnego.

Efekty uczenia się: Znajomość podstawowych pojęć z zakresu układów cyfrowych. Znajomość metod minimalizacji funkcji logicznych opisujących działanie układów cyfrowych. Znajomość sposobów opisu układów cyfrowych. Znajomość metod i narzędzi matematycznych wykorzystywanych w procesie syntezy układów cyfrowych. Umiejętność wykorzystania aparatu matematycznego w procesie projektowania prostych układów logicznych dla systemów cyfrowych. Umiejętność oceny poprawności działania prostych układów logicznych.

Przedmiot: C.III.5. ALGORYTMY I STRUKTURY DANYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
III	18		22			40	60	100	1,6	2,4	4	E	O
Ogółem	18		22			40	60	100	1,6	2,4	4	E-1	

Cele kształcenia: Nabycie umiejętności praktycznego wykorzystania znajomości podstawowych metod oceny złożoności obliczeniowej algorytmów; umiejętność oceny wpływu wykorzystanych struktur danych na złożoność obliczeniową projektowanego programu oraz dokonanie wyboru optymalnej struktury.

Treści kształcenia: Techniki projektowania algorytmów. Technika „dziel i rządź". Programowanie dynamiczne. Algorytmy zachłanne. Przeszukiwanie z nawrotami.

Złożoność obliczeniowa algorytmów. Pojęcie złożoności obliczeniowej: złożoność czasowa, złożoność pamięciowa. Asymptotyczna złożoność czasowa: O-notacja, W-notacja, Q-notacja. Złożoność optymistyczna, pesymistyczna i średnia. Złożoność zamortyzowana. Ocena złożoności obliczeniowej algorytmów iteracyjnych. Ocena złożoności obliczeniowej algorytmów rekurencyjnych.

Listy. Rodzaje struktur listowych. Podstawowe operacje na listach. Metody implementacji list.

Kolejki. Kolejka LIFO (stos). Kolejka FIFO. Kolejka priorytetowa. Podstawowe operacje na kolejkach. Implementacja kolejek.

Drzewa binarne. Implementacja drzew binarnych. Podstawowe operacje na drzewach binarnych. Drzewa BST. Drzewa AVL. Drzewa czerwono-czarne. Kopce.

Drzewa wielokierunkowe. Pojęcie i własności B-drzewa. Podstawowe operacje na B-drzewach. Rodzina B-drzew.

Algorytmy sortowania wewnętrznego. Sortowanie przez wstawianie. Sortowanie przez wybieranie. Sortowanie przez zamianę. Sortowanie przez kopcowanie. Sortowanie szybkie. Sortowanie Shella. Analiza złożoności algorytmów sortowania.

Algorytmy sortowania zewnętrznego. Sortowanie przez podział. Sortowanie przez łączenie.

Podstawowe algorytmy grafowe. Reprezentacja grafów. Przeszukiwanie wszerz. Przeszukiwanie w głąb. Wyznaczanie najkrótszych dróg.

Tablice z haszowaniem. Haszowanie. Tablice z adresowaniem bezpośrednim. Tablice z haszowaniem. Funkcje haszujące. Metody usuwania kolizji.

Problemy obliczeniowo trudne. Klasy złożoności problemów. NP-zupełność. NP-zupełność i redukowalność. Nierozstrzygalność.

Efekty uczenia się: Ma uporządkowaną wiedzę z zakresu podstawowych technik konstruowania algorytmów oraz metod oceny ich efektywności. Ma uporządkowaną wiedzę z zakresu podstawowych struktur danych oraz metod ich przetwarzania. Ma szczegółową wiedzę z zakresu oceny złożoności obliczeniowej algorytmów i programów. Potrafi praktycznie wykorzystywać znajomość podstawowych metod oceny złożoności obliczeniowej algorytmów. Umie ocenić wpływ wykorzystanych struktur danych na złożoność obliczeniową projektowanego programu oraz dokonać wyboru optymalnej struktury. Potrafi zgodnie z zadaną specyfikacją wymagań zaprojektować struktury danych oraz algorytm i opracować jego implementację, wykorzystując znajomość podstawowych technik algorytmicznych.

Przedmiot: C.III.6. TEORIA INFORMACJI I KODOWANIA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
III	18	10	12			40	35	75	1,6	1,4	3	Zo	O
Ogółem	18	10	12			40	35	75	1,6	1,4	3	Zo-1	

Cele kształcenia: Nabycie wiedzy w zakresie: standardów kodowania znaków; metod kompresji bezstratnej; metod kodowania nadmiarowego.

Treści kształcenia: Pojęcia wstępne, kod, kod jednoznacznie dekodowalny, natychmiastowy, przedrostkowy. Standardy kodowania znaków: ASCII, ISO/IEC 8859, Unicode, UTF-16, UTF-8. Kompresja bezstratna: twierdzenie Shannona, kodowanie Shannona, kodowanie Huffmana. Kompresja bezstratna: kodowanie arytmetyczne. Kompresja bezstratna: kodowanie słownikowe. Kodowanie nadmiarowe detekcyjne i korekcyjne. Kody liniowe Hamminga. Kody cykliczne. Kody BCH Kody R-S Implementacja metody kompresji bezstratnej. Implementacja funkcji CRC.

Efekty uczenia się: Wiedza (podbudowana teoretycznie) w zakresie:

- standardy kodowania znaków,
- metody kompresji bezstratnej,
- metody kodowania nadmiarowego.

Praktyczna umiejętność tworzenia programów kompresujących dane. Praktyczna umiejętność tworzenia programów wyznaczających wartości CRC.

Przedmiot: C.III.7. PROGRAMOWANIE NISKOPOZIOMOWE I ANALIZA KODU

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
III	14		16			30	20	50	1,2	0,8	2	Zo	O
Ogółem	14		16			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie wiedzy w zakresie: architektury x86; języka wewnętrznego; trybów 32 i 64-bitowego(IA-32 i x64); organizacji wewnętrznej systemów Windows: pamięci, komunikacji z systemem, funkcji API; programów sterowanych zdarzeniami; nabycie umiejętności prowadzenia analizy i inspekcji kodów binarnych różnych typów.

Treści kształcenia: Wprowadzenie do architektury IA32 i x64 Język wewnętrzny procesorów linii 80x86: wybrane rozkazy. Tryby 32 i 64-bitowe. Formaty plików PE. Programy sterowane zdarzeniami. Komunikacja z systemem. Asemblery. Organizacja wewnętrzna systemu Windows – pamięć i komunikacja z procesami. Funkcje API w programowaniu. Programy sterowane zdarzeniami. Reverse engineering, zasady inspekcji kodu binarnego. Modyfikacje niskopoziomowe.

Efekty uczenia się: Znajomość architektury mikroprocesorów linii x86. Znajomość języka wewnętrznego w trybie użytkownika IA-32. Znajomość podstaw asemblerów. Znajomość budowy programów binarnych. Znajomość organizacji pamięci i komunikacji program-system w Windows. Umiejętność prowadzenia analizy i inspekcji kodów binarnych różnych typów. Umiejętność modyfikacji postaci ładowalnych programów. Umiejętność wykorzystania dokumentacji technicznych nowych procesorów.

Przedmiot: C.III.8. PROGRAMOWANIE OBIEKTOWE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IV	20		32			52	25	77	2	1	3	Zo	O
Ogółem	20		32			52	25	77	2	1	3	Zo-1	

Cele kształcenia: Nabycie wiedzy z zakresu: paradygmatu programowania obiektowego oraz zasady użycia podstawowych konstrukcji programowania obiektowego; projektowania i implementacji programów w językach programowania zorientowanych obiektowo.

Treści kształcenia: Koncepcja obiektowości. Klasy i obiekty. Ogólna charakterystyka paradygmatu programowania obiektowego. Składowe klasy. Metody definiowania funkcji klasy. Funkcje wplatane. Operator zakresu. Argumenty domyślne funkcji. Obiekt jako argument funkcji. Ukryty wskaźnik this. Funkcje zwracające obiekty. Funkcje zaprzyjaźnione. Klasy zaprzyjaźnione. Polimorfizm. Przeciążanie funkcji i operatorów. Funkcje przeciążone. Przeciążanie operatorów. Funkcja operatora. Przeciążanie operatorów za pomocą funkcji zaprzyjaźnionych. Funkcje wirtualne. Konstruktory i destruktory. Konstruktory: konstruktory domyślne, konstruktory przeciążone. Wykorzystanie argumentów domyślnych konstruktora. Destruktory. Dziedziczenie. Status dostępu do składowych dziedziczonych. Dziedziczenie jednobazowe i wielobazowe. Kolejność uaktywniania konstruktorów i destruktorów. Szablony funkcji i klas. Funkcje wykorzystujące typy ogólne. Przeciążanie szablonu funkcji. Przykłady zastosowań szablonów funkcji. Szablony klas. Biblioteka STL. Wprowadzenie do STL. Elementy biblioteki STL: kontenery, algorytmy, iteratory, funktory. Klasy kontenerów. Przykłady wykorzystania biblioteki STL. Wprowadzenie do projektowania obiektowego. Modelowanie i projektowanie programów z wykorzystaniem języka UML oraz języka Java. Przykłady modelowania i projektowania programów.

Efekty uczenia się: Ma uporządkowaną, szczegółową wiedzę z zakresu paradygmatu programowania obiektowego. Zna przeznaczenie, zasady budowy i działania oraz zasady użycia podstawowych konstrukcji programowania obiektowego. Ma podstawową wiedzę z zakresu projektowania i implementacji programów w językach programowania zorientowanych obiektowo. Potrafi praktycznie wykorzystywać znajomość podstawowych konstrukcji programowania obiektowego. Umie ocenić konsekwencje wykorzystanych mechanizmów języka programowania zorientowanego obiektowo na jego efektywność, w tym złożoność obliczeniową. Potrafi zgodnie z zadaną specyfikacją wymagań opracować

program, wykorzystując podstawowe mechanizmy i konstrukcje języka programowania zorientowanego obiektowo.

Przedmiot: C.III.9. BAZY DANYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IV	14	12	26			52	25	77	2	1	3	E	O
Ogółem	14	12	26			52	25	77	2	1	3	E-1	

Cele kształcenia: Nabycie wiedzy w zakresie: metodyk wykorzystywanych do modelowania i projektowania baz danych; technik i narzędzi wykorzystywanych w procesie projektowania różnych modeli baz danych; metodyk, technik i narzędzi mod; projektowania baz danych, wykorzystywanych w systemach informatycznych.

Treści kształcenia: Podstawowe pojęcia z zakresu BD (pojęcie BD, definicja SBD, definicja SZBD, podstawowe właściwości SZBD). Model danych (pojęcie modelu danych, zasady projektowania pojęciowego modelu danych, związek pojęciowego modelu z logicznymi modelami hierarchicznej, sieciowej i relacyjnej bazie danych). Relacyjny model danych (struktury danych modelu relacyjnego, zbiory fizyczne i logiczne). Języki opisu danych w systemie relacyjnym (język DDS, język SQL.). Manipulowanie danymi w systemach baz danych o modelu relacyjnym (operacje w języku algebry relacji, operacje selekcji w języku SQL, operacje nawigacyjne). Ograniczenia integralnościowe w relacyjnym modelu (zależności funkcjonalne i wielowartościowe, ograniczenia w postaci predykatów). Projektowanie modeli relacyjnych (dekompozycja bez utraty danych i bez utraty zależności funkcjonalnych, normalizacja schematu). Rozproszone bazy danych (podstawowe pojęcia, fragmentacja, alokacja i replikacja zbiorów w rozproszonych bazach danych, przetwarzanie transakcyjne). Hurtownie danych (pojęcie hurtowni danych, właściwości i zasady tworzenia hurtowni danych).

Efekty uczenia się: Ma uporządkowaną wiedzę w zakresie metodyk wykorzystywanych do modelowania i projektowania baz danych. Ma uporządkowaną wiedzę w zakresie technik i narzędzi wykorzystywanych w procesie projektowania różnych modeli baz danych. Ma uporządkowaną wiedzę w zakresie metodyk, technik i narzędzi modelowania i projektowania baz danych, wykorzystywanych w systemach informatycznych. Potrafi korzystać z różnorodnych technik i narzędzi w procesie projektowania różnych modeli baz danych. Potrafi odzwierciedlić wybrany fragment rzeczywistości w postaci modelu

logicznego i fizycznego dla wybranych obszarów dziedzinowych. Potrafi zaprojektować bazę danych z wykorzystaniem wybranych narzędzi informatycznych.

Przedmiot: C.III.10. ZASTOSOWANIE KRYPTOGRAFII W SYSTEMACH TELEINFORMATYCZNYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IV	10		20			30	45	75	1,2	1,8	3	E	O
Ogółem	10		20			30	45	75	1,2	1,8	3	E-1	

Cele kształcenia: Nabycie umiejętności klasyfikacji rodzajów zagrożeń bezpieczeństwa danych, metod zabezpieczania informacji przed zniszczeniem, niepowołanym dostępem i modyfikacją, zapoznanie z wymaganiami ochrony danych osobowych i informacji niejawnych.

Treści kształcenia: Usługi bezpieczeństwa w systemach teleinformatycznych i metody ich kryptograficznego zapewniania. Zastosowania kryptografii symetrycznej: menedżery haseł, integralność danych, zabezpieczanie nośników informacji, szyfrowane archiwa, metody odzyskiwania dostępu do danych zabezpieczonych kryptograficznie. Zastosowania kryptografii asymetrycznej. Podpis elektroniczny i usługi zaufania. Ochrona danych osobowych w systemach teleinformatycznych: system ochrony informacji, wymagania bezpieczeństwa, metody spełniania wymagań. Ochrona informacji niejawnych w systemach teleinformatycznych.

Efekty uczenia się: Wiedza w zakresie wymagań ochrony danych osobowych. Wiedza w zakresie ochrony informacji niejawnych. Umiejętność doboru i oceny zabezpieczeń systemów teleinformatycznych w zakresie zapewniania poufności, dostępności, integralności i rozliczalności.

Przedmiot: C.III.11. SYSTEMY OPERACYJNE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IV	26		26			52	75	127	2	3	5	E	O
Ogółem	26		26			52	75	127	2	3	5	E-1	

Cele kształcenia: Nabycie umiejętności posługiwania się zbiorem podstawowych poleceń i usług (funkcji systemowych) systemu operacyjnego a także samodzielnej realizacji prostego systemu programowego w postaci współpracujących ze sobą procesów lub wątków z wykorzystaniem niskopoziomowych mechanizmów komunikacji i synchronizacji systemu operacyjnego.

Treści kształcenia: Wprowadzenie, struktury systemów operacyjnych: składowe systemu, usługi systemu operacyjnego, funkcje systemowe, programy systemowe, maszyny wirtualne. Procesy i zasoby w systemach operacyjnych: pojęcie procesu i zasobu. Stany procesu, struktura i atrybuty procesu. Kolejki procesów, przełączanie kontekstu. Powoływanie nowych procesów, wykorzystanie funkcji fork i exec. Funkcje systemowe związane z obsługą procesów w wybranych systemach operacyjnych. Typy zasobów. Sygnały i ich obsługa.

Wątki: procesy lekkie i wątki. Wątki wg standardu POSIX (biblioteka pthread). Wątki w wybranych systemach operacyjnych. Sygnały i ich obsługa w procesach wielowątkowych.

Zarządzanie procesami: planowanie przydziału procesora, planiści. Szeregowanie procesów, metody szeregowania, funkcja priorytetu i jej parametry, przykłady algorytmów planowania przydziału procesora.

Koordynowanie procesów: problem sekcji krytycznej, mechanizmy synchronizacji, klasyczne problemy synchronizacji. Semafory i ich implementacja w systemie operacyjnym. Mechanizmy synchronizacji wątków standardu POSIX.

Komunikacja międzyprocesowa: łącza komunikacyjne nazwane i nienazwane, pamięć dzielona, kolejki komunikatów w systemach operacyjnych.

Zarządzanie pamięcią: przydział obszarów pamięci głównej, stronicowanie, segmentacja. Pamięć wirtualna.

Zarządzanie urządzeniami WE/WY: interakcja jednostki centralnej z urządzeniami wejścia-wyjścia (odpytywanie, sterowanie przerwaniami, bezpośredni dostęp do pamięci).

Buforowanie, spooling i przechowywanie podręczne. Wirtualne wejście-wyjście. Zarządzanie pamięcią pomocniczą: metody przydziału pamięci na dysku, planowanie dostępu do dysku.

System plików: pojęcie pliku i jego atrybuty, logiczny i fizyczny obraz pliku, metody dostępu do pliku, podstawowe operacje na plikach, interfejs dostępu do pliku w systemie UNIX, logiczna organizacja systemu plików.

Fizyczna organizacja systemu plików na dysku, przydział miejsca na dysku, zarządzanie wolną przestrzenią, implementacja katalogu, przechowywanie podręczne w systemie plików, integralność systemu plików.

Przykłady implementacji systemu plików:

systemu plików FAT i FAT32, system plików ISO 9660, wybrane systemy plików Unix/Linux, system plików NTFS, system plików NFS.

Problem blokady (zakleszczenia) i jego rozwiązywanie w systemach operacyjnych: definicja problemu blokady (zakleszczenia), warunki konieczne, graf przydziału zasobów i graf oczekiwania oraz ich własności. Rozwiązywanie problemu zakleszczenia: zapobieganie zakleszczeniom, unikanie zakleszczeń, detekcja i likwidacja zakleszczeń, podejście hybrydowe.

Problem ochrony i bezpieczeństwa w systemach operacyjnych: definicja domeny ochrony, przykłady rozwiązań, zagrożenia dla bezpieczeństwa systemu operacyjnego i ich przezwyciężanie.

Podstawowe cechy systemów Windows. Własności systemów Windows, zarządzanie procesami, prawa dostępu do zasobów w systemach. Monitorowanie wykorzystania zasobów i „strojenie” wybranego systemu Windows.

Systemy operacyjne czasu rzeczywistego.

Sieciowe i rozproszone systemy operacyjne. Tendencje rozwojowe systemów operacyjnych.

Ćwiczenia laboratoryjne:

Środowisko systemu UNIX (Solaris) – polecenia, system pomocy, pliki i katalogi, wybrane programy użytkowe, strumienie, potoki, sterowanie procesami, skrypty, proste programy w języku powłoki. Procesy w systemach UNIX/Linux. Wątki w systemach UNIX/Linux. Sygnały i ich obsługa. Systemy plików, operacje wejścia/wyjścia. Komunikacja międzyprocesowa. Synchronizacja procesów i wątków.

Efekty uczenia się: Znajomość technik zarządzania podstawowymi zasobami sprzętowymi komputera (procesorem, pamięcią operacyjną, wirtualną i urządzeniami wejścia-wyjścia) — oraz ich wpływu na efektywność funkcjonowania systemu komputerowego jako całości. Znajomość podstawowych mechanizmów ochrony zasobów i bezpieczeństwa stosowanych w systemach operacyjnych. Znajomość podstawowych problemów komunikacji i synchronizacji procesów i wątków oraz ich rozwiązań na bazie mechanizmów wspieranych przez system operacyjny. Umiejętność posługiwania się zbiorem podstawowych poleceń i usług (funkcji systemowych) systemu operacyjnego. Umiejętność samodzielnej realizacji prostego systemu programowego w postaci współpracujących ze sobą procesów lub wątków z wykorzystaniem niskopoziomowych mechanizmów komunikacji i synchronizacji systemu operacyjnego.

Przedmiot: C.III.12. ELEMENTY TEORII LICZB

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IV	16	14				30	45	75	1,2	1,8	3	Zo	O
Ogółem	16	14				30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nabycie umiejętności przeprowadzenia prostej analizy systemów kryptograficznych oraz wykorzystania niezbędnej wiedzy matematycznej na potrzeby tej analizy pod kątem zastosowanych technik i zasad ich wykorzystania.

Treści kształcenia: Wprowadzenie podstawowych pojęć, metod i twierdzeń teorii liczb oraz ich zastosowania w kryptografii, metodach obliczeniowych, algorytmach i do rozwiązywania zadań. Liczby naturalne i całkowite – podstawowe definicje, własności i twierdzenia. Zastosowania relacji podzielności oraz kongruencji. Ułamki łańcuchowe. Funkcje arytmetyczne i ich zastosowania. Arytmetyka modularna. Zastosowania Chińskiego twierdzenia o resztach, twierdzenia Eulera i Małego twierdzenia Fermata. Reszty kwadratowe, symbole Legendre'a, Jacobiego. Arytmetyka wielomianów, kongruencje wielomianów. Zastosowania elementów teorii liczb w kryptologii.

Efekty uczenia się: Ma wiedzę z zakresu matematyki obejmującą arytmetykę liczb całkowitych oraz wielomianów, a także elementy teorii liczb niezbędne do rozumienia podstaw kryptologii. Potrafi przeprowadzać prostą analizę systemów kryptograficznych oraz wykorzystać niezbędną wiedzę matematyczną na potrzeby tej analizy pod kątem zastosowanych technik i zasad ich wykorzystania.

Przedmiot: C.III.13. WYBRANE ELEMENTY KRYPTOLOGII

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
V	20		32			52	50	102	2	2	4	E	O
Ogółem	20		32			52	50	102	2	2	4	E-1	

Cele kształcenia: Nabycie wiedzy nabycie wiedzy z zakresu podstaw kryptografii i kryptologii, szyfrów historycznych i współczesnych algorytmów kryptograficznych, a także z zakresu zastosowań kryptografii, bezpieczeństwa stosowanych standardów i zagadnień związanych z kryptografią postkwantową.

Treści kształcenia: Rys historyczny kryptologii. Podstawowe pojęcia kryptografii i kryptologii. Definicja kryptosystemu. Podstawowe szyfry podstawieniowe i przestawieniowe. Szyfry mono- i polialfabetyczne. Elementy kryptoanalizy. Algorytmy strumieniowe i blokowe. Kryptosystemy klucza publicznego. Algorytm RSA i jego bezpieczeństwo. Protokoły kryptograficzne i ich realizacja. Schematy podpisu cyfrowego. Bezpieczeństwo szyfrów i systemów kryptograficznych. Standardy kryptograficzne w zakresie: szyfrów strumieniowych, szyfrów blokowych, funkcji skrótu, kryptosystemów asymetrycznych, w tym opartych na krzywych eliptycznych, protokołów kryptograficznych i bezpiecznych protokołów transmisji. Zagadnienia kryptografii postkwantowej.

Efekty uczenia się: Ma ogólną wiedzę dotyczącą metod i technik kryptograficznych oraz wiedzę w zakresie podstaw kryptologii, protokołów i systemów kryptograficznych. Ma wiedzę dotyczącą szyfrów historycznych i współczesnych algorytmów kryptograficznych. Potrafi przeprowadzić prostą analizę systemów kryptograficznych. Ma także ogólną wiedzę dotyczącą zakresu zastosowań kryptografii w praktyce, zna najważniejsze standardy kryptograficzne i potrafi ocenić ich bezpieczeństwo, Rozumie zagrożenie współczesnej kryptografii związane z komputerem kwantowym i zna podstawowe zagadnienia związanych z kryptografią postkwantową.

Przedmiot: C.III.14. INTERFEJSY KOMPUTERÓW

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
V	16	4	20			40	35	75	1,6	1,4	3	Zo	O
Ogółem	16	4	20			40	35	75	1,6	1,4	3	Zo-1	O

Cele kształcenia: Nabycie umiejętności podstawowego posługiwania się pojęciami za zakresu interfejsów komputerów cyfrowych a także samodzielnej realizacji prostego systemu w postaci urządzeń komunikujących się za pomocą określonego interfejsu.

Treści kształcenia: Interfejs komputera cyfrowego. Systemy i rodzaje interfejsów komputerów. Warstwowy model interfejsu międzykomputerowego. Kanały wejścia-wyjścia współczesnych komputerów: ISA, PCI, PCI-express. Interfejsy klawiatury, myszki, touchpad. Interfejsy urządzeń zobrazowania VGA, AGP, DVI, DP, HDMI. Interfejsy portów równoległych na przykładzie IEEE 1284. Interfejsy telekomunikacyjne i multimedialne: RS232/485, IEEE 1384, HDMI, USB. Interfejsy pamięci zewnętrznych. Interfejsy komputera w BIOS i w systemie operacyjnym.

Efekty uczenia się: Znajomość technik komunikacji i standardów interfejsów wykorzystywanych do komunikacji komputer cyfrowy - urządzenie wejścia-wyjścia. Znajomość sposobów, udostępnianych przez BIOS i system operacyjny, wykorzystywanych w komunikacji komputer urządzenie wejścia-wyjścia. Umiejętność podstawowego posługiwania się pojęciami za zakresu interfejsów komputerów cyfrowych. Umiejętność samodzielnej realizacji prostego systemu w postaci urządzeń komunikujących się za pomocą określonego interfejsu.

Przedmiot: C.III.15. ZASTOSOWANIA KRYPTOGRAFII W INTERNECIE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
V	14		16			30	45	75	1,2	1,8	3	Zo	O
Ogółem	14		16			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nabycie umiejętności sposobu realizacji usług kryptograficznych realizowanych przez współczesne aplikacje internetowe.

Treści kształcenia: Polityka bezpieczeństwa w sieciach otwartych. Usługi poczty elektronicznej w sieciach komputerowych. Systemy bezpiecznej poczty elektronicznej: PGP, PEM. Usługi finansowe. Pieniądz elektroniczny: emisja, obrót, cyberpieniądze typu bitcoin. Narzędzia przeciwdziałania oszustwom przy zachowaniu poufności legalnego klienta. Bezpieczne wybory elektroniczne w sieciach ogólnie dostępnych. Bezpieczne obliczenia w sieciach rozległych. Techniki kryptograficzne w sieciach rozległych. System uwiarygodniania i autoryzacji KERBEROS.

Efekty uczenia się: Umiejętność sposobu realizacji usług kryptograficznych realizowanych przez współczesne aplikacje internetowe, podstawowych funkcji pakietów PGP, PEM i KERBEROS. Znajomość narzędzi i protokołów internetowymi wykorzystującymi kryptografię.

Przedmiot: C.III.16. INŻYNIERIA OPROGRAMOWANIA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
V	12		28			40	60	100	1,6	2,4	4	E	O
Ogółem	12		28			40	60	100	1,6	2,4	4	E-1	

Cele kształcenia: Umiejętność doboru i posłużenia się wybraną metodyką budowy sytemu informatycznego, zaprojektowania systemu informatycznego z wykorzystaniem notacji UML, zamodelowania i zaprojektowana systemu informatycznego z wykorzystaniem wybranych narzędzi wspomagających typu CASE.

Treści kształcenia: Wprowadzenie:

Odpowiedzialność oprogramowania, proces wytwarzania oprogramowania, ewolucja języków i technik programowania, geneza i dziedzina inżynierii, oprogramowania, modele cyklu życia oprogramowania.

Język UML:

Geneza, podstawowe modele, porównanie z innymi językami graficznymi modelowania systemów informatycznych.

Etap definicji wymagań na system informatyczny:

Znaczenie i czynności etapu wymagań, rodzaje wymagań, modelowanie wymagań, weryfikowalność wymagań, zakres dokumentacji wymagań.

Etap analizy systemu informatycznego:

Istota etapu analizy, modele etapu analizy, dokumentowanie etapu analizy.

Etap projektowania systemu informatycznego:

Istota etapu projektowania, modele etapu projektowania, dokumentowanie etapu projektowania.

Etap testowania systemu informatycznego:

Istota etapu testowania, rodzaje testów, dokumentowanie projektu i przebiegu testów.

Wprowadzenie do zarządzania projektem informatycznym.

Efekty uczenia się: Uporządkowana wiedza w zakresie metodyk, technik i narzędzi modelowania i projektowania systemów informatycznych. Uporządkowana wiedza w

zakresie metodyk, technik i narzędzi wytwarzania i wdrażania systemów informatycznych. Podstawowa wiedza z zakresu analizy i modelowania procesów biznesowych w organizacji. Umiejętność doboru i posłużenia się wybraną metodyką budowy sytemu informatycznego, zaprojektowania systemu informatycznego z wykorzystaniem notacji UML, zamodelowania i zaprojektowana systemu informatycznego z wykorzystaniem wybranych narzędzi wspomagających typu CASE. Umiejętność dokonania analizy procesu biznesowego oraz doboru informatycznego narzędzia pracy wspomagające doskonalenie tego procesu. Umiejętność postrzegania projektu informatycznego jako przedsięwzięcia gospodarczego połączona z myśleniem i działaniem w sposób przedsiębiorczy.

Przedmiot: C.III.17. SIECI KOMPUTEROWE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
V	28		24			52	88	140	2	3,5	5,5	E	O
Ogółem	28		24			52	88	140	2	3,5	5,5	E-1	

Cele kształcenia: Nabycie umiejętności: konfigurowania urządzeń sieciowych w lokalnych (przewodowych i bezprzewodowych) i rozległych sieciach komputerowych; realizacji prostych konfiguracji routingu statycznego i dynamicznego.

Treści kształcenia: Wprowadzenie do sieci komputerowych. Konfigurowanie interfejsu sieciowego komputera klasy PC. Arytmetyka sieciowa (ćw.1). Sposoby przyłączania sieci LAN do sieci Internet. Sieciowy elementarz. Terminologia sieciowa: sprzęt sieciowy, topologie, protokoły, LAN, WAN, MAN, SAN, VPN, intranet extranet, przepustowość. Model sieci ISO/OSI. Kapsułkowanie. Media sieciowe: miedziane, optyczne, bezprzewodowe. Parametry i właściwości. Rodzaje, parametry i metody testowania okablowania sieciowego. Wykorzystanie testerów okablowania sieciowego. Okablowanie sieci LAN i WAN. Urządzenia sieci LAN. Zasady tworzenia sieci LAN. Właściwości łączy WAN. Zasady wykorzystania połączeń WAN. Tworzenie sieci LAN w oparciu o koncentrator, przełącznik i bezprzewodowy punkt dostępowy na symulatorze PacketTracer w laboratorium. (ćw.3). Funkcje warstwy łącza danych. Metody dostępu do sieci. Kolizje i domeny kolizyjne. Struktura ramki typu Ethernet. Technologie Ethernetowe Przełączanie w sieciach Ethernet. Tryby przełączania. Protokół STP. Sieci VLAN. Rodzina protokołów TCP/IP.Adresacja IPv4. Klasy adresów. Podsieci. Protokoły warstwy sieciowej: IP, ARP/RARP, ICMP. Analiza zawartości ramek w trakcie transmisji przez sieć (z koncentratorem i przełącznikiem) w symulatorze PacketTracer (ćw.4). Podstawy routingu i podsieci. Routing statyczny

i dynamiczny. Protokoły rutujące i rutowalne. Wyznaczanie podsieci. Maski podsieci. Planowanie adresacji dla sieci. Tworzenie i testowanie sieci obejmującej kilka routerów (PacketTracer) (ćw.6). Protokoły warstwy transportowej. Protokoły połączeniowe i bezpołączeniowe. Funkcjonowanie TCP i UDP. Struktura ramki TCP i UDP. Protokoły warstwy aplikacji: DNS, FTP, HTTP, Telnet, SMTP. Konfigurowanie broadband routera (ćw.5). Odkodowywanie ramek (ćw. 7). Adresacja i właściwości protokołu IPv6.

Efekty uczenia się: Ma elementarną wiedzę w zakresie podstaw telekomunikacji oraz systemów i sieci telekomunikacyjnych. Ma uporządkowaną wiedzę w zakresie zasad funkcjonowania sieci komputerowych. Ma uporządkowaną ogólną wiedzę w zakresie użytkowania podstawowych usług sieciowych oraz projektowania i zarządzania sieciami komputerowymi. Potrafi konfigurować urządzenia sieciowe w lokalnych (przewodowych i bezprzewodowych) i rozległych sieciach komputerowych. Potrafi zrealizować proste konfiguracje routingu statycznego i dynamicznego.

Przedmiot: C.III.18. PROTOKOŁY KRYPTOGRAFICZNE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
V	16		14			30	45	75	1,2	1,8	3	Zo	O
Ogółem	16		14			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nabycie wiedzy w zakresie własności protokołów kryptograficznych i ich zastosowań i umiejętności przeprowadzenia analizy poprawności oraz podstawowej analizy bezpieczeństwa wybranych protokołów kryptograficznych.

Treści kształcenia: Wstęp do protokołów: definicja protokołu, cel stosowania, klasyfikacja protokołów. Podstawowy protokół negocjacji klucza D-H: etapy, czynności uczestników, zagrożenia, modyfikacje protokołu, ogólne zasady konstrukcji protokołów. Protokoły uwierzytelniania. Podział wiadomości poufnych, znakowanie czasowe. Protokoły pośrednie: podpisy cyfrowe z zabezpieczeniem niezaprzeczalności i niepodrabialności. Protokoły pośrednie: grupowe podpisy, obliczenia dla danych zaszyfrowanych. Protokoły zaawansowane: dowody twierdzeń o wiedzy zerowej, dowody tożsamości z zastosowaniem twierdzeń o wiedzy. Protokoły ezoteryczne: niezaprzeczalne przesłanie wiadomości, podpisy jednoczesne, uwierzytelniona poczta elektroniczna. Protokoły ezoteryczne: wymiana jednoczesna, bezpieczne wybory i obliczenia, cyfrowe pieniądze.

Efekty uczenia się: Posiada podstawową wiedzę dotyczącą własności protokołów kryptograficznych i ich zastosowań. na podstawowe metody analizy poprawności i bezpieczeństwa protokołów kryptograficznych. Zna główne ataki na protokoły kryptograficzne. Umie dokonać analizy poprawności oraz podstawowej analizy bezpieczeństwa wybranych protokołów kryptograficznych. Potrafi dokonać implementacji wybranych protokołów kryptograficznych w wybranym przez siebie języku programowania.

Przedmiot: C.III.19. NIEZAWODNOŚĆ SYSTEMÓW KOMPUTEROWYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	14	16				30	20	50	1,2	0,8	2	Zo	O
Ogółem	14	16				30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie umiejętności wyznaczania wartości wskaźników niezawodności systemów komputerowych.

Treści kształcenia: Pojęcia podstawowe, niezawodność obiektów prostych (nienaprawialnych, naprawialnych z odnowami natychmiastowymi, naprawialnych z odnowami nie natychmiastowymi), niezawodność systemów, redundancja, optymalizacja niezawodnościowa.

Efekty uczenia się: Umiejętność wyznaczania wartości wskaźników niezawodności systemów, zapoznanie z pakietami wspomagającymi analizę niezawodnościową systemów.

Przedmiot: C.III.20. BEZPIECZEŃSTWO BAZ DANYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	14		16			30	70	100	1,2	2,8	4	Zo	O
Ogółem	14		16			30	70	100	1,2	2,8	4	Zo-1	

Cele kształcenia: Znajomość podstawowych zagrożeń i ataków oraz metody i techniki zabezpieczania systemów baz danych, umiejętność wykorzystania metod i technik zabezpieczenia systemów baz danych jako elementu systemu informatycznego.

Treści kształcenia: Modele danych i języki przetwarzania w bazach danych. Architektura i eksploatacja systemów baz danych. Zagrożenia oraz metody i techniki zabezpieczania systemów baz danych. Zalecenia i wzorce zwiększające poziom bezpieczeństwa systemów baz danych.

Efekty uczenia się: Zna modele danych stosowane w bazach danych (m.in.: relacyjnych, obiektowych, sieciowych, rozproszonych) oraz języki przetwarzania stosowane bazach danych. Zna architekturę systemów baz danych oraz zasady przetwarzania danych w bazach danych. Zna podstawowe zagrożenia i ataki oraz zna metody i techniki zabezpieczania systemów baz danych. Potrafi umiejętnie wykorzystać metody i techniki zabezpieczeń systemów baz danych jako elementu systemu informatycznego.

Przedmiot: C.III.21. PROCESY STOCHASTYCZNE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	16	14				30	20	50	1,2	0,8	2	Zo	O
Ogółem	16	14				30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie umiejętności obliczania i interpretowania parametrów procesu stochastycznego, analizowania wydajności systemów, wyznaczania prawdopodobieństwa granicznego dla procesów dyskretnych w stanach.

Treści kształcenia: Ciągi losowe. Klasyfikacja i parametry procesów stochastycznych. Przykłady procesów Łańcuchy Markowa. Procesy Markowa. Klasyfikacja stanów. Ergodyczność. Procesy zliczające. Proces urodzeń i śmierci. Systemy kolejkowe.

Efekty uczenia się: Ma wiedzę niezbędną do obliczania i interpretowania parametrów procesu stochastycznego. Zna metody analizowania procesu stochastycznego. Ma wiedzę potrzebną do wyznaczania prawdopodobieństw granicznych dla procesów dyskretnych w stanach. Ma wiedzę potrzebną do projektowania systemów obsługi spełniających określone wymagania. Potrafi obliczać i interpretować parametry procesu stochastycznego. Potrafi analizować wydajności systemów. Potrafi wyznaczać prawdopodobieństwa graniczne dla procesów dyskretnych w stanach. Potrafi projektować systemy kolejkowe spełniające określone wymagania.

Przedmiot: C.III.22. METODY SYMULACJI KOMPUTEROWEJ

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	16		24			40	60	100	1,6	2,4	4	E	O
Ogółem	16		24			40	60	100	1,6	2,4	4	E-1	

Cele kształcenia: Umiejętność posługiwania się zaawansowanymi modelami metodami, narzędziami matematycznymi, a także symulacją komputerową do analizy, oceny oraz usprawniania działania systemów (w tym informatycznych) i rozwiązywania złożonych problemów inżynierskich.

Treści kształcenia: Wprowadzenie do modelowania symulacyjnego. Podstawowe pojęcia, klasyfikacja i założenia metod symulacji komputerowej oraz komputerowych generatorów liczb i procesów losowych. Metody i techniki symulacji dyskretnej krokowej, zdarzeniowej i zorientowanej na procesy. Wybrane języki programowania symulacji dyskretnej. Podstawy wielowątkowości i synchronizacji w języku Java / C#. Konstruowanie programowych mechanizmów symulacji dyskretnej w wybranych językach wysokiego poziomu. Wybrane standardy rozproszonej symulacji komputerowej. Algorytmy upływu czasu i metody sterowania przebiegiem rozproszonego eksperymentu symulacyjnego.

Efekty uczenia się: Ma rozszerzoną i pogłębioną wiedzę w zakresie programowania wysokopoziomowego i niskopoziomowego, algorytmów i struktur danych, programowania strukturalnego i obiektowego. Ma rozszerzoną i pogłębioną wiedzę w zakresie modeli, metod i narzędzi służących do modelowania i rozwiązywania problemów inżynierskich (w tym problemów z zakresu informatyki), a w szczególności metod: sztucznej inteligencji, optymalizacji, numerycznych, oceny niezawodności, oceny efektywności i jakości systemów informatycznych, eksploracji danych. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować informacje, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i uzasadniać opinie. Posługuje się językiem angielskim w stopniu wystarczającym do porozumiewania się, a także czytania za zrozumieniem dokumentacji i instrukcji związanych ze sprzętem, systemami komputerowymi, oprogramowaniem i zaawansowaną inżynierią oprogramowania. Potrafi określić kierunki dalszego uczenia się i zrealizować proces samokształcenia. Potrafi wykorzystać i posługiwać się zaawansowanymi modelami, metodami i narzędziami matematycznymi, a także symulacją komputerową do analizy, oceny oraz usprawniania działania systemów (w tym informatycznych) i rozwiązywania złożonych problemów

inżynierskich. Potrafi współdziałać w zespole realizując w nim różne role i ponosić odpowiedzialność za wspólne przedsięwzięcia.

Przedmiot: C.III.23. STEGANOGRAFIA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	16		14			30	45	75	1,2	1,8	3	Zo	O
Ogółem	16		14			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nabycie umiejętności: posługiwania się podstawowym językiem steganografii i stegoanalizy; wykorzystywania podstawowych kodów korekcji błędów, a także stosowania rachunku macierzowego do ukrywania danych; tworzenia elementarnych algorytmów steganograficznych; projektowania i analizowania prymitywów steganograficznych; projektowania systemów steganograficznych odpornych na wybrane ataki.

Treści kształcenia: Rys historyczny steganografii. Podstawowe pojęcia. Steganografia z kluczem publicznym i kluczem prywatnym. Cyfrowe znaki wodne. Steganografia w obrazach. Podstawowe algorytmy steganograficzne dla grafiki rastrowej – LSB, F5, JSteg. Algorytmy dla kompresji stratnej i bezstratnej. Steganografia audio/wideo. Algorytmy dla zastosowań w plikach multimedialnych. Kompresja stratna i bezstratna. Steganografia sieciowa. Algorytmy ukrywania informacji w protokole TCP/IP oraz danych strumieniowanych. Stegoanaliza. Stegoanaliza wizualna i statystyczna. Test chi-kwadrat, algorytm RS. Metody stegoanalizy uniweralnej. Kodowanie macierzowe. Wet Paper Codes.

Efekty uczenia się: Ma podstawową wiedzę, stanowiącą bazę dla zrozumienia i studiowania przedmiotów kierunkowych, w zakresie algebry z geometrią. Zna podstawowe algorytmy steganograficzne. Poznał i rozumie różnice pomiędzy kryptografią, steganografią a cyfrowym znakowaniem wodnym. Zna podstawowe typy strażników w systemach steganograficznych. Poznał najczęściej stosowane metody stegoanalityczne. Umie posługiwać się podstawowym językiem steganografii i stegoanalizy. Umie wykorzystywać podstawowe kody korekcji błędów, a także stosować rachunek macierzowy do ukrywania danych. Umie tworzyć elementarne algorytmy steganograficzne. Umie projektować i analizować prymitywy steganograficzne. Umie projektować systemy steganograficzne odporne na wybrane ataki. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł (także anglojęzycznych); potrafi interpretować uzyskane informacje i formułować wnioski. Ma wyrobioną wewnętrzną potrzebę i umiejętność ustawicznego uzupełniania

i nowelizacji nabytej wiedzy poprzez samokształcenie. Rozumie potrzebę ciągłego dokształcania się i odświeżania wiedzy, w szczególności związanej ze steganografią i bezpieczeństwem danych.

Przedmiot: C.III.24. DIAGNOSTYKA I TOLEROWANIE USZKODZEŃ

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	16		10	14		40	110	150	1,6	4,4	6	E	O
Ogółem	16		10	14		40	110	150	1,6	4,4	6	E-1	

Cele kształcenia: Nabycie umiejętności: konstruowania prostych testów funkcjonalnych dla współczesnych systemów mikroprocesorowych; przeprowadzania pomiarów w sieciach teleinformatycznych i oceny charakterystyk bazowych sieci; konstruowania algorytmów testowania systemu komputerowego.

Treści kształcenia: Pojęcia podstawowe z zakresu diagnostyki systemów komputerowych. Testowanie i niezawodność układów cyfrowych. Techniki testowania i diagnozowania systemów komputerowych. Testowanie i niezawodność oprogramowania. Diagnostyka systemowa, diagnostyka systemowa sieci teleinformatycznych, Diagnostyka symptomowa sieci teleinformatycznych. Wyznaczanie testów kontrolnych i lokalizacyjnych. Testowanie układów cyfrowych i podzespołów systemu komputerowego. Testowanie systemu z wykorzystaniem magistrali diagnostycznej (IEEE 1149.x). Badanie własności struktur opiniowania diagnostycznego i struktur porównawczych. Wyznaczanie diagnozowalności wybranych sieci procesorowych. Wyznaczanie charakterystyk bazowych sieci komputerowej.

Efekty uczenia się: Znajomość podstawowych technik testowania podzespołów sprzętowych i oprogramowania współczesnych systemów komputerowych. Znajomość własności i zasad projektowania struktur diagnostycznych współczesnych systemów komputerowych. Znajomość technik wyznaczania charakterystyk bazowych sieci teleinformatycznych. Umiejętność konstruowania prostych testów funkcjonalnych dla współczesnych systemów mikroprocesorowych. Umiejętność przeprowadzania pomiarów w sieciach teleinformatycznych i oceny charakterystyk bazowych sieci. Umiejętność konstruowania algorytmów testowania systemu komputerowego.

Przedmiot: C.III.25. SZTUCZNA INTELIGENCJA

Rozliczenie godzinowe

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IV	16		14			30	20	50	1,2	0,8	2	Zo	O
Ogółem	16		14			30	20	50	1,2	0,8	2	Zo - 1	

Cele kształcenia: Umiejętność programowania z wykorzystaniem języków logiki.

Treści kształcenia: Definicja sztucznej inteligencji i obszary jej zastosowań. Systemy formalne - alfabet, formuły poprawnie określone, aksjomaty. Reguły wnioskowania, rachunek zdań, rachunek predykatów, przetwarzanie zbioru klauzul, metody przeszukiwania przestrzeni rozwiązań. Wprowadzenie do języków sztucznej inteligencji - programowanie z wykorzystaniem języka Prolog. Podstawy algorytmów genetycznych. Wprowadzenie w maszynowe uczenie się.

Efekty uczenia się: Znajomość podstawowych pojęć i zakresu zastosowań sztucznej inteligencji. Podstawowa wiedza w zakresie definicji systemów formalnych oraz rachunku predykatów pierwszego rzędu. Podstawowa wiedza w zakresie algorytmów ewolucyjnych.

Umiejętność programowania z wykorzystaniem języków logiki.

8.3. Przedmioty modułu specjalistycznego realizowane w CS/JW

8.3.1. SPECJALNOŚĆ „SYSTEMY KRYPTOGRAFICZNE” C.IV

Ramowy opis przedmiotów

Przedmiot: C.IV.1. METODY STATYSTYCZNE W KRYPTOLOGII

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	10		20			30	70	100	1,2	2,8	4	Zo	O
Ogółem	10		20			30	70	100	1,2	2,8	4	Zo-1	

Cele kształcenia: Nabycie wiedzy w zakresie możliwości wykorzystania programów komputerowych w metodach statystycznych stosowanych w kryptologii; umiejętność analizy danych oraz badania zależności między danymi, a także stosowania testów statystycznych przydatnych w kryptologii.

Treści kształcenia: Charakterystyki opisu statystycznego. Szereg punktowy i przedziałowy. Kwantyle, asymetria, kurtoza. Testy statystyczne: parametryczne i nieparametryczne. Testy dotyczące wartości oczekiwanej i wariancji. Testy porównujące parametry dwóch populacji. Testy zgodności. Analiza współzależności. Współczynnik korelacji z próby i jego własności. Przedział ufności dla współczynnika korelacji. Weryfikacja hipotez dotyczących współczynnika korelacji. Autokorelacja. Istotność autokorelacji. Testy losowości: testy serii, testy kombinatoryczne, test entropii.

Efekty uczenia się: Posiada podstawową wiedzę, stanowiącą bazę dla zrozumienia i studiowania w zakresie metod statystyki w kryptologii. Zna charakterystyki opisu statystycznego. Zna podstawowe testy statystyczne: parametryczne i nieparametryczne dla dużych prób. Zna wybrane testy losowości. Umie stosować podstawowe testy statystyczne: parametryczne i nieparametryczne dla dużych prób do badania własności generatorów liczb losowych. Potrafi stosować testy losowości. Rozumie potrzebę ciągłego dokształcania się i odświeżania wiedzy.

Przedmiot: C.IV.2. PROJEKT ZESPOŁOWY

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI				44		44	58	102	1,7	2,3	4	Z	O
Ogółem				44		44	58	102	1,7	2,3	4	Zo-1	

Cele kształcenia: Umiejętność: wybrania i posłużenia się wybraną metodyką budowy sytemu informatycznego; zaprojektowania systemu kryptograficznego; dobrania środowiska i narzędzi informatycznych wspierających proces projektowania i wdrażania systemu; pacy w zespole.

Treści kształcenia: Metody projektowania algorytmów blokowych i strumieniowych. Metody projektowania algorytmów klucza publicznego. Metody projektowania protokołów kryptograficznych. Analiza bezpieczeństwa wybranych algorytmów i protokołów kryptograficznych. Implementacja wybranych algorytmów i protokołów kryptograficznych.

Przedmiot służy do nauczenia studentów pracy nad analizą, projektowaniem implementacją, a następnie wdrożeniem pewnego systemu kryptograficznego. Przedmiot ma dodatkowo za zadanie nauczyć studentów pracy w zespole.

Efekty uczenia się: Potrafi wybrać i posłużyć się wybraną metodyką budowy sytemu informatycznego; potrafi zaprojektować system kryptograficzny; potrafi dobrać środowisko i narzędzia informatyczne wspierające proces projektowania i wdrażania systemu. Ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżynierskiej, w tym jej wpływu na środowisko, i związanej z tym odpowiedzialności za podejmowane decyzje. Potrafi współdziałać w zespole realizując w niej różne role i ponosić odpowiedzialność za wspólne przedsięwzięcia.

Przedmiot: C.IV.3. FUNKCJE BOOLOWSKIE W KRYPTOLOGII

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	24	20				44	58	102	1,7	2,3	4	E	O
Ogółem	24	20				44	58	102	1,7	2,3	4	E-1	

Cele kształcenia: Poznanie i zrozumienie podstawowych pojęć i twierdzeń dotyczących podstaw matematycznych funkcji boolowskich; nabycie umiejętności zastosowania funkcji boolowskich na potrzeby konstrukcji i kryptoanalizy wybranych szyfrów strumieniowych i blokowych.

Treści kształcenia: Przedstawienia funkcji boolowskich. Algebraiczna postać normalna. Transformata Walsha-Hadamarda. Nieliniowość w sensie Hamminga. Funkcje typu bent i ich konstrukcja. Odporność korelacyjna i kryteria odporności korelacyjnej. Twierdzenie Sigenthalera. Kryteria propagacji. Konstrukcje funkcji boolowskich spełniających kilka kryteriów. Problemy optymalizacji. Zastosowanie kryptograficznych funkcji boolowskich w konstrukcji szyfrów blokowych i strumieniowych.

Efekty uczenia się: Ma wiedzę z zakresu podstawowych faktów i twierdzeń o kryptograficznych własnościach funkcji boolowskich. Ma wiedzę z zakresu zastosowania funkcji boolowskich do konstrukcji blokowych i strumieniowych algorytmów szyfrowania. Potrafi zastosować funkcje boolowskie na potrzeby kryptoanalizy.

Przedmiot: C.IV.4. PROJEKTOWANIE KRYPTOGRAFICZNYCH UKŁADÓW CYFROWYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	20		40			60	65	125	2,4	2,6	5	E	O
Ogółem	20		40			60	65	125	2,4	2,6	5	E-1	

Cele kształcenia: Poznanie i zrozumienie zasad konstruowania złożonych rozwiązań cyfrowych ze szczególnym uwzględnieniem rozwiązań szyfrowania/deszyfrowania informacji, systemów obliczeń kryptograficznych dla technik klucza publicznego.

Treści kształcenia: Wprowadzenie do przedmiotu: ewolucja i stan obecny układów programowalnych: architektury, techniki programowania, narzędzia i metodologia projektowania. Klasyfikacja układów cyfrowych, układy specjalizowane ASIC, struktury programowalne FPGA i CPLD - przegląd architektur bloków logicznych, topologii połączeń i technik programowania. Przegląd rodzin układów CPLD firmy ALTERA; omówienie architektur, parametrów technicznych, możliwości funkcjonalnych i implementacyjnych. Analiza problemu wyboru układu pod kątem aplikacji zapewnienie specyficznych wymagań co do parametrów elektrycznych, charakterystyk dynamicznych, aspektów strategicznych, ekonomicznych itp. Wprowadzenie do narzędzi komputerowego projektowania: proces opracowania układu od opisu do jego realizacji, języki opisu układów i systemów, struktura projektu, biblioteki funkcji standardowych i specjalizowanych, megafunkcje, wirtualne megafunkcje parametryzowane. Charakterystyka systemu MAX+PLUSII: proces tworzenia, optymalizacji i weryfikacji projektu w systemie – podstawowe programy użytkowe systemu, edytory specyfikacji funkcjonalnej, kompilator, edytor kanałów symulacyjnych, symulator, programator. Struktura i zasady tworzenia specyfikacji projektu prostego i złożonego - hierarchicznego przy użyciu edytora schematów logicznych i blokowych, posługiwanie się bibliotekami funkcji standardowych, podprojekt i jego symbol, weryfikacja formalna projektu. Struktura i zasady tworzenia specyfikacji projektu przy użyciu edytora tekstowego w języku ALTERA HDL, podstawowe reguły i konstrukcje języka AHDL, tworzenie symbolu i funkcji włączenia danego podprojektu, konstrukcja projektu złożonego, weryfikacja formalna, lokalizacja i usuwanie błędów. Tworzenie projektów hierarchicznych o mieszanej specyfikacji funkcjonalnej, weryfikacja formalna, usuwanie błędów. Kompilator i jego funkcje, kompilacja projektu: strategie i parametry optymalizacji logicznej i topologicznej, dobór architektury logicznej ze względu na jakość realizacji. Symulator i jego funkcje, edytora przebiegów czasowych i jego podstawowe funkcje, tworzenie przebiegów

testujących, weryfikacja projektu przy użyciu symulatora. Programator, programowanie konwencjonalne, programowanie i konfiguracja w systemie ISP, procedury programowania i testowania fizycznych realizacji, zabezpieczenie aplikacji przed nieuprawnionym odczytem i kopiowaniem.

Efekty uczenia się: Zna i rozumie podstawowe pojęcia i zasady działania elementów elektronicznych i układów cyfrowych. Rozumie pojęcia z zakresu konstruowania, opisu, działania i przeznaczenia układów cyfrowych, interfejsów oraz podzespołów komputerów. Umie posłużyć się wybranymi metodami prototypowania, programowania i konfigurowania wybranych układów cyfrowych, podzespołów komputerów oraz systemów komputerowych. Potrafi samodzielnie planować i realizować własne permanentne uczenie się, pozyskiwać informacje z literatury, baz danych i innych źródeł, dokonywać syntezy i analizy tych informacji. Rozumie potrzebę ciągłego dokształcania się i odświeżania wiedzy, w szczególności związanej ze złożoną strukturą zabezpieczania pomieszczeń.

Przedmiot: C.IV.5. STRUKTURY ALGEBRAICZNE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	20		24			44	58	102	1,7	2,3	4	E	O
Ogółem	20		24			44	58	102	1,7	2,3	4	E-1	

Cele kształcenia: Nabycie wiedzy w zakresie struktur algebraicznych i ilorazowych; znajomość pojęć rozszerzenia ciała, elementu algebraicznego i przestępnego oraz twierdzenia o homomorfizmach.

Treści kształcenia: Elementy teorii grup. Podgrupy, grupy permutacji, grupy cykliczne, warstwy, dzielnik normalny, grupy ilorazowe, kongruencje w grupach, twierdzenia o homomorfizmach. Elementy teorii pierścieni. Podpierścień, pierścień całkowity. Pierścienie wielomianów, ideały, pierścienie ilorazowe, kongruencje w pierścieniach, ideały pierwsze i maksymalne. Elementy teorii ciał. Podciała, rozszerzenie ciała. Wzór interpolacyjny Larange'a. elementy algebraiczne i przestępne. Teoria wielomianów. Wielomiany określone nad ciałem. Pierwiastki wielomianów. Algorytmy faktoryzacji. Wielomiany nierozkładalne. Elementy geometrii algebraicznej.

Efekty uczenia się: Zna podstawowe struktury algebraiczne i ilorazowe. Zna pojęcie rozszerzenia ciała, elementu algebraicznego i przestępnego oraz twierdzenia o homomorfizmach.

Przedmiot: C.IV.6. WSTĘP DO KRYPTOANALIZY ALGORYTMÓW KLUCZA PUBLICZNEGO

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	14		16			30	20	50	1,2	0,8	2	Zo	O
Ogółem	14		16			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Poznanie i zrozumienia przez studentów, trudnych obliczeniowo problemów odpowiadających za bezpieczeństwo klasycznych algorytmów asymetrycznych oraz poznanie wybranych ataków; umiejętność wykonania podstawowej analizy bezpieczeństwa algorytmów opartych o klasyczne problemy klucza publicznego i dokumentowania wyników.

Treści kształcenia: Powstanie i ewolucja kryptologii klucza publicznego; Małe twierdzenie Fermata, Twierdzenie Eulera, RSA i Twierdzenie o poprawności RSA; Problem faktoryzacji. Ułamki łańcuchowe; Atak na RSA z małym kluczem prywatnym (atak diofantyczny). Algorytm faktoryzacji p-1 Pollard'a; Liczby gładkie; Sito Kwadratowe; Faktoryzacja metodą różnicy kwadratów. NFS. Paradoks dnia urodzin; Twierdzenie o kolizjach; Zastosowanie twierdzenia o kolizjach do ataków na problem logarytmu dyskretnego. Pewne ataki kolizyjne; Algorytm Shanks'a. Metoda rho Pollard'a wraz z jej związkami z teorią dyskretnych układów dynamicznych. Algorytm Pohling'a-Hellman'a oraz jego zastosowania.

Efekty uczenia się: Ma uporządkowaną, podbudowaną teoretycznie wiedzę dotyczącą zasadniczych problemów klasycznej (nie postkwantowej) kryptologii asymetrycznej. Ma wiedzę z zakresu metod kryptoanalizy wybranych algorytmów klucza publicznego opartych o problem faktoryzacji oraz DLP. Umie posługiwać się w podstawowym zakresie językiem kryptologii asymetrycznej, wykorzystując właściwe określenia i symbole. Umie dokonać próby ataku na wybrane algorytmy asymetryczne. Umie wykonać podstawową analizę bezpieczeństwa algorytmów opartych o klasyczne problemy klucza publicznego i udokumentować wyniki. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł (także anglojęzycznych); potrafi interpretować uzyskane informacje i formułować wnioski. Ma wyrobioną wewnętrzną potrzebę i umiejętność ustawicznego uzupełniania i nowelizacji nabytej wiedzy poprzez samokształcenie. Rozumie potrzebę ciągłego dokształcania się i odświeżania wiedzy.

Przedmiot: C.IV.7. KRZYWE ELIPTYCZNE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	16		14			30	20	50	1,2	0,8	2	Zo	O
Ogółem	16		14			30	20	50	1,2	0,8	2	Zo-1	

Cel kształcenia: Poznanie i zrozumienie przez studentów podstawowych pojęć związanych z teorią krzywych eliptycznych a także algorytmów i protokołów kryptograficznych wykorzystujących krzywe eliptyczne; nabycie umiejętności dokonania analizy poprawności i bezpieczeństwa wybranych algorytmów i protokołów kryptograficznych wykorzystujących grupę punktów krzywej eliptycznej.

Treść programu: Wstęp do geometrii algebraicznej, krzywe płaskie. Krzywe eliptyczne – podstawowe definicje i twierdzenia. Grupa punktów na krzywej eliptycznej. Rząd grupy punktów na krzywej eliptycznej. Problem logarytmu dyskretnego w grupie punktów na krzywej eliptycznej. Kryptosystemy oparte o grupę punktów krzywej eliptycznej.

Efekty uczenia się: Ma uporządkowana wiedzę w zakresie teorii krzywych eliptycznych i ich związków z szyfrowaniem asymetrycznym, najnowszych wyników na temat kryptosystemów opartych na krzywych eliptycznych, arytmetyki w grupie punktów na krzywej eliptycznej. Zna podstawowe metody obliczania rzędu grupy punktów na krzywej eliptycznej nad ciałem skończonym. Potrafi dokonać analizy poprawności i bezpieczeństwa wybranych algorytmów i protokołów kryptograficznych wykorzystujących grupę punktów krzywej eliptycznej.

Przedmiot: C.IV.8. ZASTOSOWANIE TEORII KRAT W KRYPTOLOGII

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	20		24			44	33	77	1,7	1,3	3	Z	O
Ogółem	20		24			44	33	77	1,7	1,3	3	Zo-1	

Cele kształcenia: Nabycie umiejętności**:** budowy kryptosystemów opartych o kraty; zaimplementowania poznanych algorytmów z zachowaniem wymaganego poziomu bezpieczeństwa.

Treści kształcenia: Funkcje skrótu oparte o kraty. Funkcja SWIFFT. Algorytm GGH oraz jego analiza; Kryptosystem NTRU wraz z jego analizą; Kryptosystem Ajtoi-Dworak'a wraz z uogólnieniami i analizą; Analiza kryptosystemu opartego o LWE; Podpisy elektroniczne oparte na GGH i NTRU; Algorytmy redukcji zwłaszcza LLL wraz z uogólnieniami oraz zastosowaniami w kryptologii.

Przedmiot służy do poznania i zrozumienia przez studentów podstawowych zagadnień dotyczących teorii krat w kontekście ich wykorzystania zarówno w kryptografii jak i kryptoanalizie.

Efekty uczenia się: Zna zasady budowy kryptosystemów opartych o kraty; Potrafi zaimplementować poznane algorytmy z zachowaniem wymaganego poziomu bezpieczeństwa; Potrafi wykorzystać algorytmy redukcji w celach kryptoanalitycznych.

Przedmiot: C.IV.9. ALGORYTMY BLOKOWE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	40	12	8			60	40	100	2,4	1,6	4	E	O
Ogółem	40	12	8			60	40	100	2,4	1,6	4	E-1	

Cele kształcenia: Poznanie i zrozumienie przez studentów podstawowych pojęć z zakresu szyfrów blokowych, szczególnie ich trybów pracy, przykładowych algorytmów, metod kryptoanalizy oraz podstaw projektowania.

Treści kształcenia: Podstawy szyfrowania blokowego. Różnice i podobieństwa do szyfrów strumieniowych. Tryby pracy szyfrów blokowych. Podstawowe komponenty szyfrów blokowych. Typy szyfrów blokowych: sieć Feistela, sieć podstawieniowo-przestawieniowa SPN. Podstawowe szyfry blokowe: DES, IDEA. Wymagania na współczesne algorytmy blokowe. Konkurs AES. Standard AES. Konkurs NESSIE. Bezpieczeństwo szyfrów blokowych. Metody kryptoanalizy. Podstawy projektowania szyfrów blokowych. Kryteria projektowania szyfrów blokowych. Strategia szerokiej ścieżki: podstawowe założenia, warstwa dyfuzji, warstwa nieliniowa, algorytm generowania podkluczy, zapadki. Projekty szyfrów: 3-WAY, BaseKing, SHARK, SQUARE, Rijndael. Projekt szyfry blokowego na bazie innych algorytmów kryptograficznych: Bear i Lion.

Efekty uczenia się: Ma uporządkowaną, podbudowaną teoretycznie, szczegółową wiedzę w zakresie programowania, algorytmów i struktur danych. Ma ogólną wiedzę dotyczącą metod i technik kryptograficznych oraz ma uporządkowaną, podbudowaną teoretycznie, szczegółową wiedzę w zakresie matematycznych podstaw kryptologii, systemów kryptograficznych. Ma wiedzę na temat zasad szyfrowania blokowego, reguł konstruowania komponentów szyfrów blokowych. Ma wiedzę o znanych szyfrach blokowych, zna wymagania stawiane współczesnym szyfrom blokowym. Potrafi wykazać się praktycznymi umiejętnościami z zakresu podstaw informatyki takimi, jak: projektowanie efektywnych algorytmów, szacowanie złożoności algorytmów i budowa automatów skończonych.

Przedmiot: C.IV.10. ALGORYTMY STRUMIENIOWE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	24	6	14			44	33	77	1,7	1,3	3	E	O
Ogółem	24	5	14			44	33	77	1,7	1,3	3	E-1	

Cele kształcenia: Nabycie praktycznych umiejętnościami z zakresu podstaw informatyki i wykorzystać je do projektowania efektywnych algorytmów, szacowania złożoności algorytmów i budowa automatów skończonych.

Treści kształcenia: Zasady szyfrowania strumieniowego. Różnice i podobieństwa do szyfrów blokowych. Tryby pracy szyfrów. Szyfry synchroniczne i samosynchronizujące się. Rejest przesuwający z liniowym sprzężeniem zwrotnym (LFSR) jako generator klucza. Okres i złożoność liniowa generatora. Reguły konstruowania generatorów. Przykłady generatorów, generatory wykorzystujące szyfry blokowe. Ocena jakości generatora. Testy losowości.

Efekty uczenia się: Ma uporządkowaną, podbudowaną teoretycznie, szczegółową wiedzę w zakresie programowania, algorytmów i struktur danych. Ma ogólną wiedzę dotyczącą metod i technik kryptograficznych oraz ma uporządkowaną, podbudowaną teoretycznie, szczegółową wiedzę w zakresie matematycznych podstaw kryptologii, systemów kryptograficznych. Ma wiedzę na temat zasad szyfrowania strumieniowego, reguł konstruowania komponentów szyfrów strumieniowych. Ma wiedzę o znanych szyfrach strumieniowych, zna wymagania stawiane współczesnym algorytmom strumieniowym. Potrafi wykazać się praktycznymi umiejętnościami z zakresu podstaw informatyki takimi, jak: projektowanie efektywnych algorytmów, szacowanie złożoności algorytmów i budowa automatów skończonych.

Przedmiot: C.IV.11. JEDNOKIERUNKOWE FUNKCJE SKRÓTU

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	10	10	10			30	20	50	1,2	0,8	2	Zo	O
Ogółem	10	10	10			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Poznanie i zrozumienie przez studentów podstawowych pojęć z zakresu funkcji skrótu, szczególnie ich zastosowań, zasad konstrukcji, standardowych algorytmów oraz metod kryptoanalizy.

Treści kształcenia: Podstawowe pojęcia i zastosowania funkcji skrótu. Definicje i klasyfikacja. Wymagania bezpieczeństwa. Zastosowania. Zasady konstruowania funkcji skrótu. Konstrukcja iterowana na bazie funkcji kompresji. Konstrukcja Merkle – Damgarda. Przykłady konstrukcji. Konstrukcja gąbki. Standardowe funkcje skrótu: rodzina SHA i MD. Funkcje MD4 i MD5. Funkcje SHA-0 i SHA-1. Rodzina standardu SHA-2. Aktualny stan bezpieczeństwa tych standardów. Nowy standard SHA-3. Konkurs SHA-3. Wymagania na standard. Porównanie konstrukcji kandydatów. Działanie i zastosowania konstrukcji gąbki. Opis funkcji Keccak i jej własności. Aktualne bezpieczeństwo. Metody kryptoanalizy funkcji skrótu. Ataki na SHA-1. Ataki różnicowe funkcji skrótu.

Efekty uczenia się: Posiada wiedzę z zakresu zasad budowy i zastosowań funkcji skrótu, oraz reguł ich konstrukcji. Zna standardowe funkcje skrótu oraz wymagania stawiane współczesnym funkcjom. Umie korzystać z funkcji skrótu w różnych zastosowaniach. Potrafi dokonać krytycznej analizy funkcji skrótu.

Przedmiot: C.IV.12. SYSTEMY ZABEZPIECZEŃ POMIESZCZEŃ

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	10		20			30	20	50	1,2	0,8	2	Zo	O
Ogółem	10		20			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Poznanie i zrozumienie zasad budowy rozwiązań bezpieczeństwa fizycznego obiektów przeznaczonych do przetwarzania informacji niejawnych w sensie ustawy o ochronie informacji niejawnych, danych osobowych oraz obiektów cennych z punktu widzenia materialnego; zapoznanie ze stosowanymi praktycznie rozwiązaniami ochrony fizycznej oraz nauczyć jej planowania.

Treści kształcenia: Wiadomości wstępne, analiza ryzyka, klasyfikacja zagrożeń. Ulot elektromagnetyczny, charakter zjawiska, problemy zabezpieczeń urządzeń przed ulotem EM. Zasady projektowania pomieszczeń przeznaczonych do pracy nad materiałami niejawnymi i danymi osobowymi. Budowa i funkcje systemu alarmowego. Budowa i funkcje systemu kontroli dostępu. Budowa i funkcje systemu telewizji przemysłowej. Budowa i funkcje systemu sygnalizacji pożarowej. Zasady organizacji stref ochronnych. Zasady doboru i oceny skuteczności zabezpieczenia fizycznego, technicznego i organizacyjnego stref ochronnych i obszarów przetwarzania danych.

Efekty uczenia się: Ma wiedzę dotyczącą w zakresie zasad projektowania pomieszczeń przeznaczonych do pracy nad materiałami niejawnymi i danymi osobowymi. Zna budowę i funkcje systemów alarmowego, kontroli dostępu, telewizji przemysłowej oraz sygnalizacji pożarowej. Potrafi zorganizować strefy ochronne. Potrafi dobrać i ocenić skuteczność zabezpieczeń fizycznych, technicznych i organizacyjnych stref ochronnych o obszarów przetwarzania danych.

Przedmiot: C.IV.13. QUANTUM AND POST-QUANTUM CRYPTOLOGY

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	30	14				44	33	77	1,7	1,3	3	E	O
Ogółem	30	14				44	33	77	1,7	1,3	3	E-1	

Cele kształcenia: Poznanie i zrozumienie zagadnień związanych z obliczeniami kwantowymi i ich wpływie na klasyczną kryptologię; poznania podstawowych elementów tzw. Kryptologii postkwantowej.

Treści kształcenia: Podstawowe pojęcia teorii przestrzeni Hilberta oraz mechaniki kwantowej. Kubit, rejestr kwantowy, podstawowe bramki kwantowe, obwody kwantowe. Kwantowa transformata Fouriera i algorytm Shor'a. Algorytm Grouver'a i wnioski. Schematy podpisu elektronicznego oparte o funkcje skrótu. Kryptografia oparta o kraty z naciskiem na takie zagadnienia jak dowody z wiedzą zerową, LWE, RLWE. Elementy kryptografii opartej o teorię kodów oraz o równania z wieloma niewiadomym Stanowisko NIST.

Efekty uczenia się: Ma uporządkowaną, podbudowaną teoretycznie wiedzę obejmującą podstawy informatyki kwantowej w kontekście kryptologicznym. Ma uporządkowaną, podbudowaną teoretycznie wiedzę dotyczącą zasadniczych problemów kryptologii postkwantowej. Umie posługiwać się w podstawowym zakresie językiem informatyki kwantowej oraz kryptologii postkwantowej, wykorzystując właściwe określenia i symbole. Umie wykonać podstawową analizę bezpieczeństwa algorytmów opartych o rozwiązania postkwantowe i udokumentować wyniki. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł (także anglojęzycznych); potrafi interpretować uzyskane informacje i formułować wnioski. Ma wyrobioną wewnętrzną potrzebę i umiejętność ustawicznego uzupełniania i nowelizacji nabytej wiedzy poprzez samokształcenie. Rozumie potrzebę ciągłego dokształcania się i odświeżania wiedzy.

Przedmiot: C.IV.14. NARZĘDZIA KRYPTOANALIZY

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	14		16			30	20	50	1,2	0,8	2	Zo	O
Ogółem	14		16			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Poznanie i zrozumienie zasad konstruowania złożonych rozwiązań cyfrowych ze szczególnym uwzględnieniem rozwiązań szyfrowania/deszyfrowania informacji, systemów obliczeń kryptograficznych dla technik klucza publicznego.

Treści kształcenia: Wprowadzenie do przedmiotu: ewolucja i stan obecny układów programowalnych: architektury, techniki programowania, narzędzia i metodologia projektowania. Klasyfikacja układów cyfrowych, układy specjalizowane ASIC, struktury programowalne FPGA i CPLD - przegląd architektur bloków logicznych, topologii połączeń i technik programowania. Przegląd rodzin układów CPLD firmy ALTERA; omówienie architektur, parametrów technicznych, możliwości funkcjonalnych i implementacyjnych. Analiza problemu wyboru układu pod kątem aplikacji zapewnienie specyficznych wymagań co do parametrów elektrycznych, charakterystyk dynamicznych, aspektów strategicznych, ekonomicznych itp. Wprowadzenie do narzędzi komputerowego projektowania: proces opracowania układu od opisu do jego realizacji, języki opisu układów i systemów, struktura projektu, biblioteki funkcji standardowych i specjalizowanych, megafunkcje, wirtualne megafunkcje parametryzowane. Charakterystyka systemu Quartus Prime: proces tworzenia, optymalizacji i weryfikacji projektu w systemie – podstawowe programy użytkowe systemu, edytory specyfikacji funkcjonalnej, kompilator, edytor kanałów symulacyjnych, symulator, programator. Struktura i zasady tworzenia specyfikacji projektu prostego i złożonego - hierarchicznego przy użyciu edytora schematów logicznych i blokowych, posługiwanie się bibliotekami funkcji standardowych, podprojekt i jego symbol, weryfikacja formalna projektu. Struktura i zasady tworzenia specyfikacji projektu przy użyciu edytora tekstowego w języku VHDL lub Verilog HDL, podstawowe reguły i konstrukcje języka VHDL lub Verilog HDL, tworzenie symbolu i funkcji włączenia danego podprojektu, konstrukcja projektu złożonego, weryfikacja formalna, lokalizacja i usuwanie błędów. Tworzenie projektów hierarchicznych o mieszanej specyfikacji funkcjonalnej, weryfikacja formalna, usuwanie błędów. Kompilator i jego funkcje, kompilacja projektu: strategie i parametry optymalizacji logicznej i topologicznej, dobór architektury logicznej ze względu na jakość realizacji. Symulator i jego funkcje, edytor przebiegów czasowych i jego podstawowe funkcje, tworzenie przebiegów testujących, weryfikacja projektu przy użyciu symulatora.

Programator, programowanie konwencjonalne, programowanie i konfiguracja w systemie ISP, procedury programowania i testowania fizycznych realizacji, zabezpieczenie aplikacji przed nieuprawnionym odczytem i kopiowaniem.

Efekty uczenia się: Zna i rozumie podstawowe pojęcia i zasady działania elementów elektronicznych i układów cyfrowych. Rozumie pojęcia z zakresu konstruowania, opisu, działania i prze-znaczenia układów cyfrowych, interfejsów oraz podzespołów komputerów. Umie posłużyć się wybranymi metodami prototypowania, programowania i konfigurowania wybranych układów cyfrowych, podzespołów komputerów oraz systemów komputerowych. Potrafi samodzielnie planować i realizować własne permanentne uczenie się, pozyskiwać in-formacje z literatury, baz danych i innych źródeł, dokonywać syntezy i analizy tych informacji. Rozumie potrzebę ciągłego dokształcania się i odświeżania wiedzy, w szczególności związanej ze złożoną strukturą zabezpieczania pomieszczeń.

Przedmiot: C.IV.15. GENERACJA I TESTOWANIE LOSOWOŚCI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	20	10	14			44	33	77	1,7	1,3	3	Zo	O
Ogółem	20	10	14			44	33	77	1,7	1,3	3	Zo-1	

Cele kształcenia: Poznanie i zrozumienie metod generacji i testowania ciągów losowych.

Treści kształcenia: Pojęcie losowości. Test statystyczny, procedura testowa. Klasyfikacja i przegląd testów statystycznych. Testowanie generatora. PowerUP Test wg FIPS 140-2, DieHard, DIEHARDER, STS NIST. Generatory losowe oparte o zjawiska fizyczne. Implementacje sprzętowe generatorów losowych.

Efekty uczenia się: Ma wiedzę dotyczącą podstaw konstrukcji generatorów losowych. Ma pogłębioną wiedzę dotyczącą testów losowości i testowania generatorów losowych. Potrafi posługiwać się narzędziami statystycznymi do badania ciągów i generatorów losowych oraz projektowania testów i pakietów testów losowości.

Przedmiot: C.IV.16. TEORIA CIAŁ SKOŃCZONYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	20	10				30	20	50	1,2	0,8	2	Zo	O
Ogółem	20	10				30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie umiejętności rozwiązywania problemu logarytmu dyskretnego a także faktoryzowania wielomianów i konstruowania wielomianów nierozkładalnych.

Treści kształcenia: Elementy teorii ciał skończonych. Ciała skończone, grupa multiplikatywna, automorfizmy. Konstrukcje ciał skończonych. Przykłady ciał skończonych. Bazy w ciałach skończonych. Bazy wielomianowe, bazy normalne. Optymalne bazy normalne. Operacje arytmetyczne w ciałach skończonych. Mnożenie, odwracanie i dzielenie, potęgowanie, logarytmowanie dyskretne. Obliczanie logarytmu dyskretnego. Metody przeszukiwania, metoda Hellmana-Pohliga-Silvera, metoda indeksu.

Efekty uczenia się: Ma wiedzę dotyczącą ciał skończonych, konstrukcji baz, logarytmu dyskretnego w grupach. Zna metody faktoryzacji wielomianów i konstrukcję wielomianów nierozkładalnych. Potrafi konstruować bazy w ciałach skończonych. Potrafi rozwiązywać problem logarytmu dyskretnego. Potrafi faktoryzować wielomiany i konstruować wielomiany nierozkładalne.

Przedmiot: C.IV.17. PROJEKT Z ZAKRESU MATEMATYCZNYCH I INFORMATYCZNYCH PODSTAW KRYPTOLOGII

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	2			28		30	20	50	1,2	0,8	2	Zo	O
Ogółem	2			28		30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie umiejętności: doboru metodyki budowy systemu informatycznego do realizacji wyznaczonego zadania oraz wykorzystywania narzędzi typu CASE do wytworzenia oprogramowania korzystającego z niskopoziomowych mechanizmów synchronizacyjnych i komunikacyjnych systemu operacyjnego; projektowania i implementowania zaawansowanych algorytmów z zakresu kryptologii; dokonywania analizy systemów kryptograficznych (w tym na potrzeby ich akredytacji) oraz wykorzystywania posiadanej wiedzy matematycznej na potrzeby tej analizy.

Treści kształcenia: Omówienie treści Zadania Projektowego. Opracowanie harmonogramu prac w zespołach.

Etap 1: Projekt zadanego prymitywu lub systemu kryptograficznego. Prezentacja wyników realizacji zadania z Etapu 1 i dyskusja na temat poprawności przyjętych rozwiązań. Prezentacje realizują wybrane zespoły.

Etap 2: Implementacja i testowanie zadanego prymitywu lub systemu kryptograficznego. Prezentacja wyników realizacji zadania z Etapu 2 i dyskusja na temat poprawności przyjętych rozwiązań. Prezentacje realizują wybrane zespoły.

Etap 3: Analiza bezpieczeństwa zadanego prymitywu lub systemu kryptograficznego. Prezentacja wyników realizacji zadania z Etapu 3 i dyskusja na temat poprawności przyjętych rozwiązań. Prezentacje realizują wybrane zespoły.

Efekty uczenia się: Znajomość zasad projektowania systemów zorientowanych na usługi kryptograficzne. Znajomość metod i technik kryptograficznych ze szczególnym uwzględnieniem algorytmów kryptograficznych i protokołów kryptograficznych. Umiejętność oszacowania czasu potrzebnego na realizację zadania podczas pracy w zespole na podstawie dostarczonej specyfikacji problemu, dokumentacji i instrukcji związanych ze sprzętem, systemami komputerowymi, oprogramowaniem i zaawansowaną inżynierią oprogramowania, oraz kierunków dalszego uczenia się i samokształcenia. Umiejętność doboru metodyki budowy systemu informatycznego do realizacji wyznaczonego zadania

oraz wykorzystywania narzędzi typu CASE do wytworzenia oprogramowania korzystającego z niskopoziomowych mechanizmów synchronizacyjnych i komunikacyjnych systemu operacyjnego. Umiejętność projektowania i implementowania zaawansowanych algorytmów z zakresu kryptologii. Umiejętność dokonywania analizy systemów kryptograficznych (w tym na potrzeby ich akredytacji) oraz wykorzystywania posiadanej wiedzy matematycznej na potrzeby tej analizy.

Przedmiot: C.IV.18. PROJEKTOWANIE KRYPTOGRAFICZNYCH UKŁADÓW CYFROWYCH II

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	24		36			60	40	100	2,4	1,6	4	Zo	O
Ogółem	24		36			60	40	100	2,4	1,6	4	Zo-1	

Cele kształcenia: Poznanie i zrozumienie przez studentów zaawansowanych zagadnień związanych z implementacją algorytmów i projektowaniem rekonfigurowalnych układów cyfrowych pod kątem zastosowań w kryptologii, nabycie umiejętności zaimplementowania odpowiednich algorytmów kryptograficznych w układzie cyfrowym, chroniąc urządzenie przed znanymi atakami.

Treści kształcenia: Wiadomości wstępne, historia rozwoju i normalizacji języków opisu sprzętu. Podstawy opisu układów cyfrowych w języku VHDL: obiekty, typy (skalarne, złożone, wektorowo-skalarne), atrybuty, instrukcje współbieżne, instrukcje sekwencyjne, funkcje i procedury. Zapoznanie ze środowiskiem Quartus II Web Edition wraz z ModelSim. Implementacja prostych układów kombinacyjnych w języku VHDL. Testowanie implementacji sprzętowej za pomocą TestBench'a języka VHDL w środowisku ModelSim Altera. Implementacja układów kombinacyjnych i sekwencyjnych w języku VHDL. Modelowanie złożonych układów cyfrowych: sposoby opisu, weryfikacja projektów, przykłady. Projekt i implementacja układów dodawania i mnożenia w ciele charakterystyki 2 w bazie wielomianowej. Projekt i implementacja układu mnożenia modularnego w ciele charakterystyki p. Projekt i implementacja układu potęgowania modularnego w ciele charakterystyki p. Projekt i implementacja sprzętowego koprocesora kryptograficznego dla algorytmu AES.

Efekty uczenia się: Ma wiedzę na temat możliwości i ograniczeń systemów projektowych w przypadku wykorzystywania języków opisu sprzętu. Potrafi definiować projekty w języku opisu sprzętu z wykorzystaniem narzędzi wspomagających typu CASE.

Przedmiot: C.IV.19. AKREDYTACJA SYSTEMÓW TELEINFORMATYCZNYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	20		40			60	40	100	2,4	1,6	4	E	O
Ogółem	20		40			60	40	100	2,4	1,6	4	E-1	

Cele kształcenia: Pozyskanie wiedzy w zakresie przeprowadzania procesu akredytacji systemów teleinformatycznych przetwarzających informacje niejawne, organizacji systemu ochrony informacji niejawnych, metod zabezpieczania systemów przetwarzających informacje niejawne przed występującymi zagrożeniami, umiejętność samodzielnego wykonania procesu szacowania i analizy ryzyka, zaprojektowania, skonfigurowania, i wdrożenia systemu przetwarzającego informacje niejawne, w oparciu o opracowaną dokumentację bezpieczeństwa.

Treści kształcenia: Organizacja systemu ochrony informacji niejawnych. Proces akredytacji systemu teleinformatycznego. Zarządzanie ryzykiem w systemach teleinformatycznych przetwarzających informacje niejawne. Dokumentacja bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne. Zasady doboru zabezpieczeń w zakresie bezpieczeństwa osobowego, fizycznego, teleinformatycznego oraz przemysłowego. Opracowanie analizy ryzyka dla przykładowego systemu. Zaprojektowanie skonfigurowanie i wdrożenie przykładowego systemu teleinformatycznego. Opracowanie dokumentacji bezpieczeństwa dla przykładowego systemu teleinformatycznego.

Efekty uczenia się: Ma wiedzę w zakresie organizacji systemu ochrony informacji niejawnych. Ma wiedzę w zakresie procesu akredytacji systemów teleinformatycznych przetwarzających informacje niejawne. Ma wiedzę w zakresie metod metod zabezpieczania systemów przetwarzających informacje niejawne przed występującymi zagrożeniami. Potrafi samodzielnie wyko-nać proces szacowania i analizy ryzyka. Potrafi zaprojektować, skonfigurować, i wdrożyć system przetwarzający informacje niejawne. Potrafi opracować dokumentację bezpieczeństwa.

Przedmiot: C.IV.20. ELEMENTS OF PUBLIC-KEY CRYPTOLOGY

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	20		10			30	20	50	1,2	0,8	2	E	O
Ogółem	20		10			30	20	50	1,2	0,8	2	E-1	

Admission requirements (Treści kształcenia): The course is dedicated to foreign participants and will be realised in English. It shall provide basic knowledge and abilities in constructing and exploiting cryptographic systems and enabling information security. The attendees are expected to be graduated in computer science or electronic engineering and to be familiar with basics of mathematics, information systems and electronics including programmable logic hardware at graduate level.

Effects of study (Efekty uczenia się): A participant who completes the course shall achieve basic knowledge in fields of encryption algorithms, cryptographic module security and information security. A participant shall be conscious of dangers for information confidence and shall be able to manage cryptographic algorithms, to analyse safety of information systems and to estimate effectiveness of corresponding security solutions. The teaching modules are listed in table.

Information on including into Integrated Qualification System: not planned.

Przedmiot: C.IV.21. ATAKI ALGEBRAICZNE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	20		10			30	45	75	1,2	1,8	3	Zo	O
Ogółem	20		10			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nabycie umiejętności dokonania krytycznej analizy szyfrów blokowych i strumieniowych pod kątem podatności na ataki algebraiczne.

Treści kształcenia: Metody rozwiązywania układów równań liniowych. Metody rozwiązywania układów równań nieliniowych. Atak kostek. Odporność algebraiczna funkcji boolowskich. Zastosowanie metod optymalizacji. Wprowadzenie do narzędzi rozwiązywania problemu spełnialności (SAT/SMT). SAT Solvers i ich zastosowania.

Efekty uczenia się: Ma wiedzę na temat metod i narzędzi do rozwiązywania układów równań. Ma wiedzę na temat podstaw kryptoanalizy szyfrów blokowych i strumieniowych z wykorzystaniem metod algebraicznych. Zapoznał się dostępnymi pakietami umożliwiającymi rozwiązywanie układów równań. Potrafi dokonać krytycznej analizy szyfrów blokowych i strumieniowych pod kątem podatności na ataki algebraiczne. Potrafi pozyskiwać informacje z literatury, w tym głównie w języku angielskim.

Przedmiot: C.IV.22. KRYPTOANALIZA ALGORYTMÓW BLOKOWYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	20	4	6			30	45	75	1,2	1,8	3	Zo	O
Ogółem	20	4	6			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Poznanie i zrozumienie podstawowych metod kryptoanalizy szyfrów blokowych, ich stosowalności i złożoności.

Treści kształcenia: Podstawy kryptoanalizy algorytmów blokowych. Podstawy kryptoanalizy różnicowej. Pojęcie charakterystyki. Ataki 1R, 2R, 3R. Charakterystyki iteracyjne. Złożoność czasowa i pamięciowa ataku. Parametr S/N. Kryptoanaliza różnicowa algorytmu DES zredukowanego do 3, 4, 6, 8 rund. Kryptoanaliza różnicowa pełnego DES'a. Podstawy kryptoanalizy liniowej wg Matsui. Kryptoanaliza liniowa wg Bihama. Techniki kryptoanalizy różnicowej. Różniczki niemożliwe. Techniki kryptoanalizy różnicowej. Różniczki obcięte i wyższego rzędu. Techniki kryptoanalizy różnicowej. Ataki sumacyjne. Połączenie kryptoanalizy różnicowej i liniowej. Najnowsze ataki: atak typu bumerang i prostokąt.

Efekty uczenia się: Ma wiedzę na temat podstaw kryptoanalizy szyfrów blokowych, zasad działania podstawowych metod ataków na szyfry blokowych oraz podstawowych technik kryptoanalizy różnicowej. Potrafi dokonać krytycznej analizy szyfrów blokowych oraz wykorzystać niezbędną wiedzę matematyczną na potrzeby tej analizy; potrafi pozyskiwać informacje z literatury w tym głównie w języku angielskim.

Przedmiot: C.IV.23. KRYPTOANALIZA ALGORYTMÓW STRUMIENIOWYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	24		20			44	83	127	1,7	3,3	5	Zo	O
Ogółem	24		20			44	83	127	1,7	3,3	5	Zo-1	

Cele kształcenia: Poznanie i zrozumienie metod kryptoanalizy algorytmów strumieniowych; nabycie umiejętności posługiwania się atakami korelacyjnymi.

Treści kształcenia: Podstawy kryptoanalizy szyfrów strumieniowych. Atak na złożoność liniową generatora. Kryptoanalityczne modele generatora klucza. Podstawy ataków korelacyjnych. Podstawowy atak korelacyjny Sigenthalera. Szybkie ataki korelacyjne. Znajdowanie równań „parity-checks". Atak na generator z filtrem. Atak na generator sumacyjny. Atak na generatory z kontrolowanym zegarem. Kryptoanaliza wybranych algorytmów strumieniowych: LILI, A5.

Efekty uczenia się: Ma wiedzę na temat podstaw kryptoanalizy szyfrów strumieniowych, zasady przeprowadzania ataków korelacyjnych oraz różnych innych technik ataków na algorytmy strumieniowe. Potrafi dokonać krytycznej analizy szyfrów strumieniowych oraz wykorzystać niezbędną wiedzę matematyczną na potrzeby tej analizy; potrafi pozyskiwać informacje z literatury w tym głównie w języku angielskim.

‘

Przedmiot: C.IV.24. METODY NUMERYCZNE W KRYPTOLOGII

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	Kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	20		24			44	83	127	1,7	3,3	5	E	O
Ogółem	20		24			44	83	127	1,7	3,3	5	E-1	

Cele kształcenia: Nabycie umiejętności wybrania i zastosowania, z wykorzystaniem gotowych narzędzi obliczeniowych, metody numerycznego rozwiązywania układu liniowych równań algebraicznych oraz metody rozwiązywania liniowego zadania najmniejszych kwadratów.

Treści kształcenia: Podstawowe pojęcia analizy numerycznej. Arytmetyka stałoprzecinkowa. Arytmetyka zmiennoprzecinkowa. Reprezentacja liczb i błędy zaokrągleń w obliczeniach komputerowych. Uwarunkowanie zadania. Algorytmy numerycznie poprawne i numerycznie stabilne. Normy wektorów i macierzy. Wektory i wartości własne macierzy. Formy kwadratowe. Rozkład macierzy symetrycznej według wartości własnych, postać kanoniczna formy kwadratowej. Bezpośrednie metody rozwiązywania układów liniowych równań algebraicznych. Wskaźnik uwarunkowania macierzy. Metoda Gaussa. Rozkład trójkątno-trójkątny macierzy kwadratowej. Rozkład trójkątno-trójkątny macierzy symetrycznej dodatnio określonej. Metoda Choleskyego-Banachiewicza. Liniowe zadanie najmniejszych kwadratów w postaci algebraicznej. Zadanie nadokreślone z macierzą pełnego rzędu. Algorytm z równaniem normalnym. Uwarunkowanie zadania. Iteracyjne metody rozwiązywania układów liniowych równań algebraicznych. Metody iteracji prostych, Gaussa-Seidela, Jacobiego. Charakterystyki zbieżności. Metoda sprzężonych gradientów.

Efekty uczenia się: Student zna: podstawowe pojęcia analizy numerycznej oraz podstawowe metody numerycznego rozwiązywania układów liniowych równań algebraicznych (bezpośrednie i iteracyjne) i liniowego zadania najmniejszych kwadratów oraz rozumie: metodę wstecznej analizy błędów w obliczeniach komputerowych, pojęcie wartości własnej macierzy i rozkład macierzy według wartości własnych, pojęcie uogólnionej macierzy odwrotnej i rozkład macierzy według wartości szczególnych, pojęcie formy kwadratowej i jej postaci kanonicznej. Student umie wyszukać potrzebne mu informacje z literatury, baz danych i innych źródeł (także anglojęzycznych); potrafi zinterpretować uzyskane informacje, wyciągać wnioski oraz formułować proste problemy z wykorzystaniem metod i pojęć numerycznej algebry liniowej. Student umie wybrać i zastosować z wykorzystaniem gotowych narzędzi obliczeniowych: metodę numerycznego rozwiązywania

układu liniowych równań algebraicznych oraz metodę rozwiązywania liniowego zadania najmniejszych kwadratów. Student rozumie potrzebę nieustannego kształcenia i odświeżania wiedzy, szczególnie w zakresie matematyki.

Przedmiot: C.IV.25. KRZYWE HIPERELIPTYCZNE W KRYPTOLOGII

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	10		10	10		30	70	100	1,2	2,8	4	Zo	O
Ogółem	10		10	10		30	70	100	1,2	2,8	4	Zo-1	

Cele kształcenia: Poznanie i zrozumienie podstawowych pojęć związanych z teorią oraz zastosowaniami krzywych hipereliptycznych w kryptologii; nabycie umiejętności przeprowadzenia gruntownej analizy systemów opartych o problem logarytmu dyskretnego na krzywych hipereliptycznych eliptycznych.

Treści kształcenia: Krzywe hipereliptyczne – podstawowe definicje i twierdzenia. Wielomiany i funkcje wymierne na krzywych hipereliptycznych. Dywizory. Jakobian krzywej hipereliptycznej. Problem logarytmu dyskretnego w jakobianie krzywej hipereliptycznej. Algorytmy i protokoły kryptograficzne oparte na krzywych hipereliptycznych.

Efekty uczenia się: Ma rozszerzoną wiedzę dotyczącą elementów teorii krzywych hipereliptycznych i ich związków z szyfrowaniem asymetrycznym. Posiada wiedzę z zakresu systemów kryptograficznych i protokołów opartych na krzywych eliptycznych i hipereliptycznych. Potrafi przeprowadzić gruntowną analizę systemów opartych o problem logarytmu dyskretnego na krzywych eliptycznych. Potrafi dokonać implementacji wybranego systemu kryptograficznego wykorzystującego teorię krzywych hipereliptycznych w wybranym języku programowania.

8.3.2. SPECJALISTYCZNEGO: SPECJALNOŚĆ „BEZPIECZEŃSTWO INFORMACYJNE" C.IV

Ramowy opis przedmiotów

Przedmiot: C.IV.1. HURTOWNIE DANYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						Niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	14		16			30	20	50	1,2	0,8	2	Zo	O
Ogółem	14		16			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie umiejętności modelowania i konstrukcji hurtowni danych, zasady konstrukcji narzędzi analitycznych wykorzystujących hurtownie danych.

Treści kształcenia: Wprowadzenie do hurtowni danych. Podstawowe pojęcia hurtowni danych. Architektura hurtowni danych. Model wymiarowy hurtowni danych. Modelowanie zmienności w czasie. Model fizyczny hurtowni danych. Mechanizmy zwiększania wydajności zapytań. Projektowanie procesu ETL. Aplikacje analityczno-raportowe OLAP. Metadane – rola w systemie hurtowni danych, system zarządzania metadanymi. Narzędzia budowy hurtowni danych.

Efekty kształcenia: Ma wiedzę w zakresie architektury systemu hurtowni danych. Ma wiedzę w zakresie metod integracji i czyszczenia danych. Ma wiedzę w zakresie mechanizmów bazy danych stosowanych w systemach hurtowni danych. Umie zbudować model danych hurtowni danych. Umie zaprojektować i zaimplementować proces ETL. Umie zbudować aplikację analityczną OLAP.

Przedmiot: C.IV.2. METODY PROGNOZOWANIA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	14		16			30	45	75	1,2	1,8	3	Zo	O
Ogółem	14		16			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nabycie umiejętności wykorzystania/aplikowania prognozowania i symulacji w systemach zarządzania kryzysowego, znajomość metod prognozowania i umiejętności ich aplikowania stosowanie do rozwiązywanych problemów.

Treści kształcenia: Wprowadzenie do prognozowania. Prognozowanie i symulacja w systemach zarządzania kryzysowego. Prognozowanie z wykorzystaniem liniowych modeli trendu. Prognozowanie z wykorzystaniem nieliniowych modeli trendu. Prognozowanie z uwzględnieniem modelu trendu i odchyleń cyklicznych. Regresja wieloraka. Modele adaptacyjne. Modele naiwne i wygładzanie wykładnicze. Modele adaptacyjne Holta i Wintersa.

Efekty kształcenia: Zna metody prognozowania z elementami symulacji. Potrafi konstruować zadania prognostyczne w obszarze bezpieczeństwa oraz dla sytuacji kryzysowych. Umie budować programy komputerowe stosujące metody prognozowania uwzględniające modele regresji i szeregów czasowych.

Przedmiot: C.IV.3. PROGRAMOWANIE W JĘZYKACH FUNKCYJNYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	14		16			30	45	75	1,2	1,8	3	Zo	O
Ogółem	14		16			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nabycie umiejętności posługiwania się językami funkcyjnymi, oraz stosowania zasad programowania obiektowego w języku funkcyjnym, posługiwania się wybranym językiem funkcyjnym.

Treści kształcenia: Interpreter w wybranym języku funkcyjnym, Wykonywanie programu. Typy i operacje. Typy liczbowe. Typy dynamiczne. Łańcuchy znaków. Listy i słowniki. Krotki i pliki. Instrukcje wybranego języka funkcyjnego. Przypisania. Reguły instrukcji If, while, for. Przekazywanie argumentów. Funkcje i wyrażenia lambda. Iterowanie i składanie list. Moduły i operowanie modułami. Klasy, operowanie klasami, projektowanie klas. Kompozycje i dziedziczenie, przeciążanie operatorów. Dekoratory i metaklasy. Sloty i przeciążanie nazw. Wyjątki: try/else; try/finally; try/except/finally; raise; assert. Klasy wyjątków. Projektowanie oparte na wyjątkach. Operowanie łańcuchami znaków. Zarzadzanie atrybutami. Dekoratory.

Efekty kształcenia: Rozumie zasady konstrukcji języka funkcyjnego. Potrafi stosować zasady programowania zorientowanego obiektowo w języku funkcyjnym. Rozumie nowoczesne trendy konstrukcji języków programowania i potrafi wykorzystywać biblioteki specjalizowane w wybranym języku funkcyjnym. Potrafi wykorzystywać elementy struktury wybranego języka funkcyjnego. Potrafi zaprojektować obiektowo kod w języku funkcyjnym. Stosuje wzorce programowania funkcyjnego.

Przedmiot: C.IV.4. METODY NUMERYCZNE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	10		20			30	20	50	1,2	0,8	2	Zo	O
Ogółem	10		20			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie umiejętności stosowania metod numerycznych oraz rozumienia podstawowych pojęć z zakresu algebry liniowej operacji macierzowych i związanych zagadnień numerycznych. Nabycie wiedzy związanych z błędami reprezentacji i operacji na liczbach zmiennoprzecinkowych, jak również metod rozwiazywania układów równań liniowych. Celem kształcenia jest przygotowanie do świadomego stosowania metod aproksymacji i interpolacji zbiorów danych wykorzystywanych w np. w sztucznej inteligencji i systemach ekspertowych.

Treści kształcenia: Podstawowe pojęcia z algebry liniowej: wektor macierz norma, iloczyn skalarny, wartości własne i szczególne, różne postacie macierzy. Macierz i wektor permutacji. Reprezentacja liczby zmiennoprzecinkowej w pamięci komputera. Błąd reprezentacji. Błąd operacji arytmetycznych. Redukcja cyfr znaczących. Norma IEEE 754. Podstawy analizy błędów. Definicja zadania z punktu widzenia obliczeń numerycznych. Algorytm numerycznie poprawny i numerycznie stabilny. Wskaźnik uwarunkowania. Charakterystyka kumulacji błędów. Układy równań liniowych. Metody rozwiązywania układów równań. Wskaźnik uwarunkowania w układach równań. Sposoby faktoryzacji różnych postaci macierzy. Układy równań z macierzą dodatnio określoną. Regularyzacja zadań źle uwarunkowanych. Wybrane metody aproksymacji i interpolacji danych. Regresja liniowa. Interpolacja wielomianowa z optymalnym doborem węzłów. Przegląd procedur i funkcji wybranych bibliotek numerycznych na wybranych przykładach zadań z algebry liniowej.

Efekty kształcenia: Znajomość i rozumienie podstawowych pojęć z algebry liniowej: wektor macierz, norma wektora i macierzy w wybranych zagadnieniach numerycznych. Znajomość normy IEEE754 i konsekwencji zapisu liczb zmiennoprzecinkowych z wykorzystaniem tej normy w tym pojęcie błędu reprezentacji i błędu operacji na liczbach zmiennoprzecinkowych. Znajomość metod rozwiazywania układów równań liniowych z minimalizacją błędu numerycznego z wykorzystaniem algorytmów faktoryzacji. Posiada wiedzę na temat metod aproksymacji i interpolacji zbiorów danych wybranymi metodami. Znajomość sposobów regularyzacji zadań źle uwarunkowanych. Umiejętność minimalizacji

błędu związanego z operacjami na liczbach zmiennoprzecinkowych zapisanych zgodnie ze standardem IEEE754 w algorytmach. Umiejętność formułowania zadań typu ax=b tak, aby propagacja błędu danych na wynik była jak najmniejsza. Umiejętność rozwiązywania układów równań w ax=b dla różnych postaci macierzy a metodami, które minimalizują propagację błędu numerycznego danych Umiejętność wykorzystania metod aproksymacji i interpolacji w wybranych zagadnieniach. Umiejętność wykorzystania procedur i funkcji zawartych w popularnych bibliotekach numerycznych.

Przedmiot: C.IV.5. AUTOMATY I JĘZYKI FORMALNE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	12		18			30	45	75	1,2	1,8	3	E	O
Ogółem	14		16			30	45	75	1,2	1,8	3	E-1	

Cele kształcenia: Posiada umiejętność definicji języków przy pomocy pojęć niedeterministycznego i deterministycznego automatu skończonego oraz formuły regularnej, minimalizować automat skończony, definiować gramatyki i języki bezkontekstowe.

Treści kształcenia: Wzorce i wyrażenia regularne. Deterministyczne automaty skończone. Niedeterministyczne automaty skończone. Równoważność wzorców, wyrażeń regularnych i automatów skończonych. Lemat o pompowaniu dla języków regularnych. Minimalizacja deterministycznych automatów skończonych. Języki bezkontekstowe. Postać normalna Chomsky'ego, jednoznaczność, problem przynależności, algorytm Cocke-Younger'a-Kasami'ego (CYK). Lemat o pompowaniu dla języków bezkontekstowych. EBNF. Automaty ze stosem. Analiza składniowa. Języki kontekstowe. Hierarchia Chomsky'ego. Maszyny Turinga i obliczalność. Języki obliczalne, częściowo obliczalne i nieobliczalne.

Efekty uczenia się: Zna pojęcia niedeterministycznego i deterministycznego automatu skończonego, formuły regularnej, języka regularnego oraz podstawowe twierdzenia dotyczące tego aparatu pojęciowego. Zna pojęcia gramatyki bezkontekstowej, języka bezkontekstowego, drzewa wyprowadzenia, gramatyki jednoznacznej, postaci normalnej gramatyki bezkontekstowej. Umie zastosować języki regularne i bezkontekstowe. Zna metody pokazywania, że język nie należy do klasy. Zna hierarchię Chomsky’ego. Potrafi definiować języki przy pomocy pojęć niedeterministycznego i deterministycznego automatu skończonego oraz formuły regularnej. Potrafi minimalizować automat skończony. Potrafi definiować gramatyki i języki bezkontekstowe. Potrafi konstruować gramatyki jednoznaczne

dla prostych języków. Potrafi stosować lematy o pompowaniu. Potrafi dokonać klasyfikacji języków zgodnie z hierarchią Chomsky'ego.

Przedmiot: C.IV.6. ANALIZA I WIZUALIZACJA DANYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						Niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	14		16			30	45	75	1,2	1,8	3	Zo	O
Ogółem	14		16			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Znajomość statystyk opisowych, metod identyfikacji danych odstających oraz imputacji danych, znajomość metod analizy wariancji, kowariancji, analizy czynnikowej, znajomość metod wizualizacji danych.

Treści kształcenia: Pozyskiwanie, porządkowanie wstępna ocena danych do analizy. Analiza przeglądowa danych: obserwacje odstające, statystyki opisowe, tabele jedno i dwuwymiarowe, faktoryzacja zmiennych. Analiza wariancji. Analiza kowariancji. Analiza czynnikowa. Redukcja wielowymiarowości. Wizualizacja statystyk opisowych i rozkładów (wykres pudełkowy, histogram). Wizualizacja relacji w szeregach czasowych (wykresy: kolumnowy, kolumnowy skumulowany, punktowy, punktowy o dużej gęstości, liniowy, schodkowy, krzywe dopasowania). Wizualizacja proporcji (wykresy: kołowy, pierścieniowy, kolumnowy skumulowany, podział przestrzeni zmiennych - wykres treemap, wykres warstwowy). Wizualizacja relacji za pomocą wykresów: punktowych, bąbelkowych, histogramów, wykresów panelowych (mała wielokrotność, wykresy kratowe). Wizualizacja różnic pomiędzy danymi za pomocą wykresów: mapa termiczna, radarowych, współrzędnych równoległych (paralel coordinatesplot). Wizualizacja danych z wykorzystaniem metod przestrzennych. Tworzenie wykresów interaktywnych, prezentacja wielowymiarowości.

Efekty kształcenia: Umie stosować statystyki opisowe, metody identyfikacji danych odstających oraz imputacji danych. Umie stosować metody analizy wariancji, kowariancji, analizy czynnikowej. Posiada znajomość metod wizualizacji danych. Umiejętność analizy i interpretacji danych. Potrafi dobrać rodzaj wykresu do celu prezentacji i posiadanych danych. Potrafi budować wykresy obrazujące zależności pomiędzy danymi wykorzystując różnorodne środowiska programistyczne (R, JavaScript, Flash Builder). Potrafi odpowiednio określić priorytety służące realizacji określonego przez siebie lub innych zadania.

Przedmiot: C.IV.7. TECHNIKI ALGORYTMICZNE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						Niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	14		4	12		30	45	75	1,2	1,8	3	E	O
Ogółem	14		4	12		30	45	75	1,2	1,8	3	E - 1	

Cele kształcenia: Nabycie umiejętności: stosowania w praktyce różnych technik algorytmicznych; stosowania w praktyce różnych struktur danych. oszacowania złożoności i wrażliwości algorytmów.

Treści kształcenia: Algorytmy i problemy algorytmiczne: pojęcia wstępne. Definicja algorytmu, kryteria jakości algorytmów, złożoność algorytmu i złożoność zadania, stabilność numeryczna algorytmów, zasady projektowania efektywnych algorytmów. Złożoność obliczeniowa algorytmów kombinatorycznych: Rodzaje zadań, sekwencyjne modele obliczeń (DTM i NDTM), transformacje problemów, klasy złożoności obliczeniowej, NP-zupełność, złożoność czasowa i pamięciowa algorytmów (pesymistyczna i oczekiwana), wrażliwość algorytmów (pesymistyczna i oczekiwana), stabilność numeryczna algorytmów, przykłady szacowania złożoności. Algorytmy przybliżone: Metody szacowania dokładności algorytmów. Wielomianowe schematy aproksymacyjne (PTAS), w pełni wielomianowe schematy aproksymacyjne (FPTAS), przykłady algorytmów aproksymacyjnych dla problemów trudnych obliczeniowo. Metody przeszukiwania heurystycznego.

Efekty uczenia się: Zna różne metody określania efektywności algorytmów (dokładności, złożoności). Zna zasady stosowania algorytmów aproksymacyjnych i heurystyk. Zna wpływ stosowania różnych struktur danych oraz technik algorytmicznych na dokładność i złożoność algorytmów. Potrafi stosować w praktyce różne techniki algorytmiczne. Potrafi stosować w praktyce różne struktury danych. Potrafi oszacować złożoność i wrażliwość algorytmów.

Przedmiot: C.IV.8. BUSINESS MODELING IN UML

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	10		20			30	20	50	1,2	0,8	2	Zo	O
Ogółem	10		20			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Umiejętność wypowiadania się, posługując się językiem angielskim, na zagadnienia zawodowe z wykorzystaniem fachowego słownictwa z zakresu informatycznych systemów zarządzania, technik algorytmicznych, niezawodności programowania, architektury korporacyjnej.

Treści kształcenia: Specjalistyczne słownictwo i struktury tekstów mówionych i pisanych, charakterystycznych dla systemów informatycznych. Podstawowa specjalistyczna leksyka i struktury oraz wzorce podstawowych tekstów pisemnych w zakresie: systemów informatycznych, technik algorytmicznych, niezawodności programowania. Specjalistyczne słownictwo i struktury tekstów mówionych i pisanych, charakterystycznych dla informatycznych systemów zarządzania. Podstawowa specjalistyczna leksyka i struktury oraz wzorce podstawowych tekstów pisemnych w zakresie: informatycznych systemów zarządzania, technik algorytmicznych, niezawodności programowania, architektury korporacyjnej.

Efekty uczenia się: Czyta ze zrozumieniem teksty specjalistyczne na poziomie B2+. Rozumie za słuchu teksty specjalistyczne na poziomie B2+. Płynnie wypowiada się na zagadnienia zawodowe z wykorzystaniem fachowego słownictwa z zakresu systemów informatycznych, technik algorytmicznych, niezawodności programowania. Poprawnie i jasno formułuje swoje myśli na piśmie w zakresie systemów informatycznych, technik algorytmicznych, niezawodności programowania. Integruje wszechstronne umiejętności językowe z wiedzą specjalistyczną w sytuacjach zawodowych. Płynnie wypowiada się na zagadnienia zawodowe z wykorzystaniem fachowego słownictwa z zakresu informatycznych systemów zarządzania, technik algorytmicznych, niezawodności programowania, architektury korporacyjnej. Poprawnie i jasno formułuje swoje myśli na piśmie w zakresie informatycznych systemów zarządzania, technik algorytmicznych, niezawodności programowania i architektury korporacyjnej. Integruje wszechstronne umiejętności językowe z wiedzą specjalistyczną w sytuacjach zawodowych.

Przedmiot: C.IV.9. MODELOWANIE I SYMULACJA PROCESÓW BIZNESOWYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	14		16			30	20	50	1,2	0,8	2	Zo	O
Ogółem	14		16			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie umiejętności zamodelowania i zasymulowania procesów biznesowych w średnio skomplikowanej organizacji.

Treści kształcenia: Notacja BPMN. Modelowanie funkcji i procesów biznesowych. Środowiska informatyczne modelowania, analizy i symulacji procesów biznesowych.

Efekty uczenia się: Zna zasady i cele modelowania procesów biznesowych organizacji. Zna notację BPMN. Potrafi zamodelować i zasymulować procesy biznesowe średnio skomplikowanej organizacji.

Przedmiot: C.IV.10. METODY UCZENIA MASZYNOWEGO

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	14		16			30	45	75	1,2	1,8	3	Zo	O
Ogółem	14		16			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nabycie umiejętności konstrukcji i implementacji metod maszynowego uczenia do rozwiazywania określonych grup problemów, wraz z ocena skuteczności działania tych algorytmów.

Treści kształcenia: Rodzaje metod uczenia maszynowego: według metody reprezentacji wiedzy (symboliczne i subsymboliczne), sposobu używania wiedzy (klasyfikacja, klasteryzacja, aproksymacja, reguły asocjacyjne), według źródła i postaci informacji trenującej (uczenie nadzorowane i nienadzorowane), według mechanizmu nabywania i doskonalenia wiedzy (metody indukcyjne i nieindukcyjne). Omówienie wybranych algorytmów w zakresie: uczenia drzew decyzyjnych, indukcji reguł, metod bazujących na pojęciu odległości, klasteryzacji, systemów samoorganizujących się oraz metod klasyfikacji bezwzorcowej i wzorcowej oraz uczenia modeli probabilistycznych. Sztuczne sieci neuronowe.

Efekty kształcenia: Zna klasyfikację metod maszynowego uczenia, zna algorytmy metod maszynowego uczenia ich ograniczenia i zastosowania. Potrafi przypisać algorytmy maszynowego uczenia do określonego problemu i je zaimplementować. Potrafi porównać skuteczność działania poszczególnych algorytmów.

Przedmiot: C.IV.11. METODY PROJEKTOWANIA I WDRAŻANIA SYSTEMÓW INFORMATYCZNYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	30		18	12		60	40	100	2,4	1,6	4	E	O
Ogółem	30		18	12		60	40	100	2,4	1,6	4	E-1	

Cele kształcenia: Znajomość metod analizy i modelowania procesów biznesowych w organizacji oraz najlepszych praktyk z zakresu inżynierii systemów informatycznych; umiejętność modelowania i projektowania systemu z wykorzystaniem wybranych narzędzi wspomagających typu CASE i CAStE.

Treści kształcenia: Modele cyklu życia systemu informatycznego. Standardy i normy wytwarzania i wdrażania systemów informatycznych. Strukturalne metodyki projektowania systemów informatycznych. (Fazy projektowania w podejściu strukturalnym. Czynności w ramach faz. Elementy metodyki CDM. Narzędzia CASE. Designer 6i). Obiektowe metodyki projektowania systemów informatycznych. (Etapy projektowania w podejściu obiektowym. Dyscypliny (procesy) w podejściu obiektowym. Czynności w ramach faz i dyscyplin.

Elementy metodyki RUP. Narzędzia CASE). Zwinne metodyki projektowania systemów informatycznych. (Manifest zwinności. Przegląd metodyk zwinnych dostępnych na krajowym rynku informatycznym. Rozwój metodyk projektowania systemów informatycznych w kierunku metod „zwinnych"). Zorientowane na jakość metodyki projektowania systemów informatycznych (. Model „V". Przegląd metodyk zorientowanych na jakość. Wybrane elementy metodyki RTN.).

Efekty uczenia się: Znajomość metodyk, technik i narzędzi wytwarzania i wdrażania systemów informatycznych. Znajomość modeli cyklu życia systemu informatycznego oraz standardów i norm z zakresu wytwarzania i wdrażania systemów informatycznych. Znajomość metod analizy i modelowania procesów biznesowych w organizacji oraz najlepszych praktyk z zakresu inżynierii systemów informatycznych. potrafi wybrać i posłużyć się wybranym standardem projektowania systemu oraz zastosować odpowiednią metodyką budowy sytemu informatycznego. umie modelować i projektować systemy z wykorzystaniem wybranych narzędzi wspomagających typu CASE i CAStE. potrafi dokonać analizy procesu biznesowego oraz zaproponować informatyczne narzędzia pracy wspomagające doskonalenie tego procesu.

Przedmiot: C.IV.12. METODY EKSPLORACJI DANYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	12		18			30	45	75	1,2	1,8	3	E	O
Ogółem	12		18			30	45	75	1,2	1,8	3	E-1	

Cele kształcenia: Znajomość metod i algorytmów stosowanych w eksploracji danych, metod oceny modeli predykcyjnych oraz obszarów zastosowań metod eksploracji danych.

Treści kształcenia: Pojęcia podstawowe eksploracji danych. Klasyfikacja problemów eksploracji danych. Problemy predykcji, Klasyfikacja. Grupowanie i odkrywanie asocjacji. Narzędzia eksploracji danych. Metodyki eksploracji danych (SEMMA, CRISP-DM). Narzędzia oceny modelu na przykładzie SAS Enterprise Miner. Eksploracja danych tekstowych (text-mining) oraz Web-mining.

Efekty kształcenia: Zna podstawowe metody i algorytmy stosowane w eksploracji danych. Zna metody oceny zbudowanych modeli predykcyjnych. Zna obszary zastosowań metod eksploracji danych. Potrafi poprawnie sklasyfikować problem eksploracji danych i dobrać metodę eksploracji danych do rozwiązania problemów decyzyjnych. Potrafi wykorzystać

narzędzia do budowy procesów eksploracji danych. Potrafi ocenić przydatność zbudowanych modeli klasyfikacyjnych i predykcyjnych.

Przedmiot: C.IV.13. TECHNOLOGIE USŁUGOWE I MOBILNE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						Niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	10		10	10		30	20	50	1,2	0,8	2	Zo	O
Ogółem	10		10	10		30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie umiejętności: budowy oprogramowanie SOA i wdrażania na środowiskach uruchomieniowych; implementacji oprogramowania mobilnego dla platformy Android i Windows Phone.

Treści kształcenia: Podstawy projektowania systemów usługowych. Stosy technologiczne SOA. Praktyczne aspekty implementacji bezpiecznych systemów wykorzystujących podejście SOA. Podstawy projektowania oprogramowania mobilnego. Dobre praktyki konstrukcji aplikacji mobilnych dla platformy Android i Windows Phone. Technologie międzyplatformowe wytwarzania oprogramowania mobilnego. Aspekty bezpieczeństwa platform i oprogramowania mobilnego.

Efekty uczenia się: Potrafi budować oprogramowanie SOA i wdrażać na środowiskach uruchomieniowych. Potrafi implementować systemy usługowe. Zna dobre praktyki implementacji aplikacji mobilnych. Zna wytyczne i zasady konstrukcji bezpiecznego oprogramowania mobilnego. Potrafi implementować oprogramowanie mobilne dla platformy Android i Windows Phone.

Przedmiot: C.IV.14. METODY SZTUCZNEJ INTELIGENCJI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	16		14			30	20	50	1,2	0,8	2	Zo	O
Ogółem	16		14			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Znajomość rachunku predykatów, reguły wnioskowania oraz metody przetwarzania klauzul; potrafi programować w wybranych języku sztucznej inteligencji. modelowania i projektowania systemu z wykorzystaniem wybranych narzędzi wspomagających typu CASE i CAStE;

Treści kształcenia: Reguły wnioskowania, rachunek zdań, rachunek predykatów, przetwarzanie zbioru klauzul, metody przeszukiwania przestrzeni rozwiązań. Systemy formalne. Modele ontologiczne. Wprowadzenie do języków sztucznej inteligencji.

Efekty uczenia się: Zna podstawowe pojęcia sztucznej inteligencji. Zna definicje systemów formalnych. Zna rachunek predykatów, reguły wnioskowania oraz metod przetwarzania klauzul. Potrafi programować w wybranych języku sztucznej inteligencji. Potrafi zbudować prosty model ontologiczny wybranej dziedziny.

Przedmiot: C.IV.15. METODY ILOŚCIOWE ANALIZY RYZYKA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	10	6	14			30	20	50	1,2	0,8	2	Zo	O
Ogółem	10	6	14			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie umiejętności oceny ilościowej ryzyka wystąpienia zagrożeń dla bezpieczeństwa informacji, posługując się wybranymi metodami ilościowymi z zastosowaniem wybranych narzędzi informatycznych.

Treści kształcenia: Metody predykcji zagrożeń, wykorzystanie metod eksperckich, wykorzystanie modeli matematycznych do prognozowania zagrożeń (grafy ataku, modele growe, sieci stochastyczne), modele niezawodności sprzętu i oprogramowania. Identyfikacja podatności: miary powierzchni podatnej na atak; modelowanie procesów biznesowych: podatności danych i funkcji na atak; bezpieczeństwo baz danych. Ocena skutków wystąpienia zagrożeń: dostępność danych i funkcji;

Efekty uczenia się: Zna podstawowe ilościowe metody oceny ryzyka, a w tym metody predykcji zagrożeń, oceny podatności i oceny skutków wystąpienia zagrożeń. Potrafi ocenić ilościowo ryzyko wystąpienia zagrożeń dla bezpieczeństwa informacji, posługując się wybranymi metodami ilościowymi z zastosowaniem wybranych narzędzi informatycznych.

Przedmiot: C.IV.16. BAZY DANYCH NoSQL

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	6		24			30	45	75	1,2	1,8	3	Zo	O
Ogółem	6		24			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nabycie wiedzy na temat architektury systemów baz danych NoSQL, różnic pomiędzy relacyjnymi bazami danych a bazami NoSQL, umiejętność projektowania i implementowania bazy danych NoSQL.

Treści kształcenia: Nierelacyjne bazy danych, architektury i paradygmaty baz NoSQL, przegląd wybranych systemów baz danych NoSQL, języki w bazach NoSQL, przykłady zastosowań baz NoSQL.

Efekty kształcenia: Zna różne architektury systemów baz danych NoSQL. Zna zastosowania różnych typów baz danych NoSQL. Zna cel działania baz danych NoSQL. Zna różnice pomiędzy relacyjnymi bazami danych a bazami NoSQL. Potrafi projektować i implementować bazy danych NoSQL w różnych środowiskach. Potrafi dobrać i odpowiedni typ bazy danych do potrzeb.

Przedmiot: C.IV.17. BEZPIECZEŃSTWO SYSTEMÓW INFORMACYJNYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	16		14			30	45	75	1,2	1,8	3	Zo	O
Ogółem	16		14			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nabycie umiejętności: przeprowadzenia jakościowej analizy ryzyka dla typowych systemów informatycznych; zaproponowania strategii postępowania z ryzykiem.

Treści kształcenia: Jakościowa analiza ryzyka: identyfikacja zasobów i ich wartościowanie, klasyfikacja zagrożeń, identyfikacja podatności i metody ich szacowania, identyfikacja skutków zagrożeń, jakościowe podejście do szacowania ryzyka, standardy opisu. Strategie postępowania z ryzykiem. Jakościowa analiza ryzyka w świetle standardów.

Efekty uczenia się: Zna standardy określające zasady przeprowadzania analizy ryzyka. Potrafi przeprowadzić jakościową analizę ryzyka dla typowych systemów informatycznych. Potrafi zaproponować strategię postępowania z ryzykiem.

Przedmiot: C.IV.18. METODY I SYSTEMY WSPOMAGANIA DECYZJI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	14		8	8		30	45	75	1,2	1,8	3	Zo	O
Ogółem	14		8	8		30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nabycie umiejętności: klasyfikacji problemu i doboru narzędzi informatycznych w procesie wspomaga decyzji; formułowania i rozwiązywania zadań z wykorzystaniem narzędzi informatycznych**.**

Treści kształcenia: Identyfikacja procesów decyzyjnych. Teoretyczne ograniczenia. automatycznego podejmowania decyzji. Modele procesów decyzyjnych w wybranej klasie systemów, formułowanie zadań decyzyjnych w oparciu o przyjęte modele z wykorzystaniem metod optymalizacji. Prognostyczne modele decyzyjne. Wstęp do projektowania systemów wspomagania decyzji. Technologia współpracy decydenta z SWD. Projektowanie systemu SWD dla określonego. systemu zarządzania lub kierowania, (opracowanie systemu. językowego, systemu wiedzy oraz systemu przetwarzania zadań), formułowanie zadań projektowych dla SWD. Konstrukcja algorytmów wspomagania decyzji dla wyspecyfikowanych zadań decyzyjnych. Metody weryfikacji algorytmów wspomagania decyzji. Hurtownie danych, metody eksploracji danych (Data Mining), Web Mining (nurty Web Miningu, prezentacja wybranych metod). Formułowanie i rozwiązywanie zadań decyzyjnych z wykorzystaniem. wybranych informatycznych narzędzi wspomagania decyzji (Solver for Excel, R, GAMS, SAS).

Efekty uczenia się: Znajomość metod identyfikacji procesów decyzyjnych. Znajomość zasad budowania modeli decyzyjnych. Znajomość zasad projektowania systemów wspomagania wiedzy. Umiejętność klasyfikacji problemu i doboru narzędzi informatycznych w procesie wspomaga decyzji. Umiejętność formułowania i rozwiązywania zadań z wykorzystaniem narzędzi informatycznych.

Przedmiot: C.IV.19. PODSTAWY KRYPTOLOGII WSPÓŁCZESNEJ

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						Niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	14		16			30	20	50	1,2	0,8	2	Zo	O
Ogółem	14		16			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie wiedzy na temat metod konstrukcji współczesnych systemów kryptograficznych.

Treści kształcenia: Systemy kryptograficzne. Bezpieczeństwo systemów kryptograficznych. Formalne metody oceny bezpieczeństwa systemów kryptograficznych. Podstawy kryptoanalizy. Kryptosystemy symetryczne: algorytmy blokowe i strumieniowe. Kryptosystemy asymetryczne. Funkcje skrótu. Protokoły kryptograficzne. Współczesne zastosowania kryptografii.

Efekty uczenia się: Ma wiedzę na temat metod konstrukcji współczesnych systemów kryptograficznych. Potrafi ocenić bezpieczeństwa współczesnych systemów kryptograficznych oraz wykorzystać niezbędną wiedzę matematyczną na potrzeby tej oceny; potrafi pozyskiwać informacje z literatury w tym głównie w języku angielskim.

Przedmiot: C.IV.20. MODELOWANIE I ANALIZA SIECI ZŁOŻONYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						Niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	18	10	16			44	33	77	1,7	1,3	3	E	O
Ogółem	18	10	16			44	33	77	1,7	1,3	3	E-1	

Cele kształcenia: Umiejętność zamodelowania wybranych obiektów rzeczywistych z wykorzystaniem sieci złożonych i wyznaczenia wartości wybranych ilościowych charakterystyk tych obiektów z wykorzystaniem procedur numerycznych i symulacyjnych.

Treści kształcenia: Modele sieci złożonych. Dynamika sieci złożonych. Sieci społecznościowe (w tym wirtualne sieci społecznościowe). Charakterystyki sieci teleinformatycznych (w szczególności sieci Internet). Identyfikacja zespołów i ról w sieciach złożonych. Wyznaczanie charakterystyk sieci złożonych. Algorytmy wyszukiwania w sieciach złożonych. Modelowanie i symulacja rozprzestrzeniania się zjawisk (wirusy komputerowe, informacja, plotka) w sieciach złożonych.

Efekty uczenia się: Zna podstawowe definicje, typy i własności sieci złożonych. Zna podstawowe charakterystyki ilościowe sieci złożonych i metody wyznaczania ich wartości. Potrafi zamodelować wybrane obiekty rzeczywiste z wykorzystaniem sieci złożonych i wyznaczyć wartości wybranych ilościowych charakterystyk tych obiektów z wykorzystaniem procedur numerycznych i symulacyjnych.

Przedmiot: C.IV.21. ROZPROSZONE PRZETWARZANIE DANYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						Niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	14		30			44	33	77	1,7	1,3	3	Zo	O
Ogółem	14		30			44	33	77	1,7	1,3	3	Zo-1	

Cele kształcenia: Zapoznać z architekturami i środowiskami przetwarzania danych masowych w idei Big Data, trendami i kierunkami rozwoju systemów przetwarzania danych masowych. Nauczyć procedur transformacji danych masowych na platformie Hadoop w paradygmacie Map Reduce, implementacji procedur transformacji danych strumieniowych.

Treści kształcenia: Zasady dostępu i korzystania z rozproszonych baz danych, realizacja transakcji w rozproszonych bazach danych, zapytania do rozproszonych baz danych, wykorzystanie systemów baz danych w chmurze, bezpieczeństwo w rozproszonych bazach danych, ćwiczenia z wykorzystaniem rozproszonych baz danych w wybranych technologiach. Geneza systemów przetwarzania danych masowych: hurtownie danych i Big Data. Metody przetwarzanie danych masowych w trybie wsadowym (paradygmat Map Reduce) i strumieniowym. Stos technologiczny Apache Hadoop i Apache Spark jako przykłady aktualnego kierunku rozwoju narzędzi open source dla Big Data. Wykorzystanie narzędzi rozproszonego przetwarzania danych w zadaniach eksploracji danych, w tym z wykorzystaniem modeli i metod uczenia maszynowego. Wzorce projektowe i architektoniczne rozproszonego przetwarzania danych, np. architektura Lambda i Kappa.

Efekty kształcenia: Posiada znajomość architektury i środowisk przetwarzania danych masowych Big Data. Znajomość trendów i kierunków rozwoju systemów przetwarzania danych masowych. Umiejętność implementacji procedur transformacji danych masowych na platformie Hadoop w paradygmacie Map Reduce. Umiejętność implementacji procedur transformacji danych strumieniowych. Umiejętność wykorzystania narzędzi rozproszonego przetwarzania danych do rozwiązywania zadań eksploracji danych. Znajomość roli narzędzi w stosie technologicznym Hadoop.

Przedmiot: C.IV.22. ZARZĄDZANIE PROJEKTAMI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	16		14			30	45	75	1,2	1,8	3	Zo	O
Ogółem	16		14			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Zapoznać z zagadnieniami zarządzania projektami, w tym zarządzania jakością, ryzykiem i logistyką projektu informatycznego; Umiejętność stosowania zasady prowadzenia, zarządzania i kierowania projektami informatycznymi w różnej skali - od względnie małych do dużych projektów. Przedstawić standardy i podstawowe metodyki zarządzania projektami; oraz podstawowymi metodami z zakresu zarządzania projektami.

Treści kształcenia: Podstawy zarządzania projektami. Studium wykonalności projektu. Podstawowe procesy zarządzania projektem. Procesy rozpoczęcia. Procesy i planowania projektu. Procesy realizacji i kontroli. Procesy monitorowania i zamykania projektu. Podstawowe elementy metodyki prince2. Analiza jakościowa projektu. Tendencje rozwojowe zarządzania projektami.

Efekty uczenia się: Ma podstawową wiedzę dotyczącą zarządzania projektami, w tym zarządzania jakością, ryzykiem i logistyką projektu informatycznego; Zna i rozumie zasady prowadzenia, zarządzania i kierowania projektami informatycznymi w różnej skali - od względnie małych do dużych projektów. Rozumie standardy i podstawowe metodyki zarządzania projektami; zna i rozumie podstawowe metody z zakresu zarządzania projektami - metody zarządzania zakresem projektu, czasem, kosztami, jakością, zasobami, ryzykiem, komunikacją, integracją i zamówieniami. Zna i rozumie zagadnienia dotyczące: rozpoczynania projektu informatycznego i definiowania jego zakresu; planowania projektu informatycznego; realizacji, kontroli i koordynacji projektu informatycznego oraz zamykania, akceptacji i zapewniania wsparcia dla projektu informatycznego. Potrafi opracować dokumentację projektu; potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować informacje, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i uzasadniać opinie. Potrafi wykonywać funkcję kierownika projektu oraz sformułować i zbudować organizację realizującą projekt informatyczny; Potrafi pracować indywidualnie i w zespole, umie oszacować czas realizacji zadania, potrafi opracować i zrealizować harmonogram prac; Potrafi opracować bazowy plan wykonania projektu oraz zarządzać całym procesem realizacji projektu oraz procesem kontroli zmian i strategią zamknięcia projektu. Potrafi opracować strukturę podziału pracy w

projekcie i na jej podstawie wyznaczyć budżet oraz harmonogram projektu. Potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć w zakresie współczesnych modeli zarządzania projektami.

Przedmiot: C.IV.23. ILOŚCIOWE METODY OCENY BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	14		16			30	20	50	1,2	0,8	2	Zo	O
Ogółem	14		16			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Znajomość zaawansowanych metody monitorowania i wykrywania zagrożeń da bezpieczeństwa informacyjnego; umiejętność zamodelowania i oceny ilościowej skuteczności i wydajności systemów bezpieczeństwa informacyjnego.

Treści kształcenia: Monitorowanie ryzyka. Wykrywanie ataków z wykorzystaniem: analizy szeregów czasowych, rozpoznawanie wzorców, analizy sygnatur, analizy anomalii, sieci stochastycznych, modeli sieci społecznościowych. Monitorowanie otoczenia: sensory, fuzja danych, wykrywanie botnetów Identyfikacja nowych zagrożeń, wykrywanie ataków APT. Struktura systemu bezpieczeństwa. Ocena skuteczności i wydajności pojedynczych zabezpieczeń. Optymalizacja struktury systemu zabezpieczeń. Modelowanie. Ocena skuteczności i wydajności. Metody optymalizacji. Symulacja systemu bezpieczeństwa. Optymalizacja planów zapewnienia informacyjnej ciągłości działania.

Efekty uczenia się: Zna zaawansowane metody monitorowania i wykrywania zagrożeń da bezpieczeństwa informacyjnego. Potrafi wykorzystać wybrane metody monitorowania ryzyka. Potrafi zamodelować i ocenić ilościowo skuteczność i wydajność systemów bezpieczeństwa informacyjnego.

Przedmiot: C.IV.24. ZAAWANSOWANE METODY UCZENIA MASZYNOWEGO

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	10		20			30	45	75	1,2	1,8	3	E	O
Ogółem	10		20			30	45	75	1,2	1,8	3	E-1	

Cele kształcenia: Zapoznać z pojęciami z zakresu sztucznych sieci neuronowych, zasadami głębokiego uczenia się, konwolucyjnymi sieciami neuronowymi i ich zastosowaniami. Nauczyć zaprojektowania i implementacji sieci neuronowych do rozwiazywania wybranego problemu.

Treści kształcenia: Metody i algorytmy uczenia maszynowego – wprowadzenie. Sztuczne sieci neuronowe w uczeniu maszynowym. Metody głębokiego uczenia. Sieci konwolucyjne. Sieci rekurencyjne. Złożone systemy uczące się.

Efekty kształcenia: Posiada wiedzę z zakresu sztucznych sieci neuronowych. Zna zasadę głębokiego uczenia się. Posiada wiedzę na temat konwolucyjnych sieci neuronowych i ich zastosowań. Potrafi zaprojektować i zaimplementować konwolucyjną sieć neuronową do wybranego problemu. Potrafi wytrenować sieć neuronową i ocenić skuteczność jej działania.

Przedmiot: C.IV.25. TEORIA WOJNY INFORMACYJNEJ

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	16		14			30	20	50	1,2	0,8	2	Zo	O
Ogółem	16		14			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Znajomość metod modelowania, umiejętność stosowania metod badań operacyjnych, w tym symulacji komputerowej, do oddziaływania i obrony w cyberprzestrzeni.

Treści kształcenia: Formy działań w cyberprzestrzeni: CYBEROPS, INFOOPS, PSYOPS. TTP (ang. Tactics, Techniques and Procedures) stosowane do prowadzenia wojny w cyberprzestrzeni: operacje psychologiczne; strategie prowadzenia działań w cyberprzestrzeni; kierowanie działaniami w cyberprzestrzeni: planowanie działań, monitorowanie, sterowanie działaniami. Modele walki (prowadzenia operacji) w cyberprzestrzeni. Modele, metody i narzędzia identyfikacji, rozpoznania i oceny możliwości oddziaływania informacyjnego. Modele, metody i narzędzia przeciwdziałania oddziaływaniu informacyjnemu. Symulacja procesów walki (prowadzenia operacji) w cyberprzestrzeni. Zdolności do prowadzenia działań w cyberprzestrzeni.

Efekty uczenia się: Zna modele i metody analizy stosowane w wojnie informacyjnej. Stosuje narzędzia identyfikacji, rozpoznania i oceny możliwości oddziaływania informacyjnego. Zna formy i procedury działań w cyberprzestrzeni. Zna metody modelowania i symulacji działań w cyberprzestrzeni. Potrafi stosować metody badań operacyjnych, w tym symulacji komputerowej, do oddziaływania i obrony w cyberprzestrzeni. Potrafi ilościowo ocenić skutki działań w cyberprzestrzeni z wykorzystaniem wybranych narzędzi informatycznych.

Przedmiot: C.IV.26. TECHNOLOGIE INTERNETU RZECZY

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	20		24			44	58	102	1,7	2,3	4	E	O
Ogółem	20		24			44	58	102	1,7	2,3	4	E-1	

Cele kształcenia: Zapoznać z zagadnieniami dotyczącymi sieci teleinformatycznych, w tym usług oferowanych przez systemy IoT oraz systemy sieciowe, nauczyć projektowania i zarządzania sieciami, niezawodności, bezpieczeństwa sieciowego. Nauczyć metod i teorii w obszarze modelowania i projektowania systemów Internetu Rzeczy.

Treści kształcenia: Oprogramowanie i sprzęt: systemy operacyjne dla urządzeń IoT, wybrane języki i biblioteki oprogramowania. Oprogramowanie middleware. Brokerzy i usługi w IoT. Protokoły komunikacji i dystrybucji danych w IoT (MQTT, CoAP i inne).

Przetwarzanie w chmurze. Dostęp do serwerów w chmurze na przykładzie Microsoft Azure IoT, Amazon AWS, Arduino Cloud.

Problemy interoperacyjności w sieciach IoT i ich rozwiązywanie. Integracja danych oparta na semantyce danych, wykorzystanie ontologii. Standaryzacja w zakresie budowy bram dostępu do zasobów i usług. Zarządzanie zasobami w środowisku federacji.

Problemy bezpieczeństwa systemów IoT. Charakterystyka zagrożeń. Bezpieczeństwo end-to-end. Kryptograficzna kontrola dostępu do danych. Uwierzytelnianie i autoryzacja urządzeń IoT. Bezpieczeństwo urządzeń, budowa i zastosowanie układów typu TPM (Trusted Platform Modules).

Problemy zarządzania tożsamością i zaufaniem w IoT. Budowa domen zaufania. Zastosowanie rejestrów rozproszonych i technologii blockchain. Przykładowe rozwiązania dla bezpieczeństwa w wojskowych systemach IoT.

Efekty kształcenia: Zna i rozumie w pogłębionym zakresie zagadnienia dotyczące sieci teleinformatycznych, w tym usług oferowanych przez systemy IoT oraz systemów sieciowych, projektowania i zarządzania sieciami, niezawodności, bezpieczeństwa sieciowego. Zna w pogłębionym stopniu wybrane fakty, obiekty i zjawiska oraz dotyczące ich metody i teorie w obszarze modelowania i projektowania systemów teleinformatycznych, w tym systemów Internetu Rzeczy. Potrafi dokonać krytycznej analizy istniejących rozwiązań technicznych w obszarze modelowania i projektowania systemów Internetu Rzeczy. Umie planować i przeprowadzać eksperymenty w obszarze systemów

przetwarzania danych z wykorzystaniem systemów SOA, ROA oraz środowisk cloud computing. Umie interpretować i oceniać uzyskane wyniki i wyciągać wnioski.

Przedmiot: C.IV.27. PRZETWARZANIE JĘZYKA NATURALNEGO (NLP)

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	12		18			30	45	75	1,2	1,8	3	Zo	O
Ogółem	12		18			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Zapoznać z podstawowymi pojęciami związanymi z dziedziną przetwarzania języka naturalnego. Nauczyć metod analizy syntaktycznej i semantycznej zdań języka naturalnego. Nauczyć budowy narzędzi informatycznych wspomagających pracę w dziedzinie lingwistyki.

Treści kształcenia: Omówienie dziedziny maszynowego przetwarzania języka naturalnego, analiza syntaktyczna i semantyczna zdań zapisanych w języku naturalnym, analiza korpusów tekstów, n-gramy, algorytmy wyszukiwania kolokacji wyrazowych, modele statystyczne języków naturalnych, analiza sentymentu, przykłady zastosowań systemów przetwarzania języka naturalnego.

Efekty kształcenia: Zna i rozumie podstawowe pojęcia związane z dziedziną przetwarzania języka naturalnego. Posiada wiedzę na temat metod analizy syntaktycznej i semantycznej zdań języka naturalnego. Posiada wiedzę dotyczącą metod statystycznej analizy tekstów. Potrafi budować statystyczne modele do przetwarzania języka naturalnego. Potrafi opracowywać narzędzia informatyczne wspomagające pracę lingwistów.

Przedmiot: C.IV.28. PROJEKT Z ZAKRESU BEZPIECZEŃSTWA INFORMACJI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX				44		44	58	102	1,7	2,3	4	Zo	O
Ogółem				44		44	58	102	1,7	2,3	4	Zo-1	

Cele kształcenia: Zapoznać z metodami analizy problemu, wyboru odpowiedniej metody analitycznej. Nauczyć wykorzystania istniejących technologii rozproszonego masowego przetwarzania danych.

Treści kształcenia: Analiza zadania projektowego, określenie celu analizy danych w zakresie bezpieczeństwa informacji. Określenie ról w projekcie i przypisanie zadań do poszczególnych ról. Analiza dostępności i zakresu dostępnych danych niezbędnych do realizacji zadnia projektowego. Dobór metod analizy danych niezbędnych do wykonania zadania. Analiza wymagań na środowisko obliczeniowe. Wybór i konfiguracja systemów rozproszonego i masowego przetwarzania danych. Dobór metod wizualizacji i prezentacji wyników analiz. Dobranie środowiska i narzędzia informatyczne wspierające proces wdrażania systemu informatycznego.

Efekty uczenia się: Potrafi analizować problem i określić cele projektu. Potrafi analizować i dokonać wyboru metod analizy danych. Potrafi wykorzystać istniejące technologie rozproszonego i masowego przetwarzania danych. Potrafi dokonać właściwej wizualizacji i prezentacji wyników analiz danych. Potrafi współdziałać w zespole realizując w niej różne role i ponosić odpowiedzialność za wspólne przedsięwzięcia. Ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżynierskiej, w tym jej wpływu na środowisko, i związanej z tym odpowiedzialności za podejmowane decyzje.

Przedmiot: C.IV.29. ZARZĄDANIE WIEDZĄ

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	12		8	24		44	58	102	1,7	2,3	4	Zo	O
Ogółem	12		8	24		44	58	102	1,7	2,3	4	Zo-1	

Cele kształcenia: Zapoznać z metodami reprezentacji wiedzy, metodyka modelowania semantyki, językami ontologicznymi i ich właściwościami. Nauczyć konstrukcji modeli ontologicznych dziedzinowych i dedykowanych rozwiązywaniu konkretnych problemów. Nauczyć implementacji narzędzi przetwarzania semantyki i konstrukcji narzędzi baz wiedzy.

Treści kształcenia: Ontologia – definicje i składniki, typy ontologii, problemy wnioskowania w ontologiach. Reprezentacja metadanych: XML, RDF, RDFS, OWL. Języki OWL (OWL Ontology Web Language), OWL2. Podstawy inżynierii ontologii: budowa, łączenie, mapowanie, segmentacja. Analiza i modelowanie pojęć w ontologii. Modelowanie wiedzy za pomocą ontologii. Podstawowe algorytmy wnioskowania w ontologii. Systemy regułowe. Język SPARQL. Silniki programowe wnioskowania. Ontologie a bazy danych. Systemy rekomendacji. Semantyczne wyszukiwanie informacji. Wprowadzenie do analizy źródeł tekstowych. Kontrolowany język naturalny (idea i zastosowania, algorytmy).

Efekty kształcenia: Zna sposoby reprezentacji modeli ontologicznych. Potrafi modelować i budować ontologie dziedzinowe. Stosuje narzędzia budowy ontologii oraz wnioskowania regułowego. Zna podstawowe metody i narzędzia analizy tekstu.

8.3.3. SPECJALNOŚĆ „BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH" C.IV

Ramowy opis przedmiotów

Przedmiot: C.IV.1. ATAKI SIECIOWE I ZŁOŚLIWE OPROGRAMOWANIE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	Wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	10		20	14		44	33	77	1,7	1,3	3	Zo	O
Ogółem	10		20	14		44	33	77	1,7	1,3	3	Zo-1	

Cele kształcenia: Nabycie wiedzy w zakresie podstawowych sposobów ataków informacyjnych, słabości systemów i sposobów ich wykorzystywania, podstawowych technik ataków lokalnych i zdalnych.

Treści kształcenia: Podstawowe ataki teleinformatyczne. Narzędzia ataków i testów penetracyjnych. Wybrane, reprezentatywne techniki ataków. Malware. Klasyfikacja, zasady budowy i działania. Użycie, rozpoznawanie i zasady analizy malware. Narzędzia.

Efekty uczenia się: Znajomość podstawowych sposobów ataków informacyjnych – ich klasyfikacji, celów i metod. Wiedza dotycząca typowych słabości systemów i sposobów ich wykorzystywania. Wiedza o podstawach budowy malware. Znajomość podstawowych technik ataków lokalnych i zdalnych. Znajomość sposobów użycia, rozpoznawania i analizy malware.

Przedmiot: C.IV.2. BEZPIECZEŃSTWO SIECI KOMPUTEROWYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	10		20			30	45	75	1,2	1,8	3	Zo	O
Ogółem	10		20			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nabycie umiejętności: stosowania wybranych technik badania podatności systemów na zagrożenia; doboru składników i zabezpieczeń oraz oceny ich skuteczności; konfigurowania wybranych mechanizmów zabezpieczających.

Treści kształcenia: Eksploracja sieci komputerowych, analiza ruchu, kryptograficzne metody zapewniania bezpieczeństwa, bezpieczne protokoły sieciowe, systemy IDS/IPS i zapory sieciowe.

Efekty uczenia się: Zna podstawowe mechanizmy zabezpieczania informacji w sieciach komputerowych. Potrafi stosować wybrane techniki badania podatności systemów na zagrożenia. Potrafi dobrać składniki zabezpieczeń i ocenić ich skuteczność. Potrafi konfigurować wybrane mechanizmy zabezpieczające.

Przedmiot: C.IV.3. PODSTAWY PROJEKTOWANIA BEZPIECZNEGO OPROGRAMOWANIA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	12		8	24		44	58	102	1,7	2,3	4	Zo	O
Ogółem	12		8	24		44	58	102	1,7	2,3	4	Zo-1	

Cele kształcenia: Nabycie umiejętności: zastosowania zasad i składowych projektowania bezpiecznego oprogramowania; wykorzystania w praktyce metodyki wytwarzania bezpiecznego oprogramowania.

Treści kształcenia: Zasady projektowania bezpiecznego oprogramowania („privacy by design", „privacy by default"). Składowe bezpiecznego oprogramowania. Mechanizmy bezpieczeństwa stosowane w oprogramowaniu. Mechanizmy zabezpieczające wbudowane platformy wytwarzania oprogramowania i infrastruktury uruchomieniowe. Mechanizmy bezpieczeństwa wykorzystywane w procesie wytwarzania oprogramowania, w tym problematyka fizycznego bezpieczeństwa artefaktów procesu wytwórczego. Praktyki biznesowe (procedury) korzystania z oprogramowania. Zapewnianie wymogów wynikających z przepisów o ochronie danych osobowych. Metodyki wytwarzania bezpiecznego oprogramowania.

Efekty uczenia się: Zna zasady i składowe projektowania bezpiecznego oprogramowania. Potrafi zastosować zasady i składowe projektowania bezpiecznego oprogramowania. Potrafi wykorzystać w praktyce metodyki wytwarzania bezpiecznego oprogramowania.

Przedmiot: C.IV.4. AUTOMATY I JĘZYKI FORMALNE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	12		18			30	45	75	1,2	1,8	3	E	O
Ogółem	12		18			30	45	75	1,2	1,8	3	E-1	

Cele kształcenia: Posiada umiejętność definicji języków przy pomocy pojęć niedeterministycznego i deterministycznego automatu skończonego oraz formuły regularnej, minimalizować automat skończony, definiować gramatyki i języki bezkontekstowe.

Treści kształcenia: Wzorce i wyrażenia regularne. Deterministyczne automaty skończone. Niedeterministyczne automaty skończone. Równoważność wzorców, wyrażeń regularnych i automatów skończonych. Lemat o pompowaniu dla języków regularnych. Minimalizacja deterministycznych automatów skończonych. Języki bezkontekstowe. Postać normalna Chomsky'ego, jednoznaczność, problem przynależności, algorytm Cocke-Younger'a-Kasami'ego (CYK). Lemat o pompowaniu dla języków bezkontekstowych. EBNF. Automaty ze stosem. Analiza składniowa. Języki kontekstowe. Hierarchia Chomsky'ego. Maszyny Turinga i obliczalność. Języki obliczalne, częściowo obliczalne i nieobliczalne.

Efekty uczenia się: Zna pojęcia niedeterministycznego i deterministycznego automatu skończonego, formuły regularnej, języka regularnego oraz podstawowe twierdzenia dotyczące tego aparatu pojęciowego. Zna pojęcia gramatyki bezkontekstowej, języka bezkontekstowego, drzewa wyprowadzenia, gramatyki jednoznacznej, postaci normalnej gramatyki bezkontekstowej. Umie zastosować języki regularne i bezkontekstowe. Zna metody pokazywania, że język nie należy do klasy. Zna hierarchię Chomsky’ego. Potrafi definiować języki przy pomocy pojęć niedeterministycznego i deterministycznego automatu skończonego oraz formuły regularnej. Potrafi minimalizować automat skończony. Potrafi definiować gramatyki i języki bezkontekstowe. Potrafi konstruować gramatyki jednoznaczne dla prostych języków. Potrafi stosować lematy o pompowaniu. Potrafi dokonać klasyfikacji języków zgodnie z hierarchią Chomsky’ego.

Przedmiot: C.IV.5. PROGRAMOWANIE W JĘZYKACH FUNKCYJNYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	14		16			30	45	75	1,2	1,8	3	Zo	O
Ogółem	14		16			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nabycie umiejętności posługiwania się językami funkcyjnymi oraz stosowania zasad programowania obiektowego w języku funkcyjnym, posługiwania się wybranym językiem funkcyjnym.

Treści kształcenia: Interpreter w wybranym języku funkcyjnym, Wykonywanie programu. Typy i operacje. Typy liczbowe. Typy dynamiczne. Łańcuchy znaków. Listy i słowniki. Krotki i pliki. Instrukcje wybranego języka funkcyjnego. Przypisania. Reguły instrukcji If, while, for. Przekazywanie argumentów. Funkcje i wyrażenia lambda. Iterowanie i składanie list. Moduły i operowanie modułami. Klasy, operowanie klasami, projektowanie klas. Kompozycje i dziedziczenie, przeciążanie operatorów. Dekoratory i metaklasy. Sloty i przeciążanie nazw. Wyjątki: try/else; try/finally; try/except/finally; raise; assert. Klasy wyjątków. Projektowanie oparte na wyjątkach. Operowanie łańcuchami znaków. Zarzadzanie atrybutami. Dekoratory.

Efekty kształcenia: Rozumie zasady konstrukcji języka funkcyjnego. Potrafi stosować zasady programowania zorientowanego obiektowo w języku funkcyjnym. Rozumie nowoczesne trendy konstrukcji języków programowania i potrafi wykorzystywać biblioteki specjalizowane w wybranym języku funkcyjnym. Potrafi wykorzystywać elementy struktury wybranego języka funkcyjnego. Potrafi zaprojektować obiektowo kod w języku funkcyjnym. Stosuje wzorce programowania funkcyjnego.

Przedmiot: C.IV.6. TECHNIKI ALGORYTMICZNE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	14		4	12		30	45	75	1,2	1,8	3	E	O
Ogółem	14		4	12		30	45	75	1,2	1,8	3	E - 1	

Cele kształcenia: Nabycie umiejętności: stosowania w praktyce różnych technik algorytmicznych; stosowania w praktyce różnych struktur danych. oszacowania złożoności i wrażliwości algorytmów.

Treści kształcenia: Algorytmy i problemy algorytmiczne: pojęcia wstępne. Definicja algorytmu, kryteria jakości algorytmów, złożoność algorytmu i złożoność zadania, stabilność numeryczna algorytmów, zasady projektowania efektywnych algorytmów. Złożoność obliczeniowa algorytmów kombinatorycznych: Rodzaje zadań, sekwencyjne modele obliczeń (DTM i NDTM), transformacje problemów, klasy złożoności obliczeniowej, NP-zupełność, złożoność czasowa i pamięciowa algorytmów (pesymistyczna i oczekiwana), wrażliwość algorytmów (pesymistyczna i oczekiwana), stabilność numeryczna algorytmów, przykłady szacowania złożoności. Algorytmy przybliżone: Metody szacowania dokładności algorytmów. Wielomianowe schematy aproksymacyjne (PTAS), w pełni wielomianowe schematy aproksymacyjne (FPTAS), przykłady algorytmów aproksymacyjnych dla problemów trudnych obliczeniowo. Metody przeszukiwania heurystycznego.

Efekty uczenia się: Zna różne metody określania efektywności algorytmów (dokładności, złożoności). Zna zasady stosowania algorytmów aproksymacyjnych i heurystyk. Zna wpływ stosowania różnych struktur danych oraz technik algorytmicznych na dokładność i złożoność algorytmów. Potrafi stosować w praktyce różne techniki algorytmiczne. Potrafi stosować w praktyce różne struktury danych. Potrafi oszacować złożoność i wrażliwość algorytmów.

Przedmiot: C.IV.7. BUSINESS MODELING IN UML

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	10		20			30	20	50	1,2	0,8	2	Zo	O
Ogółem	10		20			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Umiejętność wypowiadania się, posługując się językiem angielskim, na zagadnienia zawodowe z wykorzystaniem fachowego słownictwa z zakresu informatycznych systemów zarządzania, technik algorytmicznych, niezawodności programowania, architektury korporacyjnej.

Treści kształcenia: Specjalistyczne słownictwo i struktury tekstów mówionych i pisanych, charakterystycznych dla systemów informatycznych. Podstawowa specjalistyczna leksyka i struktury oraz wzorce podstawowych tekstów pisemnych w zakresie: systemów informatycznych, technik algorytmicznych, niezawodności programowania. Specjalistyczne słownictwo i struktury tekstów mówionych i pisanych, charakterystycznych dla informatycznych systemów zarządzania. Podstawowa specjalistyczna leksyka i struktury oraz wzorce podstawowych tekstów pisemnych w zakresie: informatycznych systemów zarządzania, technik algorytmicznych, niezawodności programowania, architektury korporacyjnej.

Efekty uczenia się: Czyta ze zrozumieniem teksty specjalistyczne na poziomie B2+. Rozumie za słuchu teksty specjalistyczne na poziomie B2+. Płynnie wypowiada się na zagadnienia zawodowe z wykorzystaniem fachowego słownictwa z zakresu systemów informatycznych, technik algorytmicznych, niezawodności programowania. Poprawnie i jasno formułuje swoje myśli na piśmie w zakresie systemów informatycznych, technik algorytmicznych, niezawodności programowania. Integruje wszechstronne umiejętności językowe z wiedzą specjalistyczną w sytuacjach zawodowych. Płynnie wypowiada się na zagadnienia zawodowe z wykorzystaniem fachowego słownictwa z zakresu informatycznych systemów zarządzania, technik algorytmicznych, niezawodności programowania, architektury korporacyjnej. Poprawnie i jasno formułuje swoje myśli na piśmie w zakresie informatycznych systemów zarządzania, technik algorytmicznych, niezawodności programowania i architektury korporacyjnej. Integruje wszechstronne umiejętności językowe z wiedzą specjalistyczną w sytuacjach zawodowych.

Przedmiot: C.IV.8. MODELOWANIE I SYMULACJA PROCESÓW BIZNESOWYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						Niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	14		16			30	20	50	1,2	0,8	2	Zo	O
Ogółem	14		16			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie umiejętności zamodelowania i zasymulowania procesów biznesowych w średnio skomplikowanej organizacji.

Treści kształcenia: Notacja BPMN. Modelowanie funkcji i procesów biznesowych. Środowiska informatyczne modelowania, analizy i symulacji procesów biznesowych.

Efekty uczenia się: Zna zasady i cele modelowania procesów biznesowych organizacji. Zna notację BPMN. Potrafi zamodelować i zasymulować procesy biznesowe średnio skomplikowanej organizacji.

Przedmiot: C.IV.9. METODY EKSPLORACJI DANYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	12		18			30	45	75	1,2	1,8	3	E	O
Ogółem	12		18			30	45	75	1,2	1,8	3	E-1	

Cele kształcenia: Poznanie wybranych metod eksploracji danych i wybranych komputerowych narzędzi eksploracji danych; nabycie umiejętności formułowania i rozwiązywania podstawowych problemów eksploracji danych z wykorzystaniem wybranych narzędzi.

Treści kształcenia: Pojęcia podstawowe eksploracji danych. Klasyfikacja problemów eksploracji danych. Problemy predykcji. Klasyfikacja. Grupowanie i odkrywanie asocjacji. Środowisko SAS. SAS Enterprise Miner - charakterystyka narzędzia. Przygotowanie danych do eksploracji. Wstępna obróbka danych. Eksploracyjna analiza danych. Odkrywanie asocjacji i sekwencji. Klasyfikacja z zastosowaniem drzew decyzyjnych, regresji logistycznej. Grupowanie (wyznaczanie skupień - algorytmy hierarchiczne, K- średnich). Prognozowanie z zastosowaniem modułu regresji liniowej. Narzędzia oceny modelu na przykładzie SAS Enterprise Miner. Eksploracja danych tekstowych.

Efekty uczenia się: Znajomość podstawowych pojęć i problemów eksploracji danych. Znajomość wybranych metod eksploracji danych. Znajomość wybranych komputerowych narzędzi eksploracji danych. Znajomość zasad budowy i wdrażania systemów eksploracji danych. Umiejętność formułowania i rozwiązywania podstawowych problemów eksploracji danych z wykorzystaniem wybranych narzędzi.

Przedmiot: C.IV.10. METODY I NARZĘDZIA GENEROWANIA KODU WYKONYWALNEGO

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	12		32			44	58	102	1,7	2,3	4	E	O
Ogółem	12		32			44	58	102	1,7	2,3	4	E-1	

Cele kształcenia: Nabycie umiejętności: klasyfikacji problemu i doboru narzędzi informatycznych w procesie wspomaga decyzji; formułowania i rozwiązywania zadań z wykorzystaniem narzędzi informatycznych.

Treści kształcenia: Obiekty w projektowaniu kodów wykonywalnych. Języki i narzędzia do projektowania i programowania kodów wykonywalnych. Kompilatory i środowiska narzędziowe. Metody generowania kodów wykony-walnych.

Efekty uczenia się: Znajomość metod identyfikacji procesów decyzyjnych. Znajomość zasad budowania modeli decyzyjnych. Znajomość zasad projektowania systemów wspomagania wiedzy. Umiejętność klasyfikacji problemu i doboru narzędzi informatycznych w procesie wspomaga decyzji. Umiejętność formułowania i rozwiązywania zadań z wykorzystaniem narzędzi informatycznych.

Przedmiot: C.IV.11. METODY PROJEKTOWANIA I WDRAŻANIA SYSTEMÓW INFORMATYCZNYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	30		18	12		60	40	100	2,4	1,6	4	E	O
Ogółem	30		18	12		60	40	100	2,4	1,6	4	E-1	

Cele kształcenia: Znajomość metod analizy i modelowania procesów biznesowych w organizacji oraz najlepszych praktyk z zakresu inżynierii systemów informatycznych; umiejętność modelowania i projektowania systemu z wykorzystaniem wybranych narzędzi wspomagających typu CASE i CAStE.

Treści kształcenia: Modele cyklu życia systemu informatycznego. Standardy i normy wytwarzania i wdrażania systemów informatycznych. Strukturalne metodyki projektowania systemów informatycznych. (Fazy projektowania w podejściu strukturalnym. Czynności w ramach faz. Elementy metodyki CDM. Narzędzia CASE. Designer 6i). Obiektowe metodyki projektowania systemów informatycznych. (Etapy projektowania w podejściu obiektowym. Dyscypliny (procesy) w podejściu obiektowym. Czynności w ramach faz i dyscyplin. Elementy metodyki RUP. Narzędzia CASE). Zwinne metodyki projektowania systemów informatycznych. (Manifest zwinności. Przegląd metodyk zwinnych dostępnych na krajowym rynku informatycznym. Rozwój metodyk projektowania systemów informatycznych w kierunku metod „zwinnych”). Zorientowane na jakość metodyki projektowania systemów informatycznych (. Model „V”. Przegląd metodyk zorientowanych na jakość. Wybrane elementy metodyki RTN.).

Efekty uczenia się: Znajomość metodyk, technik i narzędzi wytwarzania i wdrażania systemów informatycznych. Znajomość modeli cyklu życia systemu informatycznego oraz standardów i norm z zakresu wytwarzania i wdrażania systemów informatycznych. Znajomość metod analizy i modelowania procesów biznesowych w organizacji oraz najlepszych praktyk z zakresu inżynierii systemów informatycznych. potrafi wybrać i posłużyć się wybranym standardem projektowania systemu oraz zastosować odpowiednią metodyką budowy sytemu informatycznego. umie modelować i projektować systemy z wykorzystaniem wybranych narzędzi wspomagających typu CASE i CAStE. potrafi dokonać analizy procesu biznesowego oraz zaproponować informatyczne narzędzia pracy wspomagające doskonalenie tego procesu.

Przedmiot: C.IV.12. TECHNOLOGIE USŁUGOWE I MOBILNE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	10		10	10		30	20	50	1,2	0,8	2	Zo	O
Ogółem	10		10	10		30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie umiejętności: budowy oprogramowanie SOA i wdrażania na środowiskach uruchomieniowych; implementacji oprogramowania mobilnego dla platformy Android i Windows Phone.

Treści kształcenia: Podstawy projektowania systemów usługowych. Stosy technologiczne SOA. Praktyczne aspekty implementacji bezpiecznych systemów wykorzystujących podejście SOA. Podstawy projektowania oprogramowania mobilnego. Dobre praktyki konstrukcji aplikacji mobilnych dla platformy Android i Windows Phone. Technologie międzyplatformowe wytwarzania oprogramowania mobilnego. Aspekty bezpieczeństwa platform i oprogramowania mobilnego.

Efekty uczenia się: Potrafi budować oprogramowanie SOA i wdrażać na środowiskach uruchomieniowych. Potrafi implementować systemy usługowe. Zna dobre praktyki implementacji aplikacji mobilnych. Zna wytyczne i zasady konstrukcji bezpiecznego oprogramowania mobilnego. Potrafi implementować oprogramowanie mobilne dla platformy Android i Windows Phone.

Przedmiot: C.IV.13. METODY SZTUCZNEJ INTELIGENCJI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	16		14			30	20	50	1,2	0,8	2	Zo	O
Ogółem	16		14			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Znajomość rachunku predykatów, reguły wnioskowania oraz metody przetwarzania klauzul; potrafi programować w wybranych języku sztucznej inteligencji. modelowania i projektowania systemu z wykorzystaniem wybranych narzędzi wspomagających typu CASE i CAStE;

Treści kształcenia: Reguły wnioskowania, rachunek zdań, rachunek predykatów, przetwarzanie zbioru klauzul, metody przeszukiwania przestrzeni rozwiązań. Systemy formalne. Modele ontologiczne. Wprowadzenie do języków sztucznej inteligencji.

Efekty uczenia się: Zna podstawowe pojęcia sztucznej inteligencji. Zna definicje systemów formalnych. Zna rachunek predykatów, reguły wnioskowania oraz metod przetwarzania klauzul. Potrafi programować w wybranych języku sztucznej inteligencji. Potrafi zbudować prosty model ontologiczny wybranej dziedziny.

Przedmiot: C.IV.14. METODY ILOŚCIOWE ANALIZY RYZYKA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	10	6	14			30	20	50	1,2	0,8	2	Zo	O
Ogółem	10	6	14			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie umiejętności oceny ilościowej ryzyka wystąpienia zagrożeń dla bezpieczeństwa informacji, posługując się wybranymi metodami ilościowymi z zastosowaniem wybranych narzędzi informatycznych.

Treści kształcenia: Metody predykcji zagrożeń, wykorzystanie metod eksperckich, wykorzystanie modeli matematycznych do prognozowania zagrożeń (grafy ataku, modele growe, sieci stochastyczne), modele niezawodności sprzętu i oprogramowania. Identyfikacja podatności: miary powierzchni podatnej na atak; modelowanie procesów biznesowych: podatności danych i funkcji na atak; bezpieczeństwo baz danych. Ocena skutków wystąpienia zagrożeń: dostępność danych i funkcji.

Efekty uczenia się: Zna podstawowe ilościowe metody oceny ryzyka, a w tym metody predykcji zagrożeń, oceny podatności i oceny skutków wystąpienia zagrożeń. Potrafi ocenić ilościowo ryzyko wystąpienia zagrożeń dla bezpieczeństwa informacji, posługując się wybranymi metodami ilościowymi z zastosowaniem wybranych narzędzi informatycznych.

Przedmiot: C.IV.15. SYSTEMY WEBOWE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	14		16			30	20	50	1,2	0,8	2	Zo	O
Ogółem	14		16			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Zpoznać z terminologia budowy i projektowania systemów webowych, nauczyć projektować i implementować rozwiązania w zakresie serwisów webowych i specjalizowanych portalów. Nauczyć konstrukcji poprawnych architektur systemów webowych i doboru technologii, bibliotek z których budowane są portale.

Treści kształcenia: Wprowadzenie do Web (od 2.0 do 4.0). Technologie serwerowe i klienckie w systemach webowych: HTML, JSP, PHP, JavaScript, Ajax. Serwisy www. Systemy CMS. Portale internetowe. Zastosowanie w systemach webowych ontologii i sieci semantycznych. Aspekty bezpieczeństwa w systemach webowych.

Efekty uczenia się: Ma wiedze w zakresie rozwoju technologii WEB od 2.0 do 4.0. Potrafi projektować i implementować rozwiązania w zakresie serwisów www, systemów CMS i portali internetowych z wykorzystaniem HTML, JSP, PHP, JavaScript, Ajax. Ma wiedzę w zakresie bezpieczeństwa systemów webowych.

Przedmiot: C.IV.16. BEZPIECZEŃSTWO SYSTEMÓW INFORMACYJNYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	14		16			30	45	75	1,2	1,8	3	Zo	O
Ogółem	14		16			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nabycie umiejętności: przeprowadzenia jakościowej analizy ryzyka dla typowych systemów informatycznych; zaproponowania strategii postępowania z ryzykiem.

Treści kształcenia: Jakościowa analiza ryzyka: identyfikacja zasobów i ich wartościowanie, klasyfikacja zagrożeń, identyfikacja podatności i metody ich szacowania, identyfikacja skutków zagrożeń, jakościowe podejście do szacowania ryzyka, standardy opisu. Strategie postępowania z ryzykiem. Jakościowa analiza ryzyka w świetle standardów.

Efekty uczenia się: Zna standardy określające zasady przeprowadzania analizy ryzyka. Potrafi przeprowadzić jakościową analizę ryzyka dla typowych systemów informatycznych. Potrafi zaproponować strategię postępowania z ryzykiem.

Przedmiot: C.IV.17. METODY I SYSTEMY WSPOMAGANIA DECYZJI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	14		8	8		30	45	75	1,2	1,8	3	Zo	O
Ogółem	14		8	8		30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nabycie umiejętności: klasyfikacji problemu i doboru narzędzi informatycznych w procesie wspomaga decyzji; formułowania i rozwiązywania zadań z wykorzystaniem narzędzi informatycznych.

Treści kształcenia: Identyfikacja procesów decyzyjnych. Teoretyczne ograniczenia. automatycznego podejmowania decyzji. Modele procesów decyzyjnych w wybranej klasie systemów, formułowanie zadań decyzyjnych w oparciu o przyjęte modele z wykorzystaniem metod optymalizacji. Prognostyczne modele decyzyjne. Wstęp do projektowania systemów wspomagania decyzji. Technologia współpracy decydenta z SWD. Projektowanie systemu SWD dla określonego. systemu zarządzania lub kierowania, (opracowanie systemu. językowego, systemu wiedzy oraz systemu przetwarzania zadań), formułowanie zadań projektowych dla SWD. Konstrukcja algorytmów wspomagania decyzji dla wyspecyfikowanych zadań decyzyjnych. Metody weryfikacji algorytmów wspomagania decyzji. Hurtownie danych, metody eksploracji danych (Data Mining), Web Mining (nurty Web Miningu, prezentacja wybranych metod). Formułowanie i rozwiązywanie zadań decyzyjnych z wykorzystaniem. wybranych informatycznych narzędzi wspomagania decyzji (Solver for Excel, R, GAMS, SAS).

Efekty uczenia się: Znajomość metod identyfikacji procesów decyzyjnych. Znajomość zasad budowania modeli decyzyjnych. Znajomość zasad projektowania systemów wspomagania wiedzy. Umiejętność klasyfikacji problemu i doboru narzędzi informatycznych w procesie wspomaga decyzji. Umiejętność formułowania i rozwiązywania zadań z wykorzystaniem narzędzi informatycznych.

Przedmiot: C.IV.18. OBLICZENIA RÓWNOLEGŁE I ROZPROSZONE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	14		16	14		44	33	77	1,7	1,3	3	Zo	O
Ogółem	14		16	14		44	33	77	1,7	1,3	3	Zo-1	

Cele kształcenia: Znajomość klasyfikowania algorytmów i szacowania ich złożoności obliczeniowej. Znajomość podstawowych zasad funkcjonowania i budowy środowisk równoległych i rozproszonych. Znajomość zasad projektowania algorytmów równoległych.

Treści kształcenia: Systemy obliczeń równoległych i rozproszonych. Architektura, narzędzia, środowiska. Zasady konstruowania systemów obliczeń równoległych i rozproszonych. Modele programowania równoległego (problemy: podziału, komunikacji, synchronizacji, zależności między danymi). Wprowadzenie do prowadzenia obliczeń wielkoskalowych i akcelerowanych. Narzędzia i środowiska programowania równoległego. High Performance Fortran, Parallel C, Parallel C++, Message Passing Interfaces. Algorytmiczne aspekty obliczeń równoległych i rozproszonych Model obliczeń równoległych PRAM. Struktura obliczeń równoległych i jej reprezentacja (AGS), złożoność algorytmów o strukturze AGS, przyspieszenie i efektywność, metody szacowania przyspieszenia i efektywności algorytmów równoległych, zbieżność algorytmów równoległych i jej szybkość. Deterministyczne i niedeterministyczne problemy szeregowania zadań na równoległych procesorach. Obliczenia równoległe w problemach algorytmicznych i zadaniach optymalizacji. Ogólne formuły iteracyjne (Jacobiego, Gaussa-Seidela), graf zależności, metody wyznaczania kolejności aktualizacji zmiennych. Obliczenia równoległe w problemach algorytmicznych: sortowania, wyszukiwania wzorca, operacji na macierzach (dodawanie, mnożenie, macierze odwrotne). Obliczenia równoległe w zadaniach optymalizacji: zadaniach bez ograniczeń, zadaniach z ograniczeniami, zadaniach optymalizacji nie różniczkowej, zadania optymalizacji dyskretnej (ze szczególnym uwzględnieniem zadań optymalizacji grafowo-sieciowej). Architektura systemów rozproszonych. Zasady konstruowania systemów obliczeń rozproszonych. Warstwy oprogramowania systemu rozproszonego. Sieciowe a rozproszone środowiska obliczeniowe. Równoległe a rozproszone środowisko obliczeniowe. Modele obliczeń rozproszonych. Podstawowe modele obliczeniowe: systemy NOW i COW, pula procesorów, klaster, GRID. Systemy rozproszonej pamięci dzielonej. Model obliczeniowy RPC i RMI. Synchronizacja i komunikacja w programowaniu rozproszonym. Kanoniczna postać danych. Standardy kanonicznej postaci danych. Synchronizacja w systemach obliczeń

rozproszonych: stan globalny, algorytmy elekcji, wzajemne wykluczanie. Języki i środowiska programowania rozproszonego. Zasady konstruowania języków programowania rozproszonego. Przegląd wiodących rozwiązań. Środowiska programowania rozproszonego PVM (Parallel Virtual Machine), Globus Toolkit.

Efekty kształcenia: Zna metody klasyfikowania algorytmów i szacowania ich złożoności obliczeniowej. Posida wiedzę na temat podstawowych zasad funkcjonowania i budowy środowisk równoległych i rozproszonych. Znajomość zasad projektowania algorytmów równoległych. Umiejętność projektowania struktury obliczeń równoległych. Umiejętność projektowania rozproszonej realizacji obliczeń równoległych. Umiejętność projektowania algorytmów równoległych.

Przedmiot: C.IV.19. PODSTAWY KRYPTOLOGII WSPÓŁCZESNEJ

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	14		16			30	20	50	1,2	0,8	2	Zo	O
Ogółem	14		16			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie wiedzy na temat metod konstrukcji współczesnych systemów kryptograficznych.

Treści kształcenia: Systemy kryptograficzne. Bezpieczeństwo systemów kryptograficznych. Formalne metody oceny bezpieczeństwa systemów kryptograficznych. Podstawy kryptoanalizy. Kryptosystemy symetryczne: algorytmy blokowe i strumieniowe. Kryptosystemy asymetryczne. Funkcje skrótu. Protokoły kryptograficzne. Współczesne zastosowania kryptografii.

Efekty uczenia się: Ma wiedzę na temat metod konstrukcji współczesnych systemów kryptograficznych. Potrafi ocenić bezpieczeństwa współczesnych systemów kryptograficznych oraz wykorzystać niezbędną wiedzę matematyczną na potrzeby tej oceny; potrafi pozyskiwać informacje z literatury w tym głównie w języku angielskim.

Przedmiot: C.IV.20. MODELOWANIE I ANALIZA SIECI ZŁOŻONYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						Niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	18	10	16			44	33	77	1,7	1,3	3	E	O
Ogółem	18	10	16			44	33	77	1,7	1,3	3	E-1	

Cele kształcenia: Umiejętność zamodelowania wybranych obiektów rzeczywistych z wykorzystaniem sieci złożonych i wyznaczenia wartości wybranych ilościowych charakterystyk tych obiektów z wykorzystaniem procedur numerycznych i symulacyjnych.

Treści kształcenia: Modele sieci złożonych. Dynamika sieci złożonych. Sieci społecznościowe (w tym wirtualne sieci społecznościowe). Charakterystyki sieci teleinformatycznych (w szczególności sieci Internet). Identyfikacja zespołów i ról w sieciach złożonych. Wyznaczanie charakterystyk sieci złożonych. Algorytmy wyszukiwania w sieciach złożonych. Modelowanie i symulacja rozprzestrzeniania się zjawisk (wirusy komputerowe, informacja, plotka) w sieciach złożonych

Efekty uczenia się: Zna podstawowe definicje, typy i własności sieci złożonych. Zna podstawowe charakterystyki ilościowe sieci złożonych i metody wyznaczania ich wartości. Potrafi zamodelować wybrane obiekty rzeczywiste z wykorzystaniem sieci złożonych i wyznaczyć wartości wybranych ilościowych charakterystyk tych obiektów z wykorzystaniem procedur numerycznych i symulacyjnych.

Przedmiot: C.IV.21. ZARZĄDZANIE PROJEKTAMI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	14		16			30	45	75	1,2	1,8	3	Zo	O
Ogółem	14		16			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Zapoznać z zagadnieniami zarządzania projektami, w tym zarządzania jakością, ryzykiem i logistyką projektu informatycznego; Umiejętność stosowania zasady prowadzenia, zarządzania i kierowania projektami informatycznymi w różnej skali - od względnie małych do dużych projektów. Przedstawić standardy i podstawowe metodyki zarządzania projektami; oraz podstawowymi metodami z zakresu zarządzania projektami.

Treści kształcenia: Podstawy zarządzania projektami. Studium wykonalności projektu. Podstawowe procesy zarządzania projektem. Procesy rozpoczęcia. Procesy i planowania projektu. Procesy realizacji i kontroli. Procesy monitorowania i zamykania projektu. Podstawowe elementy metodyki prince2. Analiza jakościowa projektu. Tendencje rozwojowe zarządzania projektami.

Efekty uczenia się: Ma podstawową wiedzę dotyczącą zarządzania projektami, w tym zarządzania jakością, ryzykiem i logistyką projektu informatycznego; Zna i rozumie zasady prowadzenia, zarządzania i kierowania projektami informatycznymi w różnej skali - od względnie małych do dużych projektów. Rozumie standardy i podstawowe metodyki zarządzania projektami; zna i rozumie podstawowe metody z zakresu zarządzania projektami - metody zarządzania zakresem projektu, czasem, kosztami, jakością, zasobami, ryzykiem, komunikacją, integracją i zamówieniami. Zna i rozumie zagadnienia dotyczące: rozpoczynania projektu informatycznego i definiowania jego zakresu; planowania projektu informatycznego; realizacji, kontroli i koordynacji projektu informatycznego oraz zamykania, akceptacji i zapewniania wsparcia dla projektu informatycznego. Potrafi opracować dokumentację projektu; potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować informacje, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i uzasadniać opinie. Potrafi wykonywać funkcję kierownika projektu oraz sformułować i zbudować organizację realizującą projekt informatyczny; Potrafi pracować indywidualnie i w zespole, umie oszacować czas realizacji zadania, potrafi opracować i zrealizować harmonogram prac; Potrafi opracować bazowy plan wykonania projektu oraz zarządzać całym procesem realizacji projektu oraz procesem kontroli zmian i strategią zamknięcia projektu. Potrafi opracować strukturę podziału pracy w

projekcie i na jej podstawie wyznaczyć budżet oraz harmonogram projektu. Potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć w zakresie współczesnych modeli zarządzania projektami.

Przedmiot: C.IV.22. ILOŚCIOWE METODY OCENY BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	14		16			30	20	50	1,2	0,8	2	Zo	O
Ogółem	14		16			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Znajomość zaawansowanych metody monitorowania i wykrywania zagrożeń da bezpieczeństwa informacyjnego; umiejętność zamodelowania i oceny ilościowej skuteczności i wydajności systemów bezpieczeństwa informacyjnego.

Treści kształcenia: Monitorowanie ryzyka. Wykrywanie ataków z wykorzystaniem: analizy szeregów czasowych, rozpoznawanie wzorców, analizy sygnatur, analizy anomalii, sieci stochastycznych, modeli sieci społecznościowych. Monitorowanie otoczenia: sensory, fuzja danych, wykrywanie botnetów Identyfikacja nowych zagrożeń, wykrywanie ataków APT. Struktura systemu bezpieczeństwa. Ocena skuteczności i wydajności pojedynczych zabezpieczeń. Optymalizacja struktury systemu zabezpieczeń. Modelowanie. Ocena skuteczności i wydajności. Metody optymalizacji. Symulacja systemu bezpieczeństwa. Optymalizacja planów zapewnienia informacyjnej ciągłości działania.

Efekty uczenia się: Zna zaawansowane metody monitorowania i wykrywania zagrożeń da bezpieczeństwa informacyjnego. Potrafi wykorzystać wybrane metody monitorowania ryzyka. Potrafi zamodelować i ocenić ilościowo skuteczność i wydajność systemów bezpieczeństwa informacyjnego.

Przedmiot: C.IV.23. ARCHITEKTURA KORPORACYJNA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	14		16			30	45	75	1,2	1,8	3	Zo	O
Ogółem	14		16			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nauczyć podstawowych pojęć oraz koncepcji architektury korporacyjne. Nauczyć wybranych ram architektury korporacyjnej. Zaznajomić z kryteriami wyboru ram adekwatnie do rodzaju organizacji. Nauczyć podstawowych języków (UML I ArchiMate) i metodyk (TOGAF, OBASHI, SQEME) zapewniających framework i narzędzia do rejestrowania, zobrazowania i modelowania relacji, zależności oraz przepływu danych między zasobami biznesu a IT.

Treści kształcenia: Główne koncepcje architektury korporacyjnej. Ramy architektoniczne. Budowa praktyki architektonicznej w organizacji - role, ciała i ich odpowiedzialności w obszarze architektury korporacyjnej, procesy i produkty związane z architekturą korporacyjną. Modelowanie i projektowanie architektury korporacyjnej. Ewaluacja architektury korporacyjnej i architektur rozwiązania. Architektura korporacyjna w transformacji organizacji. Zarządzanie architekturą korporacyjną.

Efekty uczenia się: Znajomość podstawowych pojęć oraz koncepcji architektury korporacyjne. Znajomość wybranych ram architektury korporacyjnej. Umiejętność wyboru ram adekwatnie do rodzaju organizacji. Znajomość podstawowych języków (UML I ArchiMate) i metodyk (TOGAF, OBASHI, SQEME) zapewniających framework i narzędzia do rejestrowania, zobrazowania i modelowania relacji, zależności oraz przepływu danych między zasobami biznesu a IT. Umiejętność modelowania wybranych widoków architektur korporacyjnych z wykorzystaniem podstawowych języków oraz narzędzi. Potrafi zdefiniować założenia projektu transformacji organizacji.

Przedmiot: C.IV.24. TEORIA WOJNY INFORMACYJNEJ

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						Niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	16		14			30	20	50	1,2	0,8	2	Zo	O
Ogółem	16		14			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Znajomość metod modelowania, umiejętność stosowania metod badań operacyjnych, w tym symulacji komputerowej, do oddziaływania i obrony w cyberprzestrzeni.

Treści kształcenia: Formy działań w cyberprzestrzeni: CYBEROPS, INFOOPS, PSYOPS. TTP (ang. Tactics, Techniques and Procedures) stosowane do prowadzenia wojny w cyberprzestrzeni: operacje psychologiczne; strategie prowadzenia działań w cyberprzestrzeni; kierowanie działaniami w cyberprzestrzeni: planowanie działań, monitorowanie, sterowanie działaniami. Modele walki (prowadzenia operacji) w cyberprzestrzeni. Modele, metody i narzędzia identyfikacji, rozpoznania i oceny możliwości oddziaływania informacyjnego. Modele, metody i narzędzia przeciwdziałania oddziaływaniu informacyjnemu. Symulacja procesów walki (prowadzenia operacji) w cyberprzestrzeni. Zdolności do prowadzenia działań w cyberprzestrzeni.

Efekty uczenia się: Zna modele i metody analizy stosowane w wojnie informacyjnej. Stosuje narzędzia identyfikacji, rozpoznania i oceny możliwości oddziaływania informacyjnego. Zna formy i procedury działań w cyberprzestrzeni. Zna metody modelowania i symulacji działań w cyberprzestrzeni. Potrafi stosować metody badań operacyjnych, w tym symulacji komputerowej, do oddziaływania i obrony w cyberprzestrzeni. Potrafi ilościowo ocenić skutki działań w cyberprzestrzeni z wykorzystaniem wybranych narzędzi informatycznych.

Przedmiot: C.IV.25. INŻYNIERIA WSTECZNA SYSTEMÓW INFORMATYCZNYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	20		24			44	58	102	1,7	2,3	4	E	O
Ogółem	20		24			44	58	102	1,7	2,3	4	E-1	

Cele kształcenia: Znajomość pojęć i metod odtwarzania architektury systemu informatycznego na podstawie kodu źródłowego, dokumentacji technicznej oraz logów systemowych, a w szczególności na podstawie wyników testowania systemu.

Treści kształcenia: Architektura systemów informatycznych, ze szczególnym uwzględnieniem struktur i procesów. Modelowanie i analiza procesów. Eksploracja danych a eksploracja procesów. Gromadzenie danych w postaci logów systemowych. Metody odkrywania procesów. Metodyki i narzędzia informatyczne wspomagające eksplorację procesów.

Efekty uczenia się: Zna i rozumie podstawowe pojęcia i metody odkrywania procesów. Posiada podstawowe umiejętności w zakresie odtwarzania architektury systemu informatycznego na podstawie danych zawartych w logach systemowych, danych pochodzących z testowania systemu oraz dostępnej wiedzy i modeli systemów. Zna przykłady wykorzystania narzędzi Open Source Intelligence do odkrywania struktur i zasobów organizacji.

Przedmiot: C.IV.26. NIEZAWODNOŚĆ I WYDAJNOŚĆ SYSTEMÓW INFORMATYCZNYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	18	10	16			44	33	77	1,7	1,3	3	Zo	O
Ogółem	18	10	16			44	33	77	1,7	1,3	3	Zo-1	

Cele kształcenia: Umiejętność wykorzystania modeli niezawodnościowych i kolejkowych do oceny wydajności i dostępności usług systemów informatycznych.

Treści kształcenia: Modele niezawodnościowe systemów komputerowych. Modele niezawodnościowe oprogramowania. Model niezawodnościowe systemów informatycznych. Zastosowanie systemów kolejkowych do oceny wydajności systemów informatycznych.

Efekty uczenia się: Zna modele niezawodnościowe systemów informatycznych. Zna modele kolejkowe systemów pojedynczych i sieciowych. Potrafi wykorzystać modele niezawodnościowe i kolejkowe do oceny wydajności i dostępności usług systemów informatycznych.

Przedmiot: C.IV.27. PROJEKT Z ZAKRESU BEZPIECZEŃSTWA SYSTEMÓW

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX				44		44	58	102	1,7	2,3	4	Zo	O
Ogółem				44		44	58	102	1,7	2,3	4	Zo-1	

Cele kształcenia: Umiejętność projektowania systemów zabezpieczeń a także identyfikacji potrzeb użytkownika, analizy ryzyka lub zagrożeń oraz sformułowania wymagań.

Treści kształcenia: Zagrożenia zasobów informacyjnych. Metody oceny stanu bezpieczeństwa systemu informatycznego. Narzędzia – Katana. Badania techniczne, testy penetracyjne. Mechanizmy ochronne. Filtrowanie ruchu. Cyber Defence. SZBI, konwersatoria. Projektowanie systemu bezpieczeństwa informacji. Modernizacja eksploatowanego systemu bezpieczeństwa.

Efekty uczenia się: Ogólna znajomość zagrożeń i zabezpieczeń zasobów informacyjnych. Znajomość zasad prowadzenia przedsięwzięć budowy lub modernizacji systemu bezpieczeństwa. Znajomość SZBI i wymagań bezpieczeństwa informacji. Systemowe podejście do zabezpieczeń i zarządzania bezpieczeństwem. Umiejętności projektowania systemów zabezpieczeń. Umiejętność identyfikacji potrzeb użytkownika, analizy ryzyka lub zagrożeń oraz sformułowania wymagań. Systemowe podejście do zabezpieczeń i zarządzania bezpieczeństwem. Umiejętności projektowania systemów zabezpieczeń. Umiejętność identyfikacji potrzeb użytkownika, analizy ryzyka lub zagrożeń oraz sformułowania wymagań.

Przedmiot: C.IV.28. INŻYNIERIA WSTECZNA ZŁOŚLIWEGO OPROGRAMOWANIA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	12		8	24		44	58	102	1,7	2,3	4	E	O
Ogółem	12		8	24		44	58	102	1,7	2,3	4	E-1	

Cele kształcenia: Nabycie umiejętności: posługiwania się narzędziami statycznej i dynamicznej inspekcji kodu oraz usług internetowych badania kodu; identyfikacji oprogramowania niepożądanego i jego bezpiecznego badania.

Treści kształcenia: Klasyfikacje i zasady bezpieczeństwa. Architektura IA-32 i x64, komunikacja z SO – wybrane treści (powtórzenie). Budowa malware. Analiza statyczna. Narzędzia inspekcji kodów binarnych, dekompilatory, deobfuskatory. Badanie zachowania się i komunikacji. Analiza dynamiczna. Usługi internetowe badania kodu wykonywalnego.

Efekty uczenia się: Znajomość klasyfikacji niepożądanego oprogramowania i sposobów jego budowy. Umiejętność posługiwania się narzędziami statycznej i dynamicznej inspekcji kodu oraz usług internetowych badania kodu. Umiejętność identyfikacji oprogramowania niepożądanego i jego bezpiecznego badania.

8.3.4. SPECJALNOŚĆ „CYBEROBRONA” C.IV

Ramowy opis przedmiotów

Przedmiot: C.IV.1. SIECI KOMPUTEROWE II

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	10		20			30	20	50	1,2	0,8	2	Zo	O
Ogółem	10		20			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie szczegółowej wiedzy z zakresu projektowania i zarządzania sieciami komputerowymi w tym administrowanie sieciowymi systemami operacyjnymi, umiejętność: konfigurowania urządzeń sieciowych w lokalnych (przewodowych i bezprzewodowych) i rozległych sieciach komputerowych; projektowania i diagnozowania, administrowania sieciowymi systemami operacyjnymi; zarządzania sieciami komputerowymi.

Treści kształcenia: Wprowadzenie do routingu dynamicznego: pojęcie protokołu IGP i EGP protokoły dystans-wektor a protokoły stanu łącza, protokoły routingu dynamicznego klasowe i bezklasowe, obsługa pakietów w trybie klasowym, wyznaczanie metryki trasy w protokołach routingu dynamicznego. Ogólne zasady konfigurowania protokołów routingu dynamicznego: podstawowe zasady i zalecenia konfiguracyjne, rozgłaszanie tras statycznych, ograniczanie źródeł informacji o routowaniu, filtrowanie tras, routowanie dynamiczne z użyciem wielu ścieżek, łączenie domen administracyjnych z różnymi protokołami routingu. Protokół RIP: cechy konstrukcyjne protokołu RIP, RIPv1 a RIPv2• pojęcie pętli routingu i metody przeciwdziałania powstawaniu pętli, aktualizacje wyzwalane a czas osiągania stanu konwergencji sieci, konfigurowanie protokołu RIPv1 i RIPv2. Protokół EIGRP: cechy konstrukcyjne protokołu EIGRP, zarządzanie trasami EIGRP, algorytm DUAL, konfigurowanie protokołu EIGRP, diagnozowanie i rozwiązywanie problemów, wynikających z błędnej konfiguracji protokołu. Protokół OSPF w pojedynczym obszarze i wieloobszarowy OSPF: cechy konstrukcyjne protokołu OSPF, stosowanie protokołu OSPF w pojedynczym obszarze.

Efekty uczenia się: Student ma uporządkowaną, podbudowaną teoretycznie ogólną wiedzę w zakresie zasad funkcjonowania sieci komputerowych i użytkowania podstawowych usług sieciowych oraz szczegółową wiedzę z zakresu projektowania i zarządzania sieciami komputerowymi w tym administrowanie sieciowymi systemami

operacyjnymi. Potrafi konfigurować urządzenia sieciowe w lokalnych (przewodowych i bezprzewodowych) sieciach komputerowych, projektować i diagnozować routing statyczny i dynamiczny, administrować sieciowymi systemami operacyjnymi, zarządzać sieciami komputerowymi. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie. Posiada umiejętność samokształcenia się.

Przedmiot: C.IV.2. JAVAEE TECHNOLOGIES

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	10		20			30	20	50	1,2	0,8	2	Zo	O
Ogółem	10		20			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Przedmiot jest prowadzony w języku angielskim w celu nabycia umiejętności w zakresie projektowania i wytwarzania oprogramowania klasy korporacyjnej; umiejętność zaprojektowania, implementacji i konfiguracji systemu w języku Java i zgodnego ze specyfikacją JakartaEE.

Treść kształcenia: Characteristics of JavaEE/JakartaEE technology; architecture of web application conformant with JakartaEE specification; Jakarta persistence; Jarta MVC; Jakarta faces; Jakarta web sockets; Jakarta RESTful web services; Jakarta Enterprise Beans;

Efekty kształcenia: Znajomość fragmentów specyfikacji JakartaEE oraz umiejętność jej wykorzystania w celu zaprojektowania i zaimplementowania oprogramowania. Umiejętność zintegrowania bazy danych z oprogramowaniem zgodnym ze specyfikacją JakartaEE. Umiejętność przygotowania komponentów frontend-owych zgodnych z JakartaEE. Umiejętność przygotowania usług sieciowych w stylu REST. Ma umiejętności językowe zgodne z wymaganiami określonymi dla poziomu B2+ Europejskiego Systemu Opisu Kształcenia Językowego, w stopniu pozwalającym na porozumiewanie się w mowie i piśmie w zakresie swojej specjalności.

Przedmiot: C.IV.3. HTML I APLIKACJE WEBOWE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	14		16			30	20	50	1,2	0,8	2	Zo	O
Ogółem	14		16			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Umiejętność wykorzystania nowoczesnych narzędzi programowych do zaprojektowania i zbudowania aplikacji internetowej; wykorzystania mechanizmów wspierających pracę aplikacji internetowych dla zwiększenia jej bezpieczeństwa i efektywności działania; wykorzystania mechanizmów komunikacji sieciowej dla integracji aplikacji internetowej z oprogramowaniem sieciowym.

Treści kształcenia: Wiadomości wstępne. Strony statyczne i dynamiczne. Działanie aplikacji webowej. Środowisko ASP.NET. Język HTML, JavaScript. Podstawowe elementy HTML. Tworzenie formularzy. Wbudowywanie skryptów. Definiowanie funkcji. Tworzenie obiektów. Hierarchia obiektów. Dostosowywanie wyglądu witryn i zarządzanie nim. Zastosowanie właściwości formatujących. Użycie CSS dla kontrolek. Użycie tematów i motywów. Strony wzorcowe. Technologia ASP. Model zdarzeń ASP.NET. Kompilacja kodu ASP.NET. Cykl życia aplikacji ASP.NET. Obsługa wyjątków. Wykorzystanie kontrolek serwera WWW. Wprowadzenie do kontrolek serwera. Przegląd kontrolek serwera. Programowe manipulowanie właściwościami. Kontrolki sprawdzania poprawności. Kontrolki użytkownika. Zarządzanie stanem w środowisku ASP.NET. Stan widoku. Stan Kontrolek. Pola ukryte. Cookies. Stan aplikacji. Stan sesji. Pamięć podręczna ASP.NET. Wykorzystanie mechanizmów AJAX. Łączenie i reprezentacja danych. Sposób korzystania z dołączania danych. Źródła danych. Wykorzystanie kolekcji. Wybór kontenera danych. Kontrolki danych. Bezpieczeństwo aplikacji. Bezpieczeństwo serwera WWW. Uwierzytelnianie formularzy. Korzystanie z uwierzytelniania formularzy. Tworzenie formularzy logowania. Kontrolki logowania.

Efekty uczenia się: Znajomość narzędzi programowych wspomagających proces projektowania i uruchamiania aplikacji internetowych. Znajomość mechanizmów wspierających pracę aplikacji internetowych. Znajomość mechanizmów integrujących aplikacje internetowe z innym oprogramowaniem sieciowym. Umiejętność wykorzystania nowoczesnych narzędzi programowych do zaprojektowania i zbudowania aplikacji internetowej. Umiejętność wykorzystania mechanizmów wspierających pracę aplikacji internetowych dla zwiększenia jej bezpieczeństwa i efektywności działania. Umiejętność

wykorzystania mechanizmów komunikacji sieciowej dla integracji aplikacji internetowej z oprogramowaniem sieciowym.

Przedmiot: C.IV.4. SYSTEMY OPERACYJNE UNIX

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	20		40			60	15	75	2,4	0,6	3	E	O
Ogółem	20		40			60	15	75	2,4	0,6	3	E-1	

Cele kształcenia: Umiejętność użytkowania systemu typu UNIX, tworzenia skryptów w języku Shell, administrowania wybranymi usługami dostępnymi w systemie Solaris 10.

Treści kształcenia: rodowisko systemu UNIX: podstawowe cechy systemu, struktura systemu, komunikowanie się z systemem, interpreter poleceń, Charakterystyka systemu plików. Prawa dostępu. Podstawowe polecenia dotyczące katalogów, plików i praw dostepu: mkdir, rmdir, mv, mvdir, copy, touch, rm, mv, cp, ln, cat, chmod, umask, chown, chgrp. Sterowanie strumieniami: rodzaje strumieni, przeadresowanie strumieni, przetwarzanie potokowe, sterowanie procesami, polecenia: ps, kill, sleep. Programy użytkowe: vi, tail, more, pg, wc grep, sort, cut, paste, uniq, tr, dd, mount. Zarządzanie procesami przez shell: powoływanie procesów, budowa skryptów, przekazywanie parametrów, zmienne shella i zmienne własne użytkownika. Operowanie kodem powrotu, polecenia if i case, operowanie parametrami skryptu - shift. Złożone warunki w skryptach powłokowych: polecenie test. Konstruowanie skryptów z wykorzystaniem polecenia test Testowanie parametrów skryptu. Programowanie w języku powłoki: pętle realizowane przy pomocy poleceń while, until i for. Funkcje wewnętrzne powłoki: break, continue, read, return. Definiowanie i wykorzystanie funkcji w skryptach powłokowych. Sprawdzian - pisanie skryptów. Zarządzanie kontami użytkowników: tworzenie i zamykanie kont, nadzorowanie kont. Tworzenie kont użytkowników przy pomocy narzędzi systemowych i przez modyfikację plików systemowych. Włączanie i wyłączanie systemu: Proces uruchamiania systemu. Procedury startowe. Wykonanie przykładowej procedury startowej. udowa systemu plików, tworzenie i montowanie systemu plików. Zarządzanie udziałami na dysku na dysku (quota). Tworzenie nowego systemu plików na dysku, konfigurowanie automatycznego montowania systemu plików; pielęgnacja systemu plików; konfigurowanie udziałów na dysku. Archiwizacja i odtwarzanie systemu plików: cele i strategie archiwizacji; narzędzia do tworzenia kopii zapasowych (tar, ufsdump, Networker). Tworzenie kopii zapasowych systemów plików, odtwarzanie zniszczonych systemów plików. Sieciowy system plików NFS i automonter.

Konfigurowanie serwera i klienta oraz diagnozowanie NFS; konfigurowanie automontera. Usługi nazwowe DNS: konfiguracja klienta i serwera, zarządzanie DNS. Konfigurowanie klienta DNS, głównego serwera domeny i serwerów zapasowych, rejestrowanie poddomen.

Efekty uczenia się: Ma uporządkowaną, podbudowaną teoretycznie, szczegółową wiedzę w zakresie budowy i zasad funkcjonowania współczesnych systemów operacyjnych. Ma uporządkowaną, podbudowaną teoretycznie ogólną wiedzę w zakresie administrowania sieciowymi systemami operacyjnymi. Jest zaznajomiony z wybranymi usługami dostępnymi w systemie Solaris 10. Umiejętność użytkowania systemu typu UNIX. Umiejętność tworzenia skryptów w języku Shell. Umiejętność administrowania wybranymi usługami dostępnymi w systemie Solaris 10.

Przedmiot: C.IV.5. ATAKI SIECIOWE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	16		28			44	33	77	1,7	1,3	3	Zo	O
Ogółem	16		28			44	33	77	1,7	1,3	3	Zo-1	

Cele kształcenia: Znajomość podstawowych rodzajów cyberataków i znajdowania/budowy narzędzi ataku, umiejętność wykrywania i badania oraz przygotowania ataków.

Treści kształcenia: Wprowadzenie. Klasyfikacje. Zasady bezpieczeństwa. Ataki lokalne, informacja o analizie powłamaniowej. Malware. Przepełnienia bufora i sterty, Shellcodes. Znane payloads, ich ukrywanie (obfuscation) i wykorzystanie jako RATs. Ataki w sieciach lokalnych i ataki zdalne. Narzędzia. Ataki złożone.

Efekty uczenia się: Znajomość rodzajów ataków i ich syptomów. Umiejętność wykorzystywania dostępnych narzędzi cyberataków (w tym także social engineering, malware i RATs) i rozpoznawania sposobu ich działania. Umiejętność uzupełniania wiedzy o nowych exploitach, payloads i możliwościach ich wykorzystania.

Przedmiot: C.IV.6. OPROGRAMOWANIE NIEPOŻĄDANE I INSPEKCJA KODU

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	14		14	16		44	33	77	1,7	1,3	3	Zo	O
Ogółem	14		14	16		44	33	77	1,7	1,3	3	Zo-1	

Cele kształcenia: Umiejętność posługiwania się narzędziami statycznej i dynamicznej inspekcji kodu oraz usług internetowych badania kodu, umiejętność identyfikacji oprogramowania niepożądanego i jego bezpiecznego badania.

Treści kształcenia: Klasyfikacje i zasady bezpieczeństwa. Narzędzia budowy i inspekcji kodów binarnych. Architektura IA-32 i x64, komunikacja z SO – wybrane treści (powtórzenie). Budowa malware. Typowe funkcje, tricki, ukrywanie przed AV, polimorfizm. Msfvenom. Sposoby inwazji: social engineering, poczta, exploity. Narzędzia ataków złożonych i kampanii phishingowych. RATs. Meterpreter.

Efekty uczenia się: Znajomość klasyfikacji niepożądanego oprogramowania i sposobów jego budowy. Umiejętność posługiwania się narzędziami statycznej i dynamicznej inspekcji kodu oraz usług internetowych badania kodu. Umiejętność identyfikacji oprogramowania niepożądanego i jego bezpiecznego badania.

Przedmiot: C.IV.7. EKSPLORACJA SIECI TELEINFORMATYCZNYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	14		20	10		44	33	77	1,7	1,3	3	E	O
Ogółem	14		20	10		44	33	77	1,7	1,3	3	E-1	

Cele kształcenia: Nabycie wiedzy w zakresie metodologii badań oraz praktycznych przykładów implementacji metod stosowanych do rozwiązywania typowych problemów w obszarze bezpieczeństwa systemów teleinformatycznych.

Treści kształcenia: Wyszukiwanie, zbieranie i korelacja informacji o systemach teleinformatycznych. Rozpoznawanie, badanie i identyfikacja zasobów sieci teleinformatycznych. Wykrywanie podatności: bugów i miskonfiguracji. Narzędzia eksploracji. Ukrywanie działań rozpoznawczych. Zdobywanie zdalnego dostępu do zasobów informacyjnych. Wydobywanie informacji.

Efekty uczenia się: Ma wiedzę w zakresie wybranych faktów, obiektów i zjawisk oraz dotyczących ich metod i teorii w obszarze bezpieczeństwa systemów teleinformatycznych. Ma wiedzę w zakresie metodologii badań oraz praktycznych przykładów implementacji metod stosowanych do rozwiązywania typowych problemów w obszarze bezpieczeństwa systemów teleinformatycznych. Zna praktyczne przykłady implementacji metod stosowanych do rozwiązywania typowych problemów właściwych dla kierunku „kryptologia i cyberbezpieczeństwo”. potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; Potrafi integrować informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie.

Przedmiot: C.IV.8. SYSTEMY WBUDOWANE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VI	20		24			44	33	77	1,7	1,3	3	Zo	O
Ogółem	20		24			44	33	77	1,7	1,3	3	Zo-1	

Cele kształcenia: Nabycie umiejętności planowania i przeprowadzania eksperymentów związanych z wykonywaniem rozkazów i optymalizacją programów dedykowanych dla procesorów potokowanych, urządzeniami peryferyjnymi i systemami wbudowanymi.

Treści kształcenia: Architektura i organizacja wybranej rodziny mikrokontrolerów. Programy wbudowane - wytwarzanie i testowanie. Systemy operacyjne czasu rzeczywistego. Przetwarzanie danych a zużycie energii - metody oszczędzania energii. Projektowanie systemów niezawodnych. Metodyki projektowania.

Efekty uczenia się: Ma uporządkowaną, podbudowaną teoretycznie szeroką wiedzę z zakresu architektury i organizacji komputerów. Ma uporządkowaną, szczegółową wiedzę w zakresie zasad programowania systemów wbudowanych, systemów zorientowanych na usługi oraz systemów multimedialnych. Potrafi planować i przeprowadzać eksperymenty związane z wykonywaniem rozkazów i optymalizacją programów dedykowanych dla procesorów potokowanych, urządzeniami peryferyjnymi i systemami wbudowanymi oraz interpretować uzyskane wyniki i wyciągać wnioski.

Przedmiot: C.IV.9. BEZPIECZEŃSTWO SIECI BEZPRZEWODOWYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	14		16			30	20	50	1,2	0,8	2	Zo	O
Ogółem	14		16			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Umiejętność: konfigurowania urządzeń sieciowych w lokalnych (przewodowych i bezprzewodowych) i rozległych sieciach komputerowych; projektowania i diagnozowania, administrowania sieciowymi systemami operacyjnymi; zarządzania sieciami komputerowymi.

Treści kształcenia: Technologie sieci bezprzewodowych, ochrona informacji w sieciach bezprzewodowych (stosowane metody szyfrowania i uwierzytelnienia), projektowanie bezpiecznych sieci bezprzewodowych, monitorowanie i zarządzanie sieciami bezprzewodowymi.

Efekty uczenia się: Ma wiedzę w zakresie wybranych faktów, obiektów i zjawisk oraz dotyczących ich metod i teorii w obszarze bezpieczeństwa systemów teleinformatycznych. Ma wiedzę w zakresie metodologii badań oraz praktycznych przykładów implementacji metod stosowanych do rozwiązywania typowych problemów w obszarze bezpieczeństwa systemów teleinformatycznych. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie. Umie samodzielnie planować i realizować własne uczenie się przez całe życie. Potrafi konfigurować urządzenia sieciowe w lokalnych (przewodowych i bezprzewodowych) i rozległych sieciach komputerowych, projektować i diagnozować routing statyczny i dynamiczny, administrować sieciowymi systemami operacyjnymi, zarządzać sieciami komputerowymi. Potrafi planować i przeprowadzać eksperymenty w obszarze bezpieczeństwa systemów teleinformatycznych, interpretować ich wyniki i wyciągać wnioski. Umie dokonać krytycznej analizy sposobu funkcjonowania istniejących rozwiązań technicznych w obszarze bezpieczeństwa systemów teleinformatycznych i ocenić te rozwiązania.

Przedmiot: C.IV.10. MODELOWANIE I ANALIZA SYSTEMÓW TELEINFORMATYCZNYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	14		20	10		44	58	102	1,7	2,3	4	E	O
Ogółem	14		20	10		44	58	102	1,7	2,3	4	E-1	

Cele kształcenia: Zapoznanie z :
- zasadami konstruowania wybranych modeli formalnych i wykorzystywania ich własności do weryfikacji działania systemu teleinformatycznego (ST);
- formalnymi modelami zachowania systemów teleinformatycznych;
- wykorzystaniem w praktyce wybranych modeli formalnych do weryfikacji właściwości systemu teleinformatycznego.

Treść kształcenia: Inżynieria oparta na modelach, formalna weryfikacja. Podstawy modelowania ST w języku UML. Sieci Petriego: definicja, własności modelu, wybrane rodzaje sieci Petriego. Automaty czasowe. Logika temporalna. Dwugrafy. Transformacja modeli.

Efekty uczenia: Znajomość zasad konstruowania wybranych modeli i wykorzystywania ich własności do weryfikacji działania systemu teleinformatycznego. Rozumienie potrzeb budowy modeli systemów teleinformatycznych. Umiejętność konstruowania kilku różnych jednakowo ekspresyjnych modeli formalnych. Umiejętność przekształcania modeli formalnych.

Przedmiot: C.IV.11. SYSTEMY BEZPIECZEŃSTWA SIECIOWEGO

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	10		20			30	20	50	1,2	0,8	2	Zo	O
Ogółem	10		20			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Umiejętność konfigurowania podstawowych mechanizmów zabezpieczeń routerów, przełączników oraz transmisji danych w sieciach teleinformatycznych.

Treści kształcenia: Wprowadzenie do bezpieczeństwa sieci. Podatności, zagrożenia, ataki sieciowe i ryzyka. Narzędzia i produkty do zabezpieczania sieci. Podstawowe mechanizmy zabezpieczania routerów i przełączników. Zarządzanie hasłami dostępu. Konfigurowanie ssh. Blokowanie nieużywanych usług. Listy kontroli dostępu - standardowe, rozszerzone i nazwane. Konfigurowanie list kontroli dostępu. Zaawansowane konstrukcje list dostępu: dynamiczne, obsługujące harmonogramy, zwrotne i oparte na zawartości. Konfigurowanie zaawansowanych list kontroli dostępu. Usługi uwierzytelniania, autoryzacji i monitorowania działań w sieciach komputerowych (TACACS+, RADIUS). Usługa syslog. Konfigurowanie lokalnej usługi AAA. Konfigurowanie usługi syslog. Zabezpieczanie transmisji w warstwie sieciowej. Protokół IPSec. Relacje zabezpieczeń. Tryby pracy IPSec. Bazy danych zabezpieczeń. Konfigurowanie tuneli IPSec z predefiniowanym kluczem w różnych środowiskach i topologiach.

Efekty uczenia się: Zaznajomienie z podatnościami i zagrożeniami sieci teleinformatycznych. Nauczyć konfigurowania podstawowych mechanizmów zabezpieczeń routerów, przełączników oraz transmisji danych w sieciach teleinformatycznych.

Przedmiot: C.IV.12. PODSTAWY PRZETWARZANIA ROZPROSZONEGO

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	10		20			30	20	50	1,2	0,8	2	Zo	O
Ogółem	10		20			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie umiejętności: tworzenia programów wykorzystujących mechanizm wywoływania procedur zdalnych – SunRPC; tworzenia programów wykorzystujących mechanizm XML-RPC. Umiejętność tworzenia programów wykorzystujących protokół SOAP.

Treści kształcenia: Podstawowe pojęcia przetwarzania rozproszonego. Mechanizm gniazd. Mechanizm Sun RPC. Mechanizm XML-RPC. Mechanizm SOAP. Samodzielne zadanie projektowe.

Efekty uczenia się: Umiejętność programowania komunikacji sieciowej na poziomie gniazd w językach C, PHP, Java. Umiejętność tworzenia programów wykorzystujących mechanizm wywoływania procedur zdalnych - SunRPC. Umiejętność tworzenia programów wykorzystujących mechanizm XML-RPC. Umiejętność tworzenia programów wykorzystujących protokół SOAP.

Przedmiot: C.IV.13. ADMINISTROWANIE ŚRODOWISKIEM WINDOWS

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	14		30			44	58	102	1,7	2,3	4	E	O
Ogółem	14		30			44	58	102	1,7	2,3	4	E-1	

Cele kształcenia: Nabycie szczegółowej wiedzy z zakresu projektowania i zarządzania sieciami komputerowymi, w tym administrowania sieciowymi systemami operacyjnymi.

Treści kształcenia: Organizacja domenowego środowiska Windows, zarządzanie kontami użytkowników, sterowanie dostępem do zasobów, implementacja i wykorzystanie mechanizmu zasad grupy, replikacja i pielęgnacja usługi katalogowej, monitorowanie systemu. Charakterystyka i konfigurowanie wybranych usług sieciowych (DHCP, DNS, RDS, inne).

Efekty uczenia się: Zna i rozumie zasady budowy i funkcjonowania współczesnych systemów operacyjnych i programowania współbieżnego. Zna i rozumie pojęcia, zasady i metody z zakresu funkcjonowania sieci komputerowych i użytkowania podstawowych usług sieciowych oraz szczegółową wiedzę z zakresu projektowania i zarządzania sieciami komputerowymi, w tym administrowania sieciowymi systemami operacyjnymi. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie.

Przedmiot: C.IV.14. BEZPIECZEŃSTWO SIECI IPv6

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	10		20			30	45	75	1,2	1,8	3	Zo	O
Ogółem	10		20			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Nabycie wiedzy z zakresu zasad funkcjonowania sieci komputerowych wykorzystujących protokół IPv6 w celu wykorzystania jej do projektowania, konfigurowania i diagnozowania sieci komputerowych.

Treści kształcenia: Charakterystyka protokołu IPv6.Adresacja IPv6 - formaty zapisu, rodzaje i przeznaczenie adresów. Przystosowanie działania stosu TCP/IP do pracy w sieci IPv6.Konfigurowanie interfejsu sieciowego komputera klasy PC do pracy w sieci IPv6.Metody integracji sieci IPv4 i IPv6. Translacja adresów i tunelowanie. Konfigurowanie mechanizmu NAT-PT statycznego i dynamicznego. Konfigurowanie wybranego tunelu IPv6 poprzez IPv4.Routing statyczny i dynamiczny w środowisku IPv6. Konfigurowanie protokołu RIPng i OSPFv3. Projekt integracji dwóch wysp IPv6 poprzez infrastrukturę IPv4 wykorzystujących routing dynamiczny.

Efekty uczenia się: Ma rozszerzoną i pogłębioną wiedzę w zakresie zasad funkcjonowania sieci komputerowych wykorzystujących protokół IPv6. Potrafi pozyskiwać informacje z literatury, baz danych, dokumentacji technicznej i innych źródeł (polskich i obcojęzycznych) oraz dokonywać interpretacji i integracji informacji. Potrafi pracować indywidualnie i w zespole przy konfigurowaniu mechanizmów protokołu IPv6, umie oszacować czas realizacji zadania, potrafi opracować i zrealizować harmonogram prac. Potrafi określić kierunki dalszego uczenia się i zrealizować proces samokształcenia. Potrafi projektować, konfigurować i diagnozować sieci komputerowe wykorzystujące protokół IPv6.

Przedmiot: C.IV.15. PROJEKTOWANIE I WYTWARZANIE SYSTEMÓW TELEINFORMATYCZNYCH

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VII	24		24	12		60	40	100	2,4	1,6	4	E	O
Ogółem	24		24	12		60	40	100	2,4	1,6	4	E-1	

Cele kształcenia: Umiejętność tworzenia specyfikacji z zakresu: analizy, architektury i projektowania systemu teleinformatycznego z wykorzystaniem narzędzi typu RAD, CASE i pracy grupowej.

Treści kształcenia: Paradygmaty modelowania (strukturalny, obiektowy, zorientowany na usługi) i wprowadzenie do modelowania obiektowego. Zasady i mechanizmy modelowania obiektowego. Perspektywy modelowania i proces wytwórczy. RUP czy SCRUM? Modelowanie biznesowe (BPMN). Wprowadzenie do architektury korporacyjnej (Archimate). Definiowanie wymagań na system. Specyfikowanie wymagań na system. Strukturalna analiza i projektowanie oprogramowania. Zaawansowane modelowanie dynamiki systemów w języku UML. Zaawansowane modelowanie statyki systemów w języku UML. Analiza systemów. Modele projektowe. Modele implementacyjne jako wynik inżynierii w przód i wstecz. Wizualne modelowanie aplikacji (webowych i bazodanowych).

Efekty uczenia się: Znajomość zasad konstruowania modeli biznesowych i systemowych w procesach wytwarzania systemów teleinformatycznych. Rozumienie motywacji, celów i potrzeb budowy modeli systemów teleinformatycznych. Podstawowa znajomość języków: modelowania architektury korporacyjnej (archimate) i modelowania biznesowego (BPMN) oraz zaawansowana znajomość języka budowy modeli systemowych (UML) uzupełniona o modelowanie ograniczeń (OCL). Umiejętności tworzenia modeli topologii systemów teleinformatycznych. Umiejętność tworzenia specyfikacji z zakresu: analizy, architektury i projektowania systemu teleinformatycznego. Pogłębiona umiejętność wykorzystania narzędzi typu RAD, CASE i pracy grupowej.

Przedmiot: C.IV.16. ZABEZPIECZENIA TELEINFORMATYCZNE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	10		20			30	20	50	1,2	0,8	2	Zo	O
Ogółem	10		20			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Umiejętność konfigurowania mechanizmów zabezpieczeń urządzeń transmisji danych oraz bezpieczeństwa w sieciach teleinformatycznych.

Treści kształcenia: Systemy IDS/IPS. Zapory sieciowe nowej generacji (ang. Next Generation). Systemy przeciwdziałania naruszeniom w warstwie aplikacji - tzw. filtry aplikacyjne. Systemy scentralizowanego monitorowania i korelacji zdarzeń (SIEM). System zarządzania bezpieczeństwem informacyjnym (SZBI), czyli kompleksowe zabezpieczenie systemów teleinformatycznych uwzględniające: klasyfikację i kategoryzację zasobów informacyjnych, zasadę wiedzy koniecznej użytkowników, projekt systemu zabezpieczeń z podziałem na strefy bezpieczeństwa (podsieci IP, VLAN-y), dokumentację SZBI, kompleksowe zabezpieczenia techniczne i proceduralne.

Efekty uczenia się: Zaznajomienie z podatnościami i zagrożeniami sieci teleinformatycznych. Nauczyć konfigurowania mechanizmów zabezpieczeń urządzeń transmisji danych oraz bezpieczeństwa w sieciach teleinformatycznych.

Przedmiot: C.IV.17. ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	20	10	10			40	35	75	1,6	1,4	3	Zo	O
Ogółem	20	10	10			40	35	75	1,6	1,4	3	Zo-1	

Cele kształcenia: Umiejętność zaprojektowania i wdrożenia systemu zarządzania bezpieczeństwem informacji.

Treści kształcenia: Wprowadzenie do bezpieczeństwa informacyjnego – Podstawowe Twierdzenie Bezpieczeństwa. Modele formalne: Belli-LaPaduli, BibyModele formalne: Brewera-Nasha, Clarka-Wilsona, HRU. Dokumentowanie systemu ochrony informacji: polityka bezpieczeństwa informacyjnego, plan bezpieczeństwa, instrukcje i procedury. Plan zapewniania informacyjnej ciągłości działania. Zarządzanie ryzykiem na potrzeby bezpieczeństwa informacyjnego. Normy i standardy z zakresu bezpieczeństwa informacyjnego: ISO/IEC 270xx, Common Criteria. Ocena stanu ochrony informacji w organizacji.

Efekty uczenia się: Ma rozszerzoną i pogłębioną wiedzę z zakresu ochrony i bezpieczeństwa w systemach informacyjnych oraz szczegółową wiedzę z wybranych zagadnień z zakresu zarządzania bezpieczeństwem informacyjnym, w tym również budowy i wdrażania SZBI. Ma wiedzę niezbędną do rozumienia społecznych, ekonomicznych, prawnych i innych pozatechnicznych uwarunkowań działalności inżynierskiej oraz ich uwzględniania w praktyce inżynierskiej. Ma rozszerzoną i pogłębioną wiedzę dotyczącą metod i technik akredytacji oraz certyfikacji urządzeń i systemów zabezpieczeń. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować informacje, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i uzasadniać opinie. Potrafi pracować indywidualnie i w zespole, umie oszacować czas realizacji zadania, potrafi opracować i zrealizować harmonogram prac, umie uzasadnić trafność stosowanych technik w środowisku zawodowym oraz innych środowiskach (także w języku angielskim lub innym). Posługuje się językiem angielskim w stopniu wystarczającym do porozumiewania się, a także czytania za zrozumieniem dokumentacji i instrukcji związanych ze sprzętem, systemami komputerowymi, oprogramowaniem i zaawansowaną inżynierią oprogramowania. Potrafi określić kierunki dalszego uczenia się i zrealizować proces samokształcenia. Potrafi dokonać krytycznej analizy i oceny ryzyka, interpretować uzyskane wyniki i wyciągać wnioski, potrafi dokonać analizy ekonomicznej,

potrafi ocenić przydatność rutynowych metod i narzędzi zabezpieczania sieci oraz wybrać i zastosować właściwą metodę, potrafi zaprojektować i wdrożyć system zarządzania bezpieczeństwem informacji.

Przedmiot: C.IV.18. TECHNIKI DOCHODZENIOWE I ŚLEDCZE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	10		20			30	20	50	1,2	0,8	2	Zo	O
Ogółem	10		20			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Zapoznanie z podstawowymi zasadami i metodami zabezpieczania śladów elektronicznych, analizą śledczą i kryptoanalizą śladów; nabycie umiejętności podstawowej obsługi incydentów.

Treści kształcenia: Dowody cyfrowe i ich zabezpieczanie. Narzędzia. Odtwarzanie zawartości nośników. Analiza nośników i obrazów. Badanie pracujących systemów. Analiza ruchu sieciowego. Analiza powłamaniowa. Analiza logów. Rozpoznanie modus operandi i scenariusza ataku. Profilowanie. Korelacja informacji.

Efekty uczenia się: Znajomość podstawowych zasad i metod zabezpieczania śladów elektronicznych. Umiejętność zabezpieczania i analizy śladów w początkowej obsłudze incydentów, formułowania i weryfikacji hipotez dotyczących przebiegu incydentu.

Przedmiot: C.IV.19. ZARZĄDZANIE SIECIAMI TELEINFORMATYCZNYMI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	10		20	10		40	35	75	1,6	1,4	3	E	O
Ogółem	10		20	10		40	35	75	1,6	1,4	3	E-1	

Cele kształcenia: Umiejętność projektowania, konfigurowania i diagnozowania zaawansowanymi sieciami komputerowymi, zarządzania nimi, administrowania zaawansowanymi usługami sieciowymi.

Treści kształcenia: Wprowadzenie do administrowania siecią: monitorowanie ruchu sieciowego w sieci przełączników warstwy II, protokół SNMP a monitorowanie urządzeń sieciowych, protokół NetFlow – zasady konfigurowania i wykorzystania. Pojęcia podstawowe związane z systemami QoS: architektura systemów gwarantowania jakości usług, model DiffServ, model IntServ. Klasyfikowanie pakietów: IP Precedence i DSCP – struktura i interpretacja wartości pól nagłówka IP, oznaczanie i klasyfikowanie pakietów przez urządzenia przełączające w warstwie 2 i 3 modelu odniesienia, konfigurowanie klasyfikatora pakietów. Metody zarządzania przepustowością, zatorami i kolejkowaniem pakietów: charakterystyka metod kolejkowania – FIFO, WFQ, PQ, CQ, LLQ, unikanie przeciążenia z wykorzystaniem algorytmu bramki RED i WRED, konfigurowanie kolejkowania i unikania przeciążenia. Badania symulacyjne systemów QoS: przygotowanie eksperymentu symulacyjnego na przykładzie pakietu OPNET, realizacja eksperymentu i interpretacja wyników. Protokół MPLS – integrowanie MPLS z systemem QoS: charakterystyka protokołu MPLS, zasady działania routerów granicznych i wewnętrznych domeny MPLS, zarządzanie ruchem i unikanie przeciążeń w sieciach VPN MPLS, konfigurowanie urządzeń przełączających z wykorzystaniem etykiet. Sieci prywatne VPN: pojęcie sieci VPN, metody i protokoły służące realizacji sieci VPN, przykłady realizacji sieci VPN z wykorzystaniem tunelowania GRE i protokołu IPSec, sieci VPN bazujące na protokole MPLS.

Efekty uczenia się: Student ma rozszerzoną i pogłębioną wiedzę w zakresie zasad funkcjonowania sieci komputerowych, usług sieciowych oraz szczegółową wiedzę z zakresu projektowania i zarządzania sieciami komputerowymi w tym administrowanie sieciowymi systemami operacyjnymi. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować informacje, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i uzasadniać opinie. Posługuje się językiem angielskim

w stopniu wystarczającym do porozumiewania się, a także czytania za zrozumieniem dokumentacji i instrukcji związanych ze sprzętem, systemami komputerowymi, oprogramowaniem i zaawansowaną inżynierią oprogramowania. Potrafi projektować, konfigurować i diagnozować zaawansowane sieci komputerowe, zarządzać sieciami komputerowymi, administrować zaawansowanymi usługami sieciowymi.

Przedmiot: C.IV.20. TECHNOLOGIE INTERNETU RZECZY

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	16			14		30	20	50	1,2	0,8	2	Zo	O
Ogółem	16			14		30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Umiejętność dokonania krytycznej analizy istniejących rozwiązań technicznych w obszarze modelowania i projektowania systemów teleinformatycznych, w tym Internetu Rzeczy.

Treści kształcenia: Wizja Internetu Rzeczy (Internet of Things – IoT), definicje IoT, Network of Things, system systemów. Wybrane zastosowania IoT: opieka medyczna pacjentów, logistyka, inteligentne budynki i miasta, militarne zastosowania IoT. Wybrane przypadki użycia IoT. Architektura systemów i sieci IoT. Technologie warstwy sensorów: RFID, układy IoT do zastosowań wbudowanych, bezprzewodowe sieci sensorów (WSNs). Ograniczenia infrastruktury IoT. Podstawowe technologie warstwy sieciowej: protokoły sieciowe (IPv6 dla IoT, 6LoWPAN). Warstwa usług IoT; odkrywanie, ochrona i orkiestracja usług w Internecie Rzeczy. Projektowanie inteligentnych aplikacji; przetwarzanie w chmurze; problemy agregacji i fuzji danych. Problemy i rozwiązania w zakresie komunikacji (machine to machine) M2M. Bezpieczeństwo, tożsamość i zaufanie w IoT. Wybrane rozwiązania zwiększania bezpieczeństwa i zaufania w IoT; zastosowanie TPM, „lekkie" protokoły kryptograficzne. Problemy standaryzacji sensorów i protokołów IoT. Technologie wytwarzania systemów IoT; środowiska i narzędzia developerskie, systemy operacyjne dla IoT; symulatory sieci IoT.

Efekty uczenia się: Zna i rozumie w pogłębionym zakresie zagadnienia dotyczące sieci komputerowych, w tym usług sieciowych, projektowania i zarządzania sieciami, niezawodności, bezpieczeństwa sieciowego. zna w pogłębionym stopniu wybrane fakty, obiekty i zjawiska oraz dotyczące ich metody i teorie w obszarze modelowania i projektowania systemów teleinformatycznych, w tym Internetu Rzeczy. potrafi dokonać

krytycznej analizy istniejących rozwiązań technicznych w obszarze modelowania i projektowania systemów teleinformatycznych, w tym Internetu Rzeczy oraz planować i przeprowadzać eksperymenty w tym obszarze, interpretować i oceniać uzyskane wyniki i wyciągać wnioski.

Przedmiot: C.IV.21. STUDIUM ATAKÓW I INCYDENTÓW

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	14		16			30	20	50	1,2	0,8	2	Zo	O
Ogółem	14		16			30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Nabycie umiejętności nadążania za aktualnym stanem wiedzy w dziedzinie cyberataków, znajomość metod ataków złożonych.

Treści kształcenia: Przegląd: słabości zasobów teleinformatycznych i sposoby ich wykorzystywania; typowe techniki ataków; metodyki i narzędzia badań technicznych bezpieczeństwa – testy penetracyjne. Wybrane narzędzia ataków teleinformatycznych. Złożone metody atakowania systemów teleinformatycznych. Warunki powodzenia. Rozpoznawanie symptomów działań nieuprawnionych. Włamanie, studium przypadku. Aktualne trendy.

Efekty uczenia się: Znajomość tradycyjnych i aktualnych technik ataków teleinformatycznych i narzędzi ataków. Znajomość narzędzi testów penetracyjnych. Znajomość metod ataków kombinowanych. Rozpoznawanie symptomów działań nieuprawnionych. Śledzenie stanu sztuki w dziedzinie ataków komputerowych oraz rozwoju narzędzi ataku i testów penetracyjnych.

Przedmiot: C.IV.22. WIRTUALIZACJA SYSTEMÓW IT

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
VIII	10		12	8		30	20	50	1,2	0,8	2	Zo	O
Ogółem	10		12	8		30	20	50	1,2	0,8	2	Zo-1	

Cele kształcenia: Umiejętność zrealizowania mechanizmów komunikacyjnych dla systemów operacyjnych, używając właściwych metod, technik i narzędzi.

Treści kształcenia: Tendencje rozwoju technologii komputerowych i systemów operacyjnych. Emulacja, parawirtualizacja, wirtualizacja, izolowanie zasobów, abstrakcja zasobów. Wirtualizacja komputerów osobistych i serwerów, konsolidacja serwerów, chmura obliczeniowa. Przegląd oprogramowania do wirtualizacji. Kierunki rozwoju wirtualizacji i rynku IT.

Efekty uczenia się: Ma rozszerzoną i pogłębioną wiedzę w zakresie wirtualizacji systemów IT i zarządzania systemami zwirtualizowanymi. Ma rozszerzoną i pogłębioną wiedzę w zakresie metodyk, technik i narzędzi wytwarzania i wdrażania systemów informatycznych. Potrafi pozyskiwać informacje z literatury i innych źródeł; potrafi integrować informacje. Posługuje się językiem angielskim w stopniu wystarczającym do czytania za zrozumieniem dokumentacji instrukcji związanych ze sprzętem, systemami komputerowymi i oprogramowaniem. Potrafi określić kierunki dalszego uczenia się. Potrafi zrealizować mechanizmy komunikacyjne dla systemów operacyjnych, używając właściwych metod, technik i narzędzi. Rozumie potrzebę i zna możliwości ciągłego dokształcania się.

Przedmiot: C.IV.23. WALKA W CYBERPRZESTRZENI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	Projekt	seminarium	łącznie							
VIII	10		20			30	45	75	1,2	1,8	3	E	O
Ogółem	10		20			30	45	75	1,2	1,8	3	E-1	

Cele kształcenia: Umiejętności: rozpoznawania symptomów i identyfikacji wrogich działań; obrony osobistej stacji roboczej przed cyberatakami zapewnienia prywatności i poufności własnych zasobów informacyjnych oraz komunikacji; wskazania możliwości ataku lub oddziaływania w cyberprzestrzeni dla osiągnięcia wybranych celów.

Treści kształcenia: Podstawowe pojęcia cyberbezpieczeństwa. Sieć rozległa i organizacja Internetu. Cele w cyberprzestrzeni (infrastruktura krytyczna, zasoby korporacyjne, media społecznościowe, osoby/urządzenia prywatne). Rodzaje ataków i metody obrony. Cyberoddziaływania skombinowane w działaniami w innych domenach. Zapewnianie cyberbezpieczeństwa: rozpoznawanie oszustw, ochrona zasobów informacyjnych, zapewnianie poufności i prywatności zasobów informacyjnych i komunikacji.

Efekty uczenia się: Znajomość: organizacji Internetu, celów wrogich oddziaływań w cyberprzestrzeni, ogólnych sposobów prowadzenia cyberataków i metod obrony przed nimi. Umiejętności: rozpoznawania symptomów i identyfikacji wrogich działań; obrony; zapewnienia prywatności i poufności własnych zasobów informacyjnych oraz komunikacji; wskazania możliwości ataku lub oddziaływania w cyberprzestrzeni dla osiągnięcia wybranych celów.

Przedmiot: C.IV.24. PROJEKT Z ZAKRESU CYBEROBRONY

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX				30		30	70	100	1,2	2,8	4	Zo	O
Ogółem				30		30	70	100	1,2	2,8	4	Zo-1	

Cele kształcenia: Nabycie umiejętności zarządzanie zakresem projektu informatycznego w cyklu jego życia.

Treści kształcenia: Omówienie i wydanie zadań projektowych. Zdefiniowanie środowiska wytwarzania projektów. Administrowanie środowiskiem projektu dla pracy grupowej. Instalacja środowisk serwerowych. Metodyka zarządzania projektem. Platforma jazz. Obszar projektu. Obszary zespołu. Środowisko projektu. Etapy i zadania. Planowanie. Zarządzanie zakresem projektu. Definiowanie i modelowanie wymagań. Zwinne modelowanie wymagań. Lokalna i hostowana instalacja szkieletu rozwiązania. Zarządzanie zmianą i kodem w projekcie. Analiza systemu. Przeglądy kodu i projektu. Model architektoniczny. Model projektowy. Implementacja i testowanie systemu. RTC - metryki projektu, zapewnianie jakości i zarządzanie ryzykiem. Końcowy przegląd projektu.

Efekty uczenia się: Zarządzanie zmianą i kodem w projekcie. Analiza systemu. Przeglądy kodu i projektu. Model architektoniczny. Model projektowy. Implementacja i testowanie systemu. RTC - metryki projektu, zapewnianie jakości i zarządzanie ryzykiem. Końcowy przegląd projektu.

Przedmiot: C.IV.25. SYSTEMY ROZPROSZONE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	16			14		30	70	100	1,2	2,8	4	E	O
Ogółem	16			14		30	70	100	1,2	2,8	4	E-1	

Cele kształcenia: umiejętność wykorzystania wiedzy z zakresu języków programowania do projektowania systemów informatycznych zgodnie z zadaną specyfikacją wymagań z wykorzystaniem zaawansowanych technik algorytmicznych.

Treści kształcenia: Podstawowe pojęcia przetwarzania rozproszonego. Synchronizacja w środowisku rozproszonym. Rozproszone szeregowanie procesów. Przetwarzanie transakcyjne w systemach rozproszonych. Zwielokrotnienie, modele i protokoły spójności, replikacja. Rozproszone systemy plików. Tolerowanie awarii, algorytmy elekcji. Rozproszona pamięć dzielona. Projektowanie systemów z wykorzystaniem rozproszonych komponentów - wybrane elementy technologii JEE. Projektowanie systemów z wykorzystaniem rozproszonych komponentów - wybrane elementy technologii .NET. Realizacja projektu aplikacji rozproszonej.

Efekty uczenia się: Ma rozszerzoną i pogłębioną wiedzę w zakresie programowania wysokopoziomowego i niskopoziomowego, algorytmów i struktur danych, programowania strukturalnego i obiektowego. Ma rozszerzoną i pogłębioną wiedzę w zakresie projektowania i wytwarzania oprogramowania dla zastosowań sieciowych. Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować informacje, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i uzasadniać opinie. Posługuje się językiem angielskim w stopniu wystarczającym do czytania za zrozumieniem dokumentacji i instrukcji związanych ze sprzętem, systemami komputerowymi i oprogramowaniem. Potrafi określić kierunki dalszego uczenia się i zrealizować proces samokształcenia. Potrafi wykorzystać wiedzę z zakresu języków programowania do projektowania systemów informatycznych zgodnie z zadaną specyfikacją wymagań; posiada umiejętność stosowania zaawansowanych technik algorytmicznych. Potrafi – zgodnie z zadaną specyfikacją– zaprojektować i zrealizować zaawansowany proces wykorzystujący niskopoziomowe mechanizmy synchronizacyjne i komunikacyjne systemu operacyjnego, używając właściwych metod, technik i narzędzi.

Przedmiot: C.IV.26. TRENDS IN COMPUTER TECHNOLOGY

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	20		10			30	70	100	1,2	2,8	4	Zo	O
Ogółem	20		10			30	70	100	1,2	2,8	4	Zo-1	

Cele kształcenia: Umiejętność: wypowiadania się, posługując się językiem angielskim, na zagadnienia zawodowe z wykorzystaniem fachowego słownictwa; projektowania i eksploatacji systemów komputerowych (np.: konfigurowanie, diagnozowanie, zarządzanie).

Treści kształcenia: A brief history of computer engineering. Personal computer and server architectures. Evolution trends of basic computer components: motherboards, CPU, GPU, RAM, SSD, HDD and optical memories. The main bus standards: PCI-E, QPI/UPI. I/O devices and interfaces. The market of personal computers and servers analysis. New trends in computer technology and on the IT market.

Efekty uczenia się: Ma rozszerzoną i pogłębioną wiedzę w zakresie wybranych zagadnień dotyczących technologii komputerowych. Ma umiejętności językowe, zgodne z wymaganiami określonymi dla poziomu B2+ Europejskiego Systemu Opisu Kształcenia Językowego, w stopniu pozwalającym na porozumiewanie się w mowie i piśmie w zakresie swojej specjalności. Posiada umiejętności w zakresie projektowania i eksploatacji systemów komputerowych (np.: konfigurowanie, diagnozowanie, zarządzanie).

Przedmiot: C.IV.27. TECHNOLOGIE MOBILNE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	14		16			30	45	75	1,2	1,8	3	Zo	O
Ogółem	14		16			30	45	75	1,2	1,8	3	Zo-1	

Cele kształcenia: Umiejętność zaprojektowania - zgodnie z zadaną specyfikacją uwzględniającą aspekty pozatechniczne złożony obiekt lub system oraz zrealizować ten projekt, co najmniej w części, używając odpowiednio dobranych metod, technik i narzędzi.

Treści kształcenia: Wprowadzenie do technologii mobilnych - pojęcia dziedzinowe; rozwiązania sprzętowe, aplikacje i obszary zastosowań. Standardy łączności bezprzewodowej wykorzystywane w rozwiązaniach mobilnych. Technologie mobilne a sieci komputerowe. Zastosowanie sieci komórkowych. Współdziałanie z chmurą obliczeniową.

Efekty uczenia się: Zna w pogłębionym zakresie główne trendy rozwojowe w informatyce oraz kryptologii. Zna i rozumie w pogłębionym zakresie zasady i metody modelowania stochastycznego. Potrafi zaprojektować - zgodnie z zadaną specyfikacją uwzględniającą aspekty pozatechniczne – związany z kierunkiem studiów złożony obiekt lub system oraz zrealizować ten projekt, co najmniej w części, używając odpowiednio dobranych metod, technik i narzędzi, przystosowując do tego celu istniejące lub opracowując nowe metody, techniki i narzędzia.

Przedmiot: C.IV.28. PROJEKTOWANIE SYSTEMÓW BEZPIECZEŃSTWA INFORMACJI

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX	14		16	14		44	83	127	1,7	3,3	5	E	O
Ogółem	14		16	14		44	83	127	1,7	3,3	5	E-1	

Cele kształcenia: Zapoznanie z procesem projektowania systemów zabezpieczeń; nauczenie identyfikacji potrzeb użytkownika; badań/oceny bezpieczeństwa; analizy ryzyka lub zagrożeń oraz formułowania wymagań.

Treści kształcenia: Zagrożenia zasobów informacyjnych. Metody oceny stanu bezpieczeństwa systemu informatycznego. Badania techniczne, testy penetracyjne. Mechanizmy ochronne. Filtrowanie ruchu. SZBI. Proces zespołowego projektowania systemu bezpieczeństwa informacji. Modernizacja eksploatowanego systemu bezpieczeństwa.

Efekty uczenia się: Ogólna znajomość zagrożeń i zabezpieczeń zasobów informacyjnych. Znajomość zasad prowadzenia przedsięwzięć budowy lub modernizacji systemu bezpieczeństwa. Znajomość SZBI i wymagań bezpieczeństwa informacji. Systemowe podejście do zabezpieczeń i zarządzania bezpieczeństwem. Umiejętności projektowania systemów zabezpieczeń. Umiejętność identyfikacji potrzeb użytkownika, analizy ryzyka lub zagrożeń oraz sformułowania wymagań.

9. PRACA DYPLOMOWA, PRAKTYKI I SZKOLENIA SPECJALISTYCZNE W CENTRACH SZKOLENIA I JW.

9.1. Praktyki zawodowe E.I

Ramowy opis przedmiotów

Przedmiot: E.I.3. Praktyka zawodowa , E.I.4. Szkolenie specjalistyczne

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
po VI		100				100		100	4		4	Zo	O
po VIII		100				100		100	4		4	Zo	O
Ogółem		200				200		200	8		8	Zo-2	

Studenci wszystkich specjalności kierunku „kryptologia i cyberbezpieczeństwo” odbywają dwie formy praktyk specjalistycznych: Praktyka zawodowa specjalistyczna, Szkolenie specjalistyczne.

Cele kształcenia: Nabycie wiedzy w zakresie: systemów informatycznych, kryptograficznych i sieciowych, aktualnie wykonywanych i/lub eksploatowanych w instytucji; procesów analizy, projektowania, wdrażania i/lub eksploatacji systemów informatycznych, kryptograficznych w instytucji; technologiami i narzędziami stosowanymi w realizacji prac programowo-implementacyjnych w instytucji.

Treści kształcenia: Szkolenie specjalistyczne obejmuje 4 tygodnie (100 godzin lekcyjnych) w JW lub instytucjach podległych MON (MSWiA). Z uwagi na to, że odbywa się bez bezpośrednich kontaktów z prowadzącym (wykładowcą), nie wlicza się tych godzin do ogólnej liczby godzin studiów. Przydziela się natomiast 8 punktów ECTS (po 4 za każdą z praktyk) za wysiłek poświęcony przez studenta w ramach aktywności studenta poza uczelnią, ukierunkowanej i zgodnej z planem praktyki. Szkolenie realizowane jest po VI i po VIII semestrze studiów. Podstawowym celem praktyki jest wykształcenie umiejętności zastosowania w praktyce wiedzy teoretycznej uzyskanej w toku studiów. Na kierunku Kryptologia i cyberbezpieczeństwo istotą praktyki jest zapoznanie z projektowaniem, programowaniem i eksploatacją systemów informatycznych, kryptograficznych i sieciowych.

Efekty uczenia się: Ma wiedzę dotyczącą instytucji, w której odbywa szkolenie. Ma wiedzę na temat systemów informatycznych, kryptograficznych i sieciowych, aktualnie wykonywanych i/lub eksploatowanych w instytucji. Ma wiedzę na temat procesów analizy,

projektowania, wdrażania i/lub eksploatacji systemów informatycznych, kryptograficznych w instytucji. Ma wiedzę na temat technologiami i narzędziami stosowanymi w realizacji prac programowo-implementacyjnych w instytucji;

Praktykę specjalistyczną zawodową studenci odbywają zawsze pod nadzorem przydzielonego opiekuna oraz w zakresie ustalonym w porozumieniu Instytucji oraz Wydziału. Zakres prowadzonych praktyk zależy od kierunku i specjalności oraz aktualnie realizowanych zadań przez Instytucję. Praktyki będą nastawione na weryfikacje praktycznej i teoretycznej wiedzy przekazywanej na studiach i aplikowane będą w zespołach projektowych, tak aby weryfikować umiejętności kooperacji i realizacji większych zadań.
W czasie praktyki podchorąży powinien:

- zapoznać się z organizacją i zadaniami instytucji;
- zapoznać się z systemami informatycznymi/sieciowymi aktualnie wykonywanymi i/lub eksploatowanymi w instytucji;
- zapoznać się z procesami analizy, projektowania, wdrażania i/lub eksploatacji systemów informatycznych/sieciowych w instytucji;
- zapoznać się z technologiami i narzędziami stosowanymi w realizacji prac programowo implementacyjnych w instytucji;

Proponowany jest czynny udział praktykanta w pracach programowo-implementacyjnych realizowanych w instytucji.
Praktyki specjalistyczne zalicza kierownik praktyk z Wydziału Cybernetyki WAT na podstawie opinii /oceny/ opiekuna praktyki z ramienia instytucji.

9.2. Praktyki dowódcze E.I

Ramowy opis przedmiotów

Przedmiot: E.1.1. Praktyka dowódcy drużyny, E.1.2. Praktyka dowódcy plutonu

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	Kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
po IV		100				100		100	4		4	Zo	O
w X		100				100		100	4		4	Zo	O
Ogółem		200				200		200	8		8	Zo-2	

W module kształcenia wojskowego realizowane jest wspólne kształcenie podchorążych (niezależnie od specjalności i kierunku studiów) w zakresie szkolenia ogólnowojskowego, kształcenia humanistyczno-przywódczego oraz szkolenia z wychowania fizycznego i językowego. Przewidziany jest obóz językowy po IV semestrze, praktyka dowódcy drużyny po IV semestrze oraz praktyka dowódcy plutonu w trakcie X semestru studiów. Praktykę dowódczą studenci odbywają w wytypowanych jednostkach wojskowych w zakresie zadań dowódczych. Przydziela się po 4 punkty ECTS za wysiłek poświęcony przez studenta w ramach odbycia każdej z praktyk.

9.3. Praca dyplomowa D.I

Ramowy opis przedmiotów

Przedmiot: D.I.1. SEMINARIUM PRZEDDYPLOMOWE
Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
IX					20	20	5	25	0,8	0,2	1	Zo	O
Ogółem					20	20	5	25	0,8	0,2	1	Zo-1	

Cele kształcenia: Nabycie umiejętności w zakresie przygotowania pod względem edycyjnym i merytorycznym pracy dyplomowej oraz przygotowania jej prezentacji**.**

Treści kształcenia: Realizacja pracy dyplomowej – etap II (główny) - wykonanie głównych elementów pracy (zakres - w zależności od tematyki i charakteru pracy dyplomowej). Prezentacja sprawozdawcza. Realizacja pracy dyplomowej – etap III (końcowy) - wykonanie końcowych elementów pracy (zakres- w zależności od tematyki i charakteru pracy dyplomowej). Prezentacja sprawozdawcza. Przygotowanie do egzaminu dyplomowego. Opracowanie dokumentacji końcowej.

Efekty uczenia się: Umiejętność przygotowania pracy dyplomowej, umiejętność przygotowania multimedialnej prezentacji pracy dyplomowej oraz jej przedstawienia.

Przedmiot: D.I.2. SEMINARIUM DYPLOMOWE

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
X					44	44	58	102	1,7	2,3	4	Zo	O
Ogółem					44	44	58	102	1,7	2,3	4	Zo-1	

Cele kształcenia: Nabycie umiejętności w zakresie przygotowania pod względem edycyjnym i merytorycznym pracy dyplomowej oraz przygotowania jej prezentacji**.**

Treści kształcenia: Realizacja pracy dyplomowej – etap II (główny) - wykonanie głównych elementów pracy (zakres - w zależności od tematyki i charakteru pracy dyplomowej). Prezentacja sprawozdawcza. Realizacja pracy dyplomowej – etap III (końcowy) - wykonanie końcowych elementów pracy (zakres- w zależności od tematyki i charakteru pracy dyplomowej). Prezentacja sprawozdawcza. Przygotowanie do egzaminu dyplomowego. Opracowanie dokumentacji końcowej.

Efekty uczenia się: Umiejętność przygotowania pracy dyplomowej, umiejętność przygotowania multimedialnej prezentacji pracy dyplomowej oraz jej przedstawienia.

Przedmiot: D.I.3. PRACA DYPLOMOWA

Rozliczenie godzinowe:

Semestr	Liczba godzin								Liczba pkt ECTS			Rygor dydaktyczny	Przedmiot O/W
	kontaktowych						niekontaktowych	Razem	kontaktowe	niekontaktowe	Razem		
	wykłady	ćwiczenia	laboratoria	projekt	seminarium	łącznie							
X				100		100	450	550	4	18	22	E	O
Ogółem				100		100	450	550	4	18	22	E-1	

Elementem programu studiów jest przedsięwzięcie rozumiane jako zaawansowane zadanie informatyczne. Opracowane w ramach przedsięwzięcia rozwiązanie wraz z odpowiednią dokumentacją stanowi pracę dyplomową. Obejmuje to około 450 godzin pracy własnej studenta. Z uwagi na fakt, że moduł ten realizowany jest bez bezpośrednich kontaktów z prowadzącym (wykładowcą), nie wlicza się tych godzin do ogólnej liczby godzin studiów. Za wkład do przedsięwzięcia oraz wysiłek włożony w redakcję prac dyplomowych oraz przygotowanie do egzaminów dyplomowych student otrzymuje 22 punktów ECTS.

Przedmiot: D.I.4. EGZAMIN NA OFICERA

Egzamin na oficera jest ostateczną formą weryfikacji nabytej wiedzy i umiejętności. W jego trakcie sprawdzeniu podlega: wyszkolenie i umiejętności strzeleckie, teoretyczna i praktyczna znajomość regulaminów i przepisów wojskowych, wyszkolenie z musztry, umiejętność dowodzenia pododdziałem oraz prowadzenia nauczania w roli instruktora i kierownika zajęć. Weryfikowana jest także wiedza z zakresu prowadzenia działań taktycznych przez pododdział, zagadnień zabezpieczenia bojowego i zabezpieczenia logistycznego. Warunkiem dopuszczającym do egzaminu jest zaliczenie wszystkich przedmiotów kształcenia wojskowego oraz uzyskanie odpowiednich kwalifikacji językowych zgodnych ze STANAG 6001. Po zdaniu egzaminu na oficera odbywa się promocja na pierwszy stopień oficerski.

10. DODATKOWE INFORMACJE O PROGRAMIE STUDIÓW

Programy jednolitych studiów magisterskich dla kandydatów na oficerów opracowywane są dla kierunków określonych w decyzji MON w sprawie rekrutacji kandydatów do uczelni wojskowych na dany rok akademicki. Studia są prowadzone na określonym kierunku w formie studiów stacjonarnych na podstawie programu studiów ustalonego przez Senat WAT, po zasięgnięciu opinii Wydziałowej rady ds. kształcenia oraz Samorządu studenckiego. Opinie Wydziałowej rady samorządu studenckiego oraz Wydziałowej rady ds. kształcenia stanowią załączniki do programu studiów.

Kierunki studiów prowadzone przez Wydział Cybernetyki uzyskały certyfikaty przyznane przez Prezydium Polskiej Komisji Akredytacyjnej.

1. Certyfikat Doskonałości Kształcenia w kategorii „Doskonały kierunek – doskonałość w kształceniu” dla kierunku „kryptologia i cyberbezpieczeństwo”
2. Certyfikat Doskonałości Kształcenia w kategorii „Zawsze dla studenta – doskonałość we wsparciu rozwoju studentów” dla kierunku „informatyka”

Certyfikaty zostały przyznane na podstawie pozytywnej oceny programowej ważnej przez sześć lat. Decyzja Prezydium PKA została poparta analizą dobrych praktyk w zakresie jakości kształcenia oraz udokumentowanymi i regularnymi osiągnięciami studentów i absolwentów wyróżnionych kierunków.

CERTYFIKAT

DOSKONAŁOŚCI KSZTAŁCENIA

w kategorii

Doskonały kierunek -
doskonałość w kształceniu

przyznany przez
Prezydium Polskiej Komisji Akredytacyjnej

kierunkowi

kryptologia i cyberbezpieczeństwo

prowadzonemu na **Wojskowej Akademii Technicznej**
im. Jarosława Dąbrowskiego w Warszawie
na poziomie studiów pierwszego i drugiego stopnia
oraz jednolitych studiów magisterskich
o profilu ogólnoakademickim

Warszawa, 23 lutego 2023 r.

Przewodniczący
Polskiej Komisji Akredytacyjnej
Stanisław Wrzosek

Certyfikat przyznany uchwałą nr 118/2023 Prezydium Polskiej Komisji Akredytacyjnej z dnia 23 lutego 2023 r. w związku z oceną programową zakończoną uchwałą nr 143/2022 Prezydium Polskiej Komisji Akredytacyjnej z dnia 10 marca 2022 r.

CERTYFIKAT

DOSKONAŁOŚCI KSZTAŁCENIA

w kategorii

Zawsze dla studenta -
doskonałość we wsparciu rozwoju studentów

przyznany przez
Prezydium Polskiej Komisji Akredytacyjnej

kierunkowi

informatyka

prowadzonemu na **Wojskowej Akademii Technicznej**
im. Jarosława Dąbrowskiego w Warszawie
na poziomie studiów pierwszego i drugiego stopnia
oraz jednolitych studiów magisterskich
o profilu ogólnoakademickim

Warszawa, 23 lutego 2023 r.

Przewodniczący
Polskiej Komisji Akredytacyjnej
Stanisław Wrzosek

Certyfikat przyznany uchwałą nr 118/2023 Prezydium Polskiej Komisji Akredytacyjnej z dnia 23 lutego 2023 r. w związku z oceną programową zakończoną uchwałą nr 116/2023 Prezydium Polskiej Komisji Akredytacyjnej z dnia 23 lutego 2023 r.

11. ZAŁĄCZNIKI, OPINIE I UCHWAŁY

Załącznik nr 1
do programu studiów na kierunku „Kryptologia i cyberbezpieczeństwo”

WARUNKI, ZASADY I TRYB UDZIELANIA URLOPÓW ŻOŁNIERZOM PEŁNIĄCYM ZAWODOWĄ SŁUŻBĘ WOJSKOWĄ W TRAKCIE KSZTAŁCENIA W WOJSKOWEJ AKADEMII TECHNICZNEJ

Na podstawie art. 280 ust. 7 ustawy o obronie Ojczyzny (Dz. U. poz. 655, z późn. zm.) ustala się następujące warunki, zasady i tryb udzielania urlopów żołnierzowi pełniącemu zawodową służbę wojskową w trakcie kształcenia, o którym mowa w art. 95 ust. 5 tej ustawy, zwanemu dalej „żołnierzem zawodowym”:

§ 1. 1. Żołnierzowi zawodowemu w trakcie kształcenia w uczelni wojskowej przysługuje coroczny urlop wypoczynkowy w wymiarze 30 dni kalendarzowych – po zakończeniu każdego roku studiów lub nauki oraz dodatkowy urlop na warunkach urlopu wypoczynkowego w wymiarze:

1) 10 dni kalendarzowych – w okresie zimowym;

2) 5 dni kalendarzowych – w okresie wiosennym;

3) liczby dni pozostających do zakończenia sesji egzaminacyjnej – po wcześniejszym zaliczeniu tej sesji.

2. Urlopów, o których mowa w ust. 1, udziela się jednorazowo, w jednym nieprzerwanym okresie, w miarę możliwości w jednym terminie dla całego rocznika żołnierzy lub stanu osobowego pododdziału, jeżeli nie koliduje to z programem kształcenia lub zaplanowanymi zadaniami realizowanymi przez uczelnię lub pododdział.

3. W przypadku, jeżeli żołnierz nie zakończył w terminie danego roku studiów, w uzasadnionym przypadku, jeżeli istnieją przesłanki, że zakończy on rok studiów w dodatkowym terminie wyznaczonym przez rektora- komendanta uczelni wojskowej, udziela się temu żołnierzowi corocznego urlopu wypoczynkowego na ogólnych zasadach lub po zakończeniu danego roku studiów.

4. Coroczny urlop wypoczynkowy planuje się w takim terminie, aby jego wykorzystanie nastąpiło przed rozpoczęciem kolejnego roku studiów.

§ 2. Żołnierzowi zawodowemu w trakcie kształcenia w uczelni wojskowej może być udzielony urlop okolicznościowy, na jego pisemny udokumentowany wniosek, w wymiarze jednorazowo do 5 dni roboczych – w przypadku:

1) zgonu i pogrzebu lub ciężkiej choroby najbliższego członka rodziny, za którego uważa się małżonka, dziecko, ojca, matkę, byłego opiekuna prawnego, siostrę, brata, babkę lub dziadka żołnierza, a także dziecko, ojca, matkę lub byłego opiekuna prawnego małżonka żołnierza;

2) zawarcia związku małżeńskiego przez żołnierza;

3) urodzenia się dziecka żołnierza;

4) potrzeby załatwienia spraw rodzinnych i osobistych.

§ 3. 1. Urlopów, o których mowa w § 1 i 2, udziela, określając ich terminy rektor - komendant uczelni wojskowej.
2. Urlopu, o którym mowa w § 2, udziela przełożony w jednostce wojskowej, w której żołnierz zawodowy w trakcie kształcenia w uczelni wojskowej odbywa praktykę.

§ 4. 1. Żołnierzowi w trakcie kształcenia w uczelni wojskowej może być udzielony urlop nagrodowy w łącznym wymiarze do 12 dni w ciągu roku kalendarzowego.
2. Urlop nagrodowy udzielony przez przełożonego w jednostce wojskowej, w której żołnierz w trakcie kształcenia w uczelni wojskowej odbywa praktykę, wykorzystuje się przed zakończeniem tej praktyki.

§ 5. 1. Żołnierzowi w trakcie kształcenia w uczelni wojskowej może być, na jego uzasadniony wniosek, przedłużony urlop, o którym mowa w § 1 i 2, w wymiarze do 5 dni kalendarzowych w razie:
1) choroby żołnierza;
2) śmierci lub ciężkiej choroby członka najbliższej rodziny żołnierza;
3) klęski żywiołowej, która dotknęła żołnierza lub członków jego najbliższej rodziny;
4) zaistnienia uzasadnionych przyczyn uniemożliwiających jego powrót z urlopu.
2. O przedłużenie urlopu, w przypadkach określonych w ust. 1, żołnierz niezwłocznie informuje przełożonego o zaistniałej sytuacji oraz zwraca się z pisemną prośbą do dowódcy (komendanta) garnizonu, w którym przebywa, lub najbliższego szefa Wojskowego Centrum Rekrutacji, przedkładając odpowiednie dokumenty na potwierdzenie zaistniałej okoliczności.

§ 6. 1. Udzielenie żołnierzowi urlopu ogłasza się w rozkazie dziennym rektora-komendanta uczelni wojskowej.
2. W rozkazie, o którym mowa w ust. 1, podaje się rodzaj urlopu, jego wymiar oraz termin rozpoczęcia i zakończenia.
3. Odwołanie żołnierza z urlopu stwierdza się w rozkazie dziennym rektora-komendanta uczelni wojskowej. Odwołanie powinno być uzasadnione i mieć wyjątkowy charakter.
4. Odwołanie żołnierza z urlopu następuje w formie pisemnego zawiadomienia lub w formie powiadomienia ustalonego z żołnierzem przed jego udaniem się na urlop.
5. Żołnierz odwołany z urlopu niezwłocznie stawia się w miejscu pełnienia służby.
6. Żołnierzowi odwołanemu z corocznego urlopu wypoczynkowego przysługuje ponownie ten urlop w pełnym wymiarze, jeżeli żołnierz przebywał na nim nie dłużej niż 3 dni kalendarzowe. W pozostałych przypadkach żołnierzowi przysługuje urlop w wymiarze niewykorzystanym.
7. Żołnierzowi odwołanemu z corocznego urlopu wypoczynkowego udziela się ponownie tego urlopu po ustaniu przyczyny z powodu, której został on z niego odwołany.

§ 7. W przypadku żołnierza kształcącego się w kraju w uczelni innej niż wojskowa urlopu udziela przełożony żołnierza wskazany przez rektora-komendanta uczelni wojskowej, na zaopatrzeniu której znajduje się żołnierz.

§ 8. W przypadku żołnierza skierowanego w trakcie kształcenia na naukę poza granicami kraju warunki, zasady i tryb udzielania urlopu określane są przez uczelnię zagraniczną, w której podjął kształcenie, zgodnie z programem kształcenia.

§ 9. W przypadku żołnierza powołanego do zawodowej służby wojskowej w trybie art. 793 ust. 2 ustawy o obronie Ojczyny, który nie wykorzystał corocznego urlopy wypoczynkowego należnego za rok studiów przed tym powołaniem, udziela się corocznego urlopu wypoczynkowego, o którym mowa w § 1 ust. 1.

§ 10. Ustalenia, o których mowa w § 1-9, nie naruszają uprawnień żołnierza do następujących urlopów przysługujących mu na podstawie:

1) art. 285 ustawy o obronie Ojczyny – do urlopu bezpłatnego na okres ciąży i połogu;
2) art. 346 ustawy o obronie Ojczyny – do urlopu bezpłatnego z tytułu prowadzenia własnej kampanii wyborczej do Sejmu Rzeczypospolitej Polskiej i Senatu Rzeczypospolitej Polskiej oraz Parlamentu Europejskiego, na kierownicze stanowiska w państwie obsadzane na podstawie wyboru oraz do organów samorządu terytorialnego.

Kamila Nawotczyńska
Gen. S. Kaliskiego 11A
01-476 Warszawa
kamila.nawotczynska@student.wat.edu.pl
+48 512 949 576

Warszawa dn. 16.06.2025 r.

OPINIA

Dotyczy: *Programów studiów na kierunku Kryptologia i cyberbezpieczeństwo oraz na kierunku Informatyka*

Rada Samorządu Wydziału Cybernetyki na posiedzeniu w dniu 16.06.2025 r. rozpatrzyła pozytywnie:

- program studiów na kierunku Informatyka, I st., realizowanych w formie stacjonarnej
- program studiów na kierunku Informatyka, I st., realizowanych w formie niestacjonarnej
- program studiów na kierunku Informatyka, II st., realizowanych w formie niestacjonarnej
- program studiów na kierunku Informatyka, jednolitych magisterskich dla kandydatów na oficerów
- program studiów na kierunku Kryptologia i cyberbezpieczeństwo, I st., realizowanych w formie stacjonarnej
- program studiów na kierunku Kryptologia i cyberbezpieczeństwo, I st., realizowanych w formie niestacjonarnej
- programów studiów na kierunku Kryptologia i cyberbezpieczeństwo, jednolitych magisterskich dla kandydatów na oficerów

Przewodniczący RS WCY
p. o. Kamila Nawotczyńska

Kamila Nawotczyńska

Wojskowa Akademia Techniczna

Wydział Cybernetyki

Opinia
Wydziałowej Rady ds. Kształcenia
Wydziału Cybernetyki Wojskowej Akademii Technicznej

nr 13/WRdsK/2025 z dnia 17 czerwca 2025 r.

w sprawie projektów programów studiów I, II stopnia i jednolitych studiów magisterskich dla kandydatów na oficerów prowadzonych w WCY

Na podstawie § 92 ust. 1 pkt. 1 *Statutu WAT, stanowiącego załącznik do uchwały Senatu WAT nr 16/WAT/2019 z dnia 25 kwietnia 2019 r. w sprawie uchwalenia Statutu Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego* (tj. obwieszczenie Rektora WAT nr 2/WAT/2024 z dnia 27 marca 2024 r.) oraz § 17 ust. 1 pkt. 1 *Regulaminu Wydziałowej Rady do spraw Kształcenia Wydziału Cybernetyki Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego* stanowiącego załącznik *do decyzji Dziekana Wydziału Cybernetyki Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego nr 57/WCY/2019 z dnia 4 listopada 2019 r. w sprawie nadania regulaminu wydziałowej radzie do spraw kształcenia* ze zmianami wprowadzonymi *Decyzją Dziekana nr 32/WCY/2022 z dnia 28 czerwca 2022 r.* postanawia się, co następuje

§ 1

Pozytywnie opiniuje się projekty niżej wymienionych programów studiów dla studiów rozpoczynających się od roku akademickiego 2025/2026:

1) projekty programów studiów stacjonarnych i niestacjonarnych I stopnia na kierunku *informatyka* stanowiące załączniki nr 1, 2 do opinii;
2) projekt programu studiów niestacjonarnych II stopnia na kierunku *informatyka* stanowiący załącznik nr 3 do opinii;
3) projekty programów studiów stacjonarnych i niestacjonarnych I stopnia na kierunku *kryptologia i cyberbezpieczeństwo* stanowiące załączniki nr 4, 5 do opinii;
4) projekty programów jednolitych studiów magisterskich dla kandydatów na oficerów na kierunkach:
   a) *informatyka* – stanowiący załącznik nr 6 do opinii,
   b) *kryptologia i cyberbezpieczeństwo* – stanowiący załącznik nr 7 do opinii.

PRZEWODNICZĄCY
Wydziałowej Rady ds. Kształcenia
dr inż. Dariusz PIERZCHAŁA, prof. WAT

ARKUSZ UZGODNIEŃ
do projektu programu studiów dla kandydatów na oficerów

Uczelnia: WOJSKOWA AKADEMIA TECHNICZNA

Kierunek studiów: KRYPOLOGIA I CYBERBEZPIECZEŃSTWO

Poziom studiów: jednolite studia magisterskie

Profil studiów: ogólnoakademicki

Korpus osobowy: KRYPTOLOGII I CYBERBEZPIECZEŃSTWA
grupa osobowa kryptologii,
grupa osobowa cyberbezpieczeństwa

Rok rozpoczęcia kształcenia: 2025/2026

Nazwa komórki (jednostki) organizacyjnej, z którą projekt był uzgadniany	Stanowisko instytucji opiniującej (*uzgodniono /nie uzgodniono*) *Uwagi*	Stopień, imię, nazwisko i podpis osoby opiniującej oraz pieczęć urzędowa instytucji
Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni	Uzgodniono DOWÓDZTWO KOMPONENTU WOJSK OBRONY CYBERPRZESTRZENI VIII	Z upoważnienia DOWÓDCY KOMPONENTU WOJSK OBRONY CYBERPRZESTRZENI płk Grzegorz WIELOSZ Szef Sztabu 11.06.2025

ARKUSZ UZGODNIEŃ
do projektu programu studiów dla kandydatów na oficerów

Uczelnia: WOJSKOWA AKADEMIA TECHNICZNA

Kierunek studiów: KRYPTOLOGIA I CYBERBEZPIECZEŃSTWO

Poziom studiów: jednolite studia magisterskie

Profil studiów: ogólnoakademicki

Korpus osobowy: KRYPTOLOGII I CYBERBEZPIECZEŃSTWA
grupa osobowa kryptologii
grupa osobowa cyberbezpieczeństwa

Rok rozpoczęcia kształcenia: 2025/2026

Nazwa komórki (jednostki) organizacyjnej, z którą projekt był uzgadniany	Stanowisko instytucji opiniującej (uzgodniono /nie uzgodniono) Uwagi	Stopień, imię, nazwisko i podpis osoby opiniującej oraz pieczęć urzędowa instytucji
Departament Szkolnictwa Wojskowego	Uzgodniono	DYREKTOR DEPARTAMENTU SZKOLNICTWA WOJSKOWEGO Jakub MYKOWSKI