Załącznik nr 2
do uchwały Senatu WAT nr 136/WAT/2023
z dnia 28 września 2023 r.

WOJSKOWA AKADEMIA TECHNICZNA
im. Jarosława Dąbrowskiego

Wydział Cybernetyki

PROGRAM STUDIÓW

Poziom studiów: studia drugiego stopnia

Kierunek studiów: „kryptologia i cyberbezpieczeństwo”

Profil studiów: ogólnoakademicki

Forma studiów: stacjonarne

Uchwała Senatu Wojskowej Akademii Technicznej
im. Jarosława Dąbrowskiego
nr 136/WAT/2023 z dnia 28 września 2023 r.

Obowiązuje od roku akademickiego 2023/2024

Warszawa

2023

Spis treści

PROGRAM STUDIÓW
założenia organizacyjne

dla kierunku studiów „kryptologia i cyberbepieczeństwo”

Poziom studiów drugi

Profil studiów ogólnoakademicki

Forma(y) studiów stacjonarna

Tytuł zawodowy nadawany absolwentom magister inżynier

Poziom Polskiej Ramy Kwalifikacji siódmy (7)

Kierunek studiów przyporządkowany jest do:

Dziedzina nauki inżynieryjno-techniczne

Dyscyplina naukowa informatyka techniczna i telekomunikacja

W programie specjalności profilowanej przedmiotami wybieralnymi	*% udział ECTS dla dyscypliny naukowej*
bezpieczeństwo informacyjne	**83%**
cyberobrona	**83%**
systemy kryptograficzne	**80%**
bezpieczeństwo systemów informatycznych	**83%**

Język studiów polski

Liczba semestrów trzy

Łączna liczba godzin

W programie specjalności profilowanej przedmiotami wybieralnymi	*Łączna liczba godzin*
bezpieczeństwo informacyjne	**802**
cyberobrona	**794**
systemy kryptograficzne	**804**
bezpieczeństwo systemów informatycznych	**802**

Liczba punktów ECTS konieczna do ukończenia studiów **90**

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*
bezpieczeństwo informacyjne	**45,5**
cyberobrona	**45,5**
systemy kryptograficzne	**46,5**
bezpieczeństwo systemów informatycznych	**48,5**

- **z dziedziny nauk humanistycznych lub nauk społecznych - 5**

CHARAKTERYSTYKA KIERUNKU STUDIÓW

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. Kierunek jest odpowiedzią na rosnące zapotrzebowanie na specjalistów z zakresu najnowszych osiągnięć naukowych i technologicznych w obszarze IT/InfoSec. Program studiów obejmuje efekty uczenia się właściwe dla obszaru kształcenia w zakresie nauk technicznych, dziedziny nauk technicznych i dyscypliny naukowej informatyka techniczna i telekomunikacja.

REALIZACJA STUDIÓW

Kierunek „kryptologia i cyberbezpieczeństwo" realizowany jest niemalże w całości przez Wydział Cybernetyki, ze wsparciem innych jednostek organizacyjnych WAT w przedmiotach reprezentujących dziedziny nauk humanistycznych i społecznych. Istotną cechą koncepcji kształcenia na kierunkach prowadzonych przez Wydział Cybernetyki jest ciągła konfrontacja i modyfikowanie treści kształcenia z potrzebami rynku i pracodawców. Na kształt programu silny wpływ mają interesariusze z otoczenia społeczno-gospodarczego, wpływając na treści programu studiów, uzyskiwane przez absolwentów efekty kształcenia oraz program i miejsca praktyk zawodowych. Ponadto, kształcenie jest powiązane z prowadzonymi w Wydziale badaniami naukowymi.
Studia drugiego stopnia trwają jeden i pół roku, obejmują trzy semestry i kończą się nadaniem tytułu zawodowego magistra inżyniera.

SYLWETKA OSOBOWO-ZAWODOWA ABSOLWENTA

Absolwent tego kierunku uzyskuje zaawansowaną wiedzę i umiejętności z zakresu

informatyki, szczególnie z zakresu sieci komputerowych, a także wiedzę z zakresu inżynierii bezpieczeństwa, w tym zwłaszcza z obszaru bezpieczeństwa systemów technicznych. W tym obszarze absolwenci będą ekspertami w zakresie eksploracji sieci rozumianej jako wyszukiwanie i korelacja informacji o systemach teleinformatycznych oraz rozpoznawanie, badanie i identyfikację zasobów sieci. Ponadto poznają charakterystykę i narzędzia przeprowadzanych ataków sieciowych oraz uzyskują wiedzę i umiejętności w zakresie wykorzystywania różnorodnych zabezpieczeń teleinformatycznych. Posiadać będą wiedzę i umiejętności w zakresie obsługi urządzeń sieciowych, administrowania systemami operacyjnymi Windows i Linux, projektowania i zarządzania bezpieczeństwem w zakresie sieci bezprzewodowych. Studenci uzyskują również umiejętności w zakresie projektowania i implementacji oprogramowania systemów rozproszonych, z zastosowaniem współcześnie stosowanych technologii, w tym IoT.
Potencjalnymi miejscami pracy są: struktury instytucji państwowych odpowiedzialnych za bezpieczeństwo, Dowództwo Komponentu WOC, gospodarka narodowa, instytucje zajmujące się analizą i oceną bezpieczeństwa i ryzyka, podmioty zaangażowane w projektowanie systemów bezpieczeństwa informacji.

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,

[1] *dotyczy kierunków studiów, absolwentom których nadawany jest tytuł zawodowy: inż., mgr inż.*

- 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]_P6S_WG - kod składnika opisu charakterystyk drugiego stopnia dla kwalifikacji na poziome 6 Polskiej Ramy Kwalifikacji.

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 rozszerzonym zakresie problematykę wybranych działów matematyki, niezbędną do: analizowania, modelowania, konstruowania i eksploatacji systemów informatycznych	P7S_WG
K_W03	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	P7S_WK P7S_WG Inż_P7S_WG
K_W04	zna i rozumie w pogłębionym stopniu teorię algorytmów i struktur danych, zarządzania danymi oraz narzędzia, modele, metody i metodyki projektowania systemów informatycznych (różnych klas i rodzajów), jak również wytwarzania oprogramowania pracującego pod ich kontrolą	P7S_WG Inż_P7S_WG
K_W05	zna i rozumie w pogłębionym zakresie metody i narzędzia wykorzystywane do modelowania oraz symulacji obiektów i systemów, formułowania i rozwiązywania problemów decyzyjnych oraz problemów z zakresu inteligencji obliczeniowej	P7S_WG
K_W06	zna podstawowe techniki testowania podzespołów sprzętowych i oprogramowania, zasady projektowania struktur diagnostycznych i techniki tolerowania błędów	P7S_WG
K_W07	ma rozszerzoną i pogłębioną wiedzę w zakresie zasad funkcjonowania sieci komputerowych, usług sieciowych, projektowania i zarządzania sieciami komputerowymi w tym administrowania sieciowymi systemami operacyjnymi	P7S_WG
K_W08	ma pogłębioną wiedzę w zakresie metod i technik zapewniania bezpieczeństwa systemów informatycznych	P7S_WG

[2] *w przypadku kompetencji inżynierskich;*

K_W09	zna i rozumie procesy zarządzania oraz w pogłębionym stopniu informatyczne metody, narzędzia oraz środowiska służące do wspomagania tych procesów	P7S_WG
K_W10	zna i rozumie ekonomiczne, prawne i inne uwarunkowania różnych rodzajów działań związanych z wykorzystywaniem metod i środków informatyki, w tym zasady ochrony własności przemysłowej i prawa autorskiego	P7S_WK
K_W11	zna i rozumie ogólne zasady tworzenia i rozwoju form indywidualnej przedsiębiorczości	P7S_WK Inż_P7S_WK
K_W12	zna i rozumie zasady konstrukcji i eksploatacji algorytmów szyfrowania	P7S_WK
	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	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_U03	umie pracować w zespole, kierować zespołem projektowym, dokonać krytycznej analizy istniejących rozwiązań technicznych, wstępnej oceny ekonomicznej oraz zarządzać procesami wdrażania, utrzymywania i doskonalenia systemów informatycznych, a także komunikować się z odbiorcami tych systemów	P7S_UW P7S_UO P7S_UK Inż_P7S_UW
K_U04	potrafi zarządzać procesami analizy oraz dokumentowania zadania projektowego i badawczego z zastosowaniem inżynierii oprogramowania oraz wybranych metod i narzędzi wytwarzania oprogramowania	P7S_UW Inż_P7S_UW
K_U05	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; potrafi zaplanować i przeprowadzić eksperymenty obliczeniowe i symulacyjne oraz dokonać przetworzenia i interpretacji ich wyników	P7S_UW Inż_P7S_UW
K_U06	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_U07	umie wykorzystać rozszerzoną i pogłębioną wiedzę w zakresie zasad funkcjonowania sieci komputerowych, usług sieciowych, projektowania i zarządzania sieciami komputerowymi, w tym administrowania sieciowymi systemami operacyjnymi	P7S_UW
K_U08	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_U09	potrafi stosować metody i techniki oceniania oraz zapewniania bezpieczeństwa systemów informatycznych	P7S_UW Inż_P7S_UW
K_U10	potrafi wykorzystać wiedzę z zakresu procesów zarządzania organizacją oraz informatyczne metody, narzędzia i środowiska do wspomagania tych procesów	P7S_UW

K_U11	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_U12	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_U13	potrafi posługiwać się językiem obcym na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego, w stopniu pozwalającym na porozumiewania się w mowie i w piśmie w zakresie ogólnym oraz w wyższym stopniu w zakresie terminologii informatycznej	P7S_UK
K_U14	potrafi samodzielnie planować i realizować własne permanentne uczenie się i ukierunkowywać innych w tym zakresie	P7S_UU
K_U15	umie wykorzystywać wybrane algorytmy kryptograficzne	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	P7S_KK
K_K02	jest gotów do wypełniania zobowiązań społecznych	P7S_KO
K_K03	jest gotów do inspirowania i organizowania działalności na rzecz środowiska społecznego	P7S_KO
K_K04	jest gotów do inicjowania działania na rzecz interesu publicznego	P7S_KO
K_K05	jest gotów do: - myślenia i działania w sposób przedsiębiorczy - 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

WYKAZ ZAJĘĆ

Grupy zajęć / przedmioty , ich skrócone opisy (programy ramowe), przypisane do nich punkty ECTS i efekty uczenia (odniesienie do efektów kierunkowych)

l.p.	nazwa grupy zajęć / przedmiot z opisem	liczba punktów ECTS	kod dyscy-pliny	odniesienie do efektów kierunkowych
	A. Grupa treści kształcenia ogólnego	**2**		
A1	***BEZPIECZEŃSTWO I HIGIENA PRACY*** Treść programu ramowego: BHP w obowiązującym stanie prawnym. Zasady bezpieczeństwa i higieny pracy (nauki) - reguły bezpiecznego postępowania, wymagane przy wykonywaniu określonej pracy (czynności), wynikające z przesłanek naukowych i technicznych. Ochrona przed	**0**		K_W10

	zagrożeniami dla zdrowia i bezpieczeństwa studentów. Stosowanie środków ochrony indywidualnej na zajęciach (ćwiczeniach). Ubezpieczenia od następstw nieszczęśliwych wypadków. Postępowanie w razie wypadków i w sytuacjach zagrożeń. Zasady udzielania pierwszej pomocy przedlekarskiej.			
A1	***JĘZYK OBCY*** Treść programu ramowego: Materiał strukturalno-gramatyczny; powtórzenie, rozszerzenie i usystematyzowanie następujących zagadnień; czasy gramatyczne/czasy narracji; strona czynna/bierna; mowa zależna; tryb warunkowy; tworzenie pytań; kolokacje; zdania złożone; szyk wyrazów w zdaniu; czasowniki modalne; czasowniki frazowe; Materiał pojęciowo-funkcyjny; prośby; sugestie; oferty; porady; przyzwolenie/odmowa; zaprzeczenia; zgoda/niezgoda; wyrażanie opinii; przyczyny/skutku; powodu/celu; życzenie, przepraszanie; podsumowanie; wybór rejestru/stylu.	**2**	J	K_U02
	B. Grupa treści kształcenia podstawowego	**8**		
B1	***NOWOCZESNE METODY I TECHNIKI ZARZĄDZANIA*** Treść programu ramowego: System zarządzania organizacją. Ewolucja teorii i praktyki zarządzania. Uwarunkowania i wyzwania współczesnego zarządzania. Koncepcje zorientowane na klienta. Nowoczesny marketing. Zarządzanie 2.0: nowe paradygmaty. Orientacja organizacji na jakość. Koncepcje zarządzania jakością: TQM, ISO 9000, Six Sigma. System zrównoważonego zarządzania. Orientacje organizacji na innowacje i know-how. Zasady i błędy w przekształcania organizacji. Koncepcje optymalizujące działanie organizacji. Koncepcje zorientowane na wiedzę, człowieka i podejście zasobowe. Koncepcje organizacji uczącej się i inteligentnej. Kapitał niematerialny wybranych przedsiębiorstw – analiza porównawcza. Koncepcje nowych układów strukturalnych. Organizacje wirtualne i sieciowe. Analiza porównawcza nowoczesnych metod i technik zarządzania.	**2**	NZJ	K_W09, K_W11, K_U10, K_U14, K_K01, K_K05, K_K06
B2	***PROCESY STOCHASTYCZNE*** Treść programu ramowego: Ciągi losowe. Klasyfikacja i parametry procesów stochastycznych. Przykłady procesów. Łańcuchy Markowa. Procesy Markowa. Klasyfikacja stanów. Ergodyczność. Procesy zliczające. Proces urodzeń i śmierci. Systemy kolejkowe	**3**	M	K_W02, K_W05, K_U02, K_U14
B3	***EKONOMIA*** Treść programu ramowego: Wprowadzenie do nauki ekonomii. Rynek i gospodarka rynkowa. Podstawy decyzji ekonomicznych konsumenta, popyt konsumenta. Produkcja, koszty produkcji. Modele struktur rynkowych - konkurencja doskonała. Rachunek dochodu narodowego. Determinanty dochodu narodowego. Równowaga makroekonomiczna. Popyt globalny a polityka fiskalna. System bankowy i podaż pieniądza. Polityka pieniężna i fiskalna w gospodarce zamkniętej. Inflacja, przyczyny i skutki.	**2**	EF	K_W01, K_U01, K_U14, K_K03, K_K05,
B4	***SOCJOLOGIA*** Treść programu ramowego: Zapoznanie z podstawowymi pojęciami, koncepcjami i zastosowaniami socjologii w nauce i praktyce życia społecznego. Ukazanie możliwości socjologii w kształtowaniu wizji bezpieczeństwa narodowego. Ukazanie wspólnotowego charakteru struktur społeczeństwa i ich wpływu na rozwój cywilizacyjny. Przygotowanie do aktywnego udziału w życiu społecznym w duchu służebności i zaangażowania. Elementy struktury społecznej. Statusy i role. Organizacje, instytucje, wspólnoty i interakcje społeczne.	**1**	NS	K_W01, K_U01, K_U14, K_K02, K_K03, K_K04, K_K06

	Zbiorowości i wartości wspólnotowe (wspólno-grupowe). Wewnętrzna organizacja grupy. Relacje międzyludzkie (inscenizacja interakcji). Socjalizacja, stratyfikacja społeczna.			
	C. Grupa treści kształcenia kierunkowego	**20**		
C1	***BEZPIECZEŃSTWO BAZ DANYCH*** Treść programu ramowego: 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.	**3**	ITT	K_W06, K_W08, K_U05, K_U06, K_U07, K_U11
C2	***STEGANOGRAFIA*** Treść programu ramowego: 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 uniwersalnej. Kodowanie macierzowe. Wet Paper Codes.	**3**	ITT	K_W03, K_W04, K_W08, K_U09, K_U14, K_K01
C3	***DIAGNOSTYKA I TOLEROWANIE USZKODZEŃ*** Treść programu ramowego: Wprowadzenie, podstawowe pojęcia wiarygodności systemów: wiarygodność a niezawodność systemów komputerowych, podstawowy łańcuch zagrożeń dla wiarygodności, strategie i techniki zwiększania wiarygodności, tolerowanie uszkodzeń. Testowanie i niezawodność układów cyfrowych: modele błędów, elementy ogólnej teorii testów, metody wyznaczania testów. Techniki testowania: generacja wymuszeń, analiza wyników, testowanie z kompresją wyników, analiza sygnatur. Algebra Roth'a. D-algorytm i jego modyfikacje. Wyznaczanie testów dla automatów sekwencyjnych. Problemy testowalności układów VLSI: układy łatwo testowalne (Design for Testability). Ścieżka krawędziowa, magistrala diagnostyczna, standard IEEE 1149.x. Układy samosprawdzalne, samotestujące (BIST) i układy typu fail-safe. Diagnostyka systemowa: modele i metody diagnostyki systemowej (PMC, BGM, MM), miary diagnozowalności. Struktury samodiagnozowalne i ich wyznaczanie. Strategie diagnostyczne. Algorytmy identyfikacji niezdatnych elementów systemu (scentralizowane, rozproszone, adaptacyjne). Zastosowanie metod diagnostyki w systemach z łagodną degradacją. Zastosowanie N-krotnej redundancji, problem konsensusu w systemach rozproszonych, problem Bizantyjskich Generałów (BGP), algorytm Lamporta, algorytm PBGP. Konsensus a diagnostyka systemowa. Architektura systemów odpornych na błędy. Systemy samosprawdzalne oraz samonaprawialne (ang. self-healing). Zastosowanie redundancji informacyjnej w układach kryptograficznych: techniki kodowania, kody detekcji i korekcji błędów, wykrywanie i korygowanie błędów seryjnych (grupowych), kody jednokierunkowe, kody arytmetyczne. Techniki i narzędzia oceny niezawodności. Analiza odpornych na uszkodzenia architektur sprzętowych i programowych. Detekcja i tolerowanie uszkodzeń w systemach kryptograficznych: tolerowa-nie uszkodzeń w układach szyfratorów, detekcja ataków typu "fault injection", środki zapobiegania atakom.	**4**	ITT	K_W06, K_U02, K_U06, K_K01, K_K05, K_K06
C4	***WIRTUALIZACJA SYSTEMÓW IT*** Treść programu ramowego:	**2**	ITT	K_W05, K_U08, K_K01, K_K06

	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.			
C5	***TECHNIKI ALGORYTMICZNE*** Treść programu ramowego: 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.	**3**	ITT	K_W03, K_W04, K_W09, K_U03, K_U04
C6	***METODY NUMERYCZNE W KRYPTOLOGII*** Treść programu ramowego: Podstawowe pojęcia analizy numerycznej. Arytmetyka stałoprzecinkowa. Arytmetyka zmiennoprzecinkowa i błędy zaokrągleń w obliczeniach komputerowych. Uwarunkowanie zadania. Algorytmy numerycznie poprawne. Normy wektorów i macierzy. Wektory i wartości własne macierzy. Formy kwadratowe. Bezpośrednie metody rozwiązywania układów liniowych równań algebraicznych. Wskaźnik uwarunkowania macierzy. Metoda Gaussa. Rozkład trójkątno-trójkątny macierzy kwadratowej. Metoda Choleskyego-Banachiewicza. Rozkład ortonormalno-trójkątny macierzy. Rozkład macierzy według wartości szczególnych. Liniowe zadanie najmniejszych kwadratów w postaci algebraicznej. Zadanie nadokreślone z macierzą pełnego rzędu. Algorytm z równaniem normalnym. Uwarunkowanie zadania. Zadanie nieregularne i regularyzacja. Iteracyjne metody rozwiązywania układów liniowych równań algebraicznych	**5**	M	K_W02, K_U02
	D. Grupa treści kształcenia specjalistycznego – wybieralnego	**38**		
specjalność „bezpieczeństwo informacyjne”				
DB1	***BAZY DANYCH NOSQL*** Treść programu ramowego: Nierelacyjne bazy danych, architektury i paradygmaty baz NoSQL, przegląd wybranych systemów baz danych NoSQL, języki w bazach NoSQL, przykłady zastosowań baz NoSQL.	**3**	ITT	K_W03, K_W04, K_W09, K_U03, K_U04
DB2	***MODELOWANIE I ANALIZA SIECI ZŁOŻONYCH*** Treść programu ramowego: Modele sieci złożonych. Dynamika sieci złożonych. 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.	**4**	ITT	K_W02, K_W04, K_W05, K_U02, K_U05, K_U14

DB3	***ZARZĄDZANIE PROJEKTAMI*** Treść programu ramowego: 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.	**3**	ITT	K_W03, K_W04, K_U03, K_U04, K_K01, K_KK06
DB4	***ZAAWANSOWANE METODY UCZENIA MASZYNOWEGO*** Treść programu ramowego: Metody i algorytmy uczenia maszynowego – wprowadzenie. Sztuczne sieci neuronowe w uczeniu maszynowym. Metody głębokiego uczenia. Sieci konwolucyjne. Sieci rekurencyjne. Złożone systemy uczące się.	**3**	ITT	K_W02, K_W05, K_W09, K_U02, K_U04, K_U14
DB5	***BUSSINES MODELING IN UML*** ***(w języku angielskim)*** Treść programu ramowego: 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.	**3**	ITT	K_W09, K_U10, K_U13
DB6	***ROZPROSZONE PRZETWARZANIE DANYCH*** Treść programu ramowego: 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.	**4**	ITT	K_W03, K_W04, K_W09, K_U03, K_U04
DB7	***PODSTAWY KRYPTOLOGII WSPÓŁCZESNEJ*** Treść programu ramowego: 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.	**3**	ITT	K_W03, K_W04, K_W08, K_W09, K_W12, K_U03, K_U10, K_U12, K_U15
DB8	***PRZETWARZANIE JĘZYKA NATURALNEGO*** Treść programu ramowego: Omówienie dziedziny maszynowego przetwarzania języka naturalnego , analiza syntaktyczna i semantyczna zdań zapisanych w	**3**	ITT	K_W03, K_W04, K_W09, K_U03, K_U04

	języku naturalnym, analiza korpusów tekstów, n-gramy, algorytmy wyszukiwania kolokacji wyrazowych, modele statystyczne języków naturalnych, analiza sentymentu, przykłady zastosowań systemów przetwarzania języka naturalnego.			
DB9	***BIG DATA – PROJEKT Z ZAKRESU BEZPIECZEŃSTWA INFORMACJI*** Treść programu ramowego: 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.	**4**	ITT	K_W06, K_W09, K_W11, K_U03, K_U04, K_U05, K_U06, K_U12, K_K02, K_K03
DB10	***ZARZĄDZANIE WIEDZĄ*** Treść programu ramowego: 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).	**3**	ITT	K_W03, K_W04, K_W05, K_U03, K_U10
DB11	***ILOŚCIOWE METODY OCENY BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH*** Treść programu ramowego: 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.	**3**	ITT	K_W02, K_W05, K_W08, K_U02, K_U05, K_U09, K_U14, K_K01
DB14	***TEORIA WOJNY INFORMACYJNEJ*** Treść programu ramowego: Formy działań stosowane w cyberprzestrzeni: operacje psychologiczne, strategie prowadzenia działań w cyberprzestrzeni; kierowanie działaniami w cyberprzestrzeni: planowanie działań, monitorowanie, sterowanie działaniami. Modele walki w cyberprzestrzeni. Symulacja procesów walki w cyberprzestrzeni. Zdolności do prowadzenia działań w cyberprzestrzeni.	**2**	ITT	K_W01, K_W02, K_W04, K_W05, K_U01, K_U02, K_U05, K_U14
specjalność „bezpieczeństwo systemów informatycznych				
DS1	***SYSTEMY WEBOWE*** Treść programu ramowego: 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.	**3**	ITT	K_W03, K_W08, K_U05, K_U09

	Zastosowanie w systemach webowych ontologii i sieci semantycznych. Aspekty bezpieczeństwa w systemach webowych.			
DS2	***MODELOWANIE I ANALIZA SIECI ZŁOŻONYCH*** Treść programu ramowego: Modele sieci złożonych. Dynamika sieci złożonych. 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.	**4**	ITT	K_W02, K_W04, K_W05, K_U02, K_U05, K_U14
DS3	***ZARZĄDZANIE PROJEKTAMI*** Treść programu ramowego: Podstawy zarządzania projektami. Studium wykonalności projektu. Podstawowe procesy zarządzania projektem. Procesy rozpoczęcia. Procesy planowania projektu. Procesy realizacji i kontroli. Procesy monitorowania i zamykania projektu. Podstawowe elementy metodyki prince2. Analiza jakościowa projektu. Tendencje rozwojowe zarządzania projektami.	**3**	ITT	K_W03, K_W04, K_U03, K_U04, K_K01, K_KK06
DS4	***BUSSINES MODELING IN UML*** ***(w języku angielskim)*** Treść programu ramowego: 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.	**3**	ITT	K_W09, K_U10, K_U13, K_U13
DS5	***ARCHITEKTURA KORPORACYJNA*** Treść programu ramowego: 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.	**3**	ITT	K_W02, K_W03, K_W04, K_W10, K_U03, K_U04, K_U10
DS6	***PODSTAWY KRYPTOLOGII WSPÓŁCZESNEJ*** Treść programu ramowego: 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.	**3**	ITT	K_W03, K_W04, K_W08, K_W09, K_W12, K_U03, K_U10, K_U12, K_U15
DS7	***INŻYNIERIA WSTECZNA SYSTEMÓW INFORMATYCZNYCH*** Treść programu ramowego: 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	**4**	ITT	K_W03, K_W08, K_U05, K_U09

	procesów. Metodyki i narzędzia informatyczne wspomagające eksplorację procesów.			
DS8	***NIEZAWODNOŚĆ I WYDAJNOŚĆ SYSTEMÓW INFORMATYCZNYCH*** Treść programu ramowego: Modele niezawodnościowe systemów komputerowych. Modele niezawodnościowe oprogramowania. Model niezawodnościowe systemów informatycznych. Zastosowanie systemów kolejkowych do oceny wydajności systemów informatycznych.	**3**	ITT	K_W02, K_W05, K_U02, K_U5, K_U14
DS9	***PROJEKT Z ZAKRESU BEZPIECZEŃSTWA SYSTEMÓW*** Treść programu ramowego: Zagrożenia zasobów informacyjnych. Metody oceny stanu bezpieczeństwa systemu informatycznego. Narzędzia – Katana. Badania techniczne, testy penetracyjne. Mechanizmy ochronne. Filtrowanie ruchu. Cyberobrona. Projektowanie systemu bezpieczeństwa informacji. Modernizacja eksploatowanego systemu bezpieczeństwa.	**4**	ITT	K_W06, K_W09, K_W11, K_U03, K_U04, K_U05, K_U06, K_U12, K_K02, K_K03
DS10	***INŻYNIERIA WSTECZNA ZŁOŚLIWEGO OPROGRAMOWANIA*** Treść programu ramowego: Podstawowe ataki teleinformatyczne; narzędzia ataków i testów 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.	**3**	ITT	K_W03, K_W08, K_U05, K_U09
DS12	***ILOŚCIOWE METODY OCENY BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH*** Treść programu ramowego: 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.	**3**	ITT	K_W02, K_W05, K_W08, K_U02, K_U05, K_U09, K_U14, K_K01
DS13	***TEORIA WOJNY INFORMACYJNEJ*** Treść programu ramowego: Formy działań w cyberprzestrzeni stosowane w cyberprzestrzeni: operacje psychologiczne, strategie prowadzenia działań w cyberprzestrzeni, kierowanie działaniami w cyberprzestrzeni: planowanie działań, monitorowanie, sterowanie działaniami. Modele walki w cyberprzestrzeni. Symulacja procesów walki w cyberprzestrzeni. Zdolności do prowadzenia działań w cyberprzestrzeni.	**3**	ITT	K_W01, K_W02, K_W04, K_W05, K_U01, K_U02, K_U05, K_U14
specjalność „cyberobrona”				
DC1	***MODELOWANIE SYSTEMÓW TELEINFORMATYCZNYCH*** Treść programu ramowego: Tematyka wykładów:	**3**	ITT	K_U07, K-K01

	Inżynieria oparta na modelach, formalna weryfikacja. Podstawy modelowania ST w języku UML. Modelowanie wymagań na sys-tem teleinformatyczny. Modelowanie architektury i zachowania ST. Diagramy interakcji, diagram maszyny stanów. Rozszerzenia języ-ka UML do modelowania protokołów, aplikacji i usług sieciowych. Modelowanie protokołów: diagramy przepływu wywołań, prze-kształcanie diagramów wywołań do diagramu maszyny stanów. Podstawy weryfikacji systemu teleinformatycznego w oparciu o modele formalne: weryfikacja modelu, modele systemów równole-głych, własności liniowo-czasowe, bezpieczeństwo i żywotność. Sieci Petriego: definicja, własności modelu, drzewo osiągalności, wybrane rodzaje sieci Petriego. Modelowanie ST uwarunkowanych czasowo: rozszerzenia SP, czasowe i stochastyczne SP. Analiza prostych i przedziałowych czasowych SP. Modelowanie ST uwa-runkowanych czasowo: automaty czasowe. Przykładowe zadania modelowania systemów teleinformatycznych: badanie własności systemu na podstawie modelu. Tematyka ćwiczeń laboratoryjnych: Modelowanie protokołów z wykorzystaniem diagramów UML. Modelowanie protokołów i usług sieciowych z wykorzystaniem języków dziedzinowych. Budowa profilu języka modelowania. Modelowanie protokołów z wykorzystaniem sieci Petriego. Mode-lowanie systemów równoległych z wykorzystaniem kolorowanych sieci Petriego. Modelowanie ST uwarunkowanych czasowo z wyko-rzystaniem czasowych sieci Petriego. Modelowanie i weryfikacja ST uwarunkowanych czasowo z wykorzystaniem automatów czaso-wych. Tematyka zajęć projektowych: Wydanie i omówienie zadań projektowych z zakresu modelowania ST. Realizacja zadań projektowych według indywidualnego planu. Prezentacja rozwiązań i rozliczenie projektów.			
DC2	***BEZPIECZEŃSTWO SIECI IPv6*** Treść programu ramowego: 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.	**3**	ITT	K_W07, K_W08, K_U09, K_K03, K_K06
DC3	***ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI*** Treść programu ramowego: 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.	**4**	ITT	K_W03, K_W08, K_U10

DC4	***TRENDS IN COMPUTER TECHNOLOGY*** ***(w języku angielskim)*** Treść programu ramowego: 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.	**3**	ITT	K_W03, K_U08, K_K01, K_K06, K_U13
DC5	***TECHNOLOGIE MOBILNE*** Treść programu ramowego: 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.	**2**	ITT	K_W02, K_W07, K_U11, K_K05, K_K06
DC6	***PROJEKTOWANIE SYSTEMÓW BEZPIECZEŃSTWA INFORMACJI*** Treść programu ramowego: 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.	**4**	ITT	K_W03, K_W08, K_U04, K_K03, K_K06
DC7	***ANALIZA I PROJEKTOWANIE SYSTEMÓW TELEINFORMATYCZNYCH*** Treść programu ramowego: Paradygmaty modelowania systemów informatycznych (ST). Cykle życiowe; przegląd i klasyfikacja metodyk zrządzania projektowaniem systemów teleinformatycznych. Techniki oceny systemu. Wzorce projektowe GoF. Wprowadzenie do MDA. Symulacja modeli UML. Język modelowania systemów (SysML). Zaawansowane modele wdrożenia. DSM i DSML. Wprowadzenie do architektury zorientowanej na usługi (SOA). Proces SOMA. Modelowanie systemów zorientowanych na usługi w SoaML. Zarządzanie projektami i środowisko modelowania wymagań. Zaawansowane modelowanie dynamiki ST i statyki ST. Modelowanie architektury systemu. Testowanie oprogramowania. Modelowanie ograniczeń. Środowisko projektu. Struktura zespołu projektowego. Metodyka zarządzania projektem. Obszar projektu. Etapy i zadania. Zarządzanie zakresem projektu. Wymagania na system. Przegląd projektu. Modelowanie kandydatów na usługi i ekspozycja usług. Specyfikacja i implementacja usług w architekturze SOA. Zapewnianie jakości i zarządzanie ryzykiem w projektach IT. Metryki projektu. Implementacja i testowanie. Zwinne zarządzanie projektami na platformie JAZZ. Modelowanie wymagań w metodyce SCRUM. Modelowanie usług w architekturze SOA, RTC - metryki projektu, zapewnianie jakości. Końcowy przegląd projektu.	**4**	ITT	K_W04, K_W09, K_U03, K_U04, K_U10, K_K04, K_K06
DC8	***TECHNIKI DOCHODZENIOWE I ŚLEDCZE*** Treść programu ramowego: 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.	**3**	ITT	K_W03, K_W08, K_U09, K_K05, K_K06
DC9	***ZARZĄDZANIE SIECIAMI TELEINFORMATYCZNYMI*** Treść programu ramowego:	**4**	ITT	K_W03, K_W07, K_U07, K_K03, K_K06

	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, modele. Klasyfikowanie pakietów, 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, realizacja eksperymentu i interpretacja wyników. Protokół MPLS – integrowanie MPLS z systemem QoS: charakterystyka protokołu, 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.			
DC10	***STUDIUM ATAKÓW I INCYDENTÓW*** Treść programu ramowego: 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.	**3**	ITT	K_W03, K_W08, K_U09, K_K03, K_K06
DC11	***TECHNOLOGIE INTERNETU RZECZY*** Treść programu ramowego: 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). 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). 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.	**2**	ITT	K_W05, K_W07, K_U08, K_K04, K_K06
DC12	***WALKA W CYBERPRZESTRZENI*** Treść programu ramowego: 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.	**3**	ITT	K_W03, K_W08, K_U09, K_K04, K_K06
	specjalność „systemy kryptograficzne"			
DK1	***GENERACJA I TESTOWANIE LOSOWOŚCI***	**4**	ITT	K_W02, K_U02

	Treść programu ramowego: Pojęcie losowości. Test statystyczny, procedura testowa. Klasyfikacja i przegląd testów statystycznych. Testowanie generatora; wybrane testy. Generatory losowe oparte na zjawiskach fizycznych. Implementacje sprzętowe generatorów losowych.			
DK2	***TEORIA CIAŁ SKOŃCZONYCH*** Treść programu ramowego: 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.	**3**	M	K_W02, K_U02
DK3	***PROJEKTOWANIE KRYPTOGRAFICZNYCH UKŁADÓW CYFROWYCH II*** Treść programu ramowego: Wiadomości wstępne, historia rozwoju i normalizacji języków opisu sprzętu. Podstawy opisu układów cyfrowych w języku VHDL; zapoznanie ze środowiskiem programowania. Implementacja prostych układów kombinacyjnych w języku VHDL. Testowanie implementacji sprzętowej. 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.	**5**	ITT	K_W03, K_W04, K_W08, K_U09, K_U11, K_U14, K_K01
DK4	***AKREDYTACJA SYSTEMÓW TELEINFORMATYCZNYCH*** Treść programu ramowego: 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.	**5**	ITT	K_W03, K_W07, K_U07, K_U14, K_K01 K_K03, K_K06
DK5	***ATAKI ALGEBRAICZNE*** Treść programu ramowego: Metody rozwiązywania układów równań liniowych. Metody rozwiązywania układów równań nieliniowych. Atak kostek. Odporność algebraiczna funkcji boolowskich. Zastosowanie metod optymalizacji. SAT Solvers i ich zastosowania.	**3**	ITT	K_W02, K_U02, K_U09
DK6	***QUANTUM AND POST-QUANTUM CRYPTOLOGY (w języku angielskim)*** Treść programu ramowego: Przedmiot służy do poznania i zrozumienia przez studentów zagadnień związanych z obliczeniami kwantowymi i ich wpływie na klasyczną kryptologię oraz poznania podstawowych elementów tzw. kryptologii postkwantowej.	**4**	ITT	K_W03, K_W04, K_W08, K_U09, K_U14, K_K01

DK7	***KRYPTOANALIZA ALGORYTMÓW BLOKOWYCH*** Treść programu ramowego: Przedmiot służy do poznania i zrozumienia przez studentów podstawowych metod kryptoanalizy szyfrów blokowych, ich stosowalności i złożoności. Podstawy kryptoanalizy algorytmów blokowych. Podstawy kryptoanalizy różnicowej. Pojęcie charakterystyki. Złożoność czasowa i pamięciowa ataku. Kryptoanaliza różnicowa algorytmu DES. Kryptoanaliza liniowa. Techniki kryptoanalizy różnicowej. Połączenie kryptoanalizy różnicowej i liniowej. Najnowsze ataki.	**3**	ITT	K_W03, K_W04, K_W08, K_U09, K_U14, K_K01
DK8	***KRYPTOANALIZA ALGORYTMÓW STRUMIENIOWYCH*** Treść programu ramowego: 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.	**3**	ITT	K_W03, K_W04, K_W08, K_U09, K_U14, K_K01
DK9	***KRZYWE HIPERELIPTYCZNE W KRYPTOLOGII*** Treść programu ramowego: 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.	**3**	ITT	K_W02, K_W12, K_U02, K_U15
DK10	***ELEMENTS OF PUBLIC-KEY CRYPTOLOGY*** ***(w języku angielskim)*** Treść programu ramowego: The course is dedicated to foreign participants and will be realised in English. It shall pro-vide 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.	**3**	ITT	K_W02, K_U09, K_U13
DK14	***PROJEKT Z ZAKRESU MATEMATYCZNYCH I INFORMATYCZNYCH PODSTAW KRYPTOLOGII*** Treść programu ramowego: 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 rozwią-zań. 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 kryptograficzne-go. Prezentacja wyników realizacji zadania z Etapu 3 i dyskusja na temat poprawności przyjętych rozwiązań. Prezentacje realizują wybrane zespoły.	**2**	ITT	K_W02, K_W03, K_W04, K_W02, K_U08, K_U09, K_U14, K_K01
	Przedmioty dyplomowania	**22**		
E1	***SEMINARIUM DYPLOMOWE*** Treść programu ramowego: Seminarium uzupełnia konsultacje studenta z promotorem podczas przygotowywania pracy dyplomowej i przygotowuje go do egzaminu dyplomowego.	**2**		K_W02, K_W03, K_W04, K_W05, K_W06, K_W07, K_W08, K_W09, K_U02, K_U05,

			ITT	K_U06, K_U07, K_U08, K_U09, K_U10, K_U11, K_U12, K_U13, K_U14, K_K01
E2	***PRACA DYPLOMOWA*** Treść programu ramowego: W ramach programu studiów II stopnia, student realizuję pracę dyplomową magisterską. Obejmuje ona 500 godzin pracy własnej studenta. Z uwagi na fakt, że moduły te realizowane są bez bezpośrednich kontaktów z prowadzącym (wykładowcą), nie wlicza się tych godzin do ogólnej liczby godzin studiów. Za wkład do przedsięwzięcia magisterskiego, wysiłek włożony w redakcję pracy dyplomowej oraz przygotowanie do egzaminów dyplomowych student otrzymuje 20 punktów ECTS.	**20**	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
	Razem (dla każdej specjalności)	**90**		

WERYFIKACJA I OCENA EFEKTÓW UCZENIA SIĘ

Sposoby weryfikacji i oceny efektów uczenia się[3] osiągniętych przez studenta w trakcie całego cyklu kształcenia

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 pierwszych zajęciach w ramach poszczególnych modułów kształcenia prowadzący zajęcia informują studentów o zakładanych przedmiotowych efektach uczenia się o formach i sposobach ich weryfikacji. Sposoby weryfikacji zakładanych efektów uczenia się zależą przede wszystkim od rodzaju zajęć. Szczegółowe zasady określone są w sylabusach poszczególnych modułów kształcenia. Uogólniając, można jednakże wskazać wiele powtarzalnych zasad oceniania i weryfikacji. Każdy moduł kształcenia kierunkowego zaliczany jest na podstawie egzaminu lub zaliczenia na ocenę. Egzamin może mieć formę 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

[3] *opis ogólny - szczegóły w kartach informacyjnych przedmiotów udostępnianych studentom 2 tygodnie przed rozpoczęciem semestru*

studentów ze schematami rozwiązywania problemów na przykładach, samodzielna praca studentów nadzorowana przez prowadzącego, praca własna.
Sylabusy do modułów 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 przedmiotowych i (przed)dyplomowych.

Innym sposobem sprawdzenia zakładanych efektów uczenia się kierunkowego jest praktyka zawodowa – dotyczy to przede wszystkim umiejętności wykorzystania wiedzy teoretycznej w praktyce oraz współdziałania w zespole.

Część efektów uczenia się objętych programem studiów może być uzyskana w ramach zajęć prowadzonych z wykorzystaniem metod i technik kształcenia na odległość przy wykorzystaniu infrastruktury i oprogramowania zapewniających synchroniczną i asynchroniczną interakcję między studentami i osobami prowadzącymi zajęcia.

PLANY STUDIÓW

Plany studiów:

1. Plan studiów stacjonarnych II stopnia dla specjalności *Systemy kryptograficzne* – Załącznik nr 7a
2. Plan studiów stacjonarnych II stopnia dla specjalności *Cyberobrona* – Załącznik nr 7b
3. Plan studiów stacjonarnych II stopnia dla specjalności *Bezpieczeństwo informacyjne* – Załącznik nr 7c
4. Plan studiów stacjonarnych II stopnia dla specjalności *Bezpieczeństwo systemów informatycznych* – Załącznik nr 7d

Wojskowa Akademia Techniczna

PLAN STACJONARNYCH STUDIÓW DRUGIEGO STOPNIA "MAGISTERSKICH" O PROFILU OGÓLNOAKADEMICKIM

DYSCYPLINA NAUKOWA: INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA

KIERUNEK STUDIÓW: KRYPTOLOGIA I CYBERBEZPIECZEŃSTWO

Specjalność profilowana przedmiotami wybieralnymi: Systemy kryptograficzne

Załącznik nr 7a

początek 2023 rok

	GRUPY ZAJĘĆ / PRZDMIOTY	ogółem godzin/ pkt ECTS		w tym godzin:					liczba godzin/rygor/pkt ECTS w semestrze: I						jednostka organizacyjna administrująca odpowiedzialna za przedmiot	Uwagi
									I		II		III			
		l. godz	ECTS	wykł.	ćwicz.	lab.	projekt	semin.	godz.	ECTS	godz.	ECTS	godz.	ECTS		
	A. Grupa treści kształcenia ogólnego	34	2,0	4	30				34	2,0						
1	Bezpieczeństwo i higiena pracy	4		4					4 +						ZBHP	(*)
2	Język obcy	30	2,0		30 +				30 +	2					SJO	(*)
	B. Grupa treści kształcenia podstawowego	90	8,0	58	32				90	8,0						
1	Nowoczesne metody i techniki zarządzania	20	2,0	14	6				20 +	2					WBL/IOZ	(*)
2	Procesy stochastyczne	30	3,0	16	14 +				30 +	3					WCY/IMK	(*)
3	Ekonomia	20	2,0	14	6				20 +	2					WBL/IOZ	(*)
4	Socjologia	20	1,0	14	6				20 +	1					WBL/IOZ	(*)
	C. Grupa treści kształcenia kierunkowego	204	20,0	90,0		92	22		204	20,0						
1	Bezpieczeństwo baz danych	30	3,0	14		16 +			30 +	3					WCY/ISI	(*)
2	Steganografia	30	3,0	16		14 +			30 +	3					WCY/IMK	(*)
3	Diagnostyka i tolerowanie uszkodzeń	40	4,0	16		10 +	14 +		40 x	4					WCY/ITC	(*)
4	Wirtualizacja systemów IT	30	2,0	10		12 +	8 +		30 +	2					WCY-ITC	(*)
5	Techniki algorytmiczne	30	3,0	14		16			30 +	3					WCY-ISI	(*)
6	Metody numeryczne w kryptologii	44	5,0	20		24 +			44 x	5					WCY-IMK	(*)
	D. Grupa treści wybieralnych	432	38,0	210,0	38	146	38				328	30,0	104	8,0		
1	Generacja i testowanie losowosci	44	4	20	10 +	14 +					44 x	4			WCY-IMK	(*)
2	Teoria ciał skończonych	30	3	20	10 +						30 +	3			WCY-IMK	(*)
3	Projektowanie kryptograficznych układow cyfrowych II	60	5	24		36 +					60 x	5			WCY-IMK	(*)
4	Akredytacja systemów teleinformatycznych	60	5	20		40 +					60 x	5			WCY-IMK	(*)
5	Ataki algebraiczne	30	3	20		10 +					30 +	3			WCY-IMK	(*)
6	Quantum and Post-Quantum Cryptology	44	4	30	14 +						44 x	4			WCY-IMK	(*)
7	Kryptoanaliza algorytmów blokowych	30	3	20	4 +	6 +					30 +	3			WCY-IMK	(*)
8	Kryptoanaliza algorytmów strumieniowych	44	3	24		20 +							44 +	3	WCY-IMK	(*)
9	Krzywe hipereliptyczne w kryptologii	30	3	10		10 +	10 +				30 +	3			WCY-IMK	(*)
10	Elements of Public-Key Cryptology	30	3	20		10 +							30 x	3	WCY-IMK	(*)
11	Projekt z zakresu matematycznych i informatycznych podstaw kry	30	2	2			28 +						30 +	2	WCY-IMK	(*)
	E. Praca dyplomowa	44	22,0					44					44	22		
1	Seminarium dyplomowe	44	2					44					44 +	2	WCY	(*)
2	Praca dyplomowa		20										x	20	WCY	(*)
	OGÓŁEM GODZIN/pkt. ECTS	804	90	362	100	238	60	44	328	30,0	328	30,0	148	30,0		
	dopuszczalny deficyt pkt. ECTS								15		15					Łącznie nie więcej niż 30
	Rodzaje i liczba rygorów w semestrze: liczba egzaminów x								2		4		2			
	liczba zaliczeń +								8		4		3			
	liczba projektów przejściowych															

(*)Możliwa realizacja oraz ocena metodami i technikami kształcenia na odległość. Informacje szczegółowe w karcie informacyjnej przedmiotu.

Wojskowa Akademia Techniczna

PLAN STACJONARNYCH STUDIÓW DRUGIEGO STOPNIA "MAGISTERSKICH" O PROFILU OGÓLNOAKADEMICKIM

DYSCYPLINA NAUKOWA: INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA

KIERUNEK STUDIÓW: KRYPTOLOGIA I CYBERBEZPIECZEŃSTWO

Specjalność profilowana przedmiotami wybieralnymi: Cyberobrona

Załącznik nr 7b

początek 2023 rok

	GRUPY ZAJĘĆ / PRZDMIOTY	ogółem godzin/ pkt ECTS		w tym godzin:					Ilozba godzin/rygor/pkt ECTS w semestrze:						jednostka organizacyjna administrująca odpowiedzialna za przedmiot	Uwagi
									I		II		III			
		l. godz	ECTS	wykł.	ćwicz.	lab.	projekt	semin.	godz.	ECTS	godz.	ECTS	godz.	ECTS		
	A.Grupa treści kształcenia ogólnego	**34**	**2,0**	**4**	**30**				**34**	**2,0**						
1	Bezpieczeństwo i higiena pracy	4		4					4 +						ZBHP	(*)
2	Język obcy	30	2,0		30 +				30 +	2					SJO	(*)
	B. Grupa treści kształcenia podstawowego	**90**	**8,0**	**58**	**32**				**90**	**8,0**						
1	Nowoczesne metody i techniki zarządzania	20	2,0	14	6				20 +	2					WBL/IOZ	(*)
2	Procesy stochastyczne	30	3,0	16	14 +				30 +	3					WCY/IMK	(*)
3	Ekonomia	20	2,0	14	6				20 +	2					WBL/IOZ	(*)
4	Socjologia	20	1,0	14	6				20 +	1					WBL/IOZ	(*)
	C. Grupa treści kształcenia kierunkowego	**204**	**20,0**	**90,0**		**92**	**22**		**204**	**20,0**						
1	Bezpieczeństwo baz danych	30	3,0	14		16 +			30 +	3					WCY/ISI	(*)
2	Steganografia	30	3,0	16		14 +			30 +	3					WCY/IMK	(*)
3	Diagnostyka i tolerowanie uszkodzeń	40	4,0	16		10 +	14 +		40 x	4					WCY/ITC	(*)
4	Wirtualizacja systemów IT	30	2,0	10		12 +	8 +		30 +	2					WCY-ITC	(*)
5	Techniki algorytmiczne	30	3,0	14		16			30 +	3					WCY-ISI	(*)
6	Metody numeryczne w kryptologii	44	5,0	20		24 +			44 x	5					WCY-IMK	(*)
	D. Grupa treści wybieralnych	**422**	**38,0**	**170**	**10**	**174**	**68**				**332**	**30,0**	**90**	**8,0**		
1	Modelowanie systemów teleinformatycznych	44	3	16		12 +	16 +				44 +	3			WCY-ITC	(*)
2	Bezpieczeństwo sieci IPv6	30	3	10		20 +					30 +	3			WCY-ITC	(*)
3	Zarządzanie bezpieczeństwem informacji	40	4	20	10 +	10 +					40 x	4			WCY-ITC	(*)
4	Trends in computer technology	30	3	20		10							30 +	3	WCY-ITC	(*)
5	Technologie mobilne	30	2	14		16 +					30 +	2			WCY-ITC	(*)
6	Projektowanie systemów bezpieczeństwa informacji	44	4	14		16 +	14 +				44 x	4			WCY-ITC	(*)
7	Analiza i projektowanie systemów teleinformatycznych	44	4	16		14 +	14 +				44 x	4			WCY-ITC	(*)
8	Techniki dochodzeniowe i śledcze	30	3	10		20 +					30 +	3			WCY-ITC	(*)
9	Zarządzanie sieciami teleinformatycznymi	40	4	10		20 +	10 +				40 x	4			WCY-ITC	(*)
10	Studium ataków i incydentów	30	3	14		16 +					30 +	3			WCY-ITC	(*)
11	Technologie Internetu Rzeczy	30	2	16			14 +						30 +	2	WCY-ITC	(*)
12	Walka w cyberprzestrzeni	30	3	10		20 +							30 x	3	WCY-ITC	(*)
	E. Praca dyplomowa	**44**	**22,0**					**44**					**44**	**22**		
1	Seminarium dyplomowe	44	2					44					44 +	2	WCY	(*)
2	Praca dyplomowa		20										x	20	WCY	(*)
	OGÓŁEM GODZIN/pkt. ECTS	**794**	**90**	**322**	**72**	**266**	**90**	**44**	**328**	**30,0**	**332**	**30,0**	**134**	**30,0**		
	dopuszczalny deficyt pkt. ECTS								**15**		**15**					**Łącznie nie więcej niż 30**
	Rodzaje i liczba rygorów w semestrze: liczba egzaminów x								2		4		2			
	liczba zaliczeń +								8		5		3			
	liczba projektów przejściowych															

(*)Możliwa realizacja oraz ocena metodami i technikami kształcenia na odległość. Informacje szczegółowe w karcie informacyjnej przedmiotu.

Wojskowa Akademia Techniczna

PLAN STACJONARNYCH STUDIÓW DRUGIEGO STOPNIA "MAGISTERSKICH" O PROFILU OGÓLNOAKADEMICKIM

DYSCYPLINA NAUKOWA: INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA

KIERUNEK STUDIÓW: KRYPTOLOGIA I CYBERBEZPIECZEŃSTWO

Specjalność profilowana przedmiotami wybieralnymi: Bezpieczeństwo informacyjne

Załącznik nr 7c

początek 2023 rok

	GRUPY ZAJĘĆ / PRZDMIOTY	ogółem godzin/ pkt ECTS		w tym godzin:					liczba godzin/rygor/pkt ECTS w semestrze:						jednostka organizacyjna administrująca odpowiedzialna za przedmiot	Uwagi
									I		II		III			
		l. godz	ECTS	wykł.	ćwicz.	lab.	projekt	semin.	godz.	ECTS	godz.	ECTS	godz.	ECTS		
	A.Grupa treści kształcenia ogólnego	**34**	**2,0**	**4**	**30**				**34**	**2,0**						
1	Bezpieczeństwo i higiena pracy	4		4					4 +						ZBHP	(*)
2	Język obcy	30	2,0		30 +				30 +	2					SJO	(*)
	B. Grupa treści kształcenia podstawowego	**90**	**8,0**	**58**	**32**				**90**	**8,0**						
1	Nowoczesne metody i techniki zarządzania	20	2,0	14	6				20 +	2					WBL/IOZ	(*)
2	Procesy stochastyczne	30	3,0	16	14 +				30 +	3					WCY/IMK	(*)
3	Ekonomia	20	2,0	14	6				20 +	2					WBL/IOZ	(*)
4	Socjologia	20	1,0	14	6				20 +	1					WBL/IOZ	(*)
	C. Grupa treści kształcenia kierunkowego	**204**	**20,0**	**90,0**		**92**	**22**		**204**	**20,0**						
1	Bezpieczeństwo baz danych	30	3,0	14		16 +			30 +	3					WCY/ISI	(*)
2	Steganografia	30	3,0	16		14 +			30 +	3					WCY/IMK	(*)
3	Diagnostyka i tolerowanie uszkodzeń	40	4,0	16		10 +	14 +		40 x	4					WCY/ITC	(*)
4	Wirtualizacja systemów IT	30	2,0	10		12 +	8 +		30 +	2					WCY-ITC	(*)
5	Techniki algorytmiczne	30	3,0	14		16			30 +	3					WCY-ISI	(*)
6	Metody numeryczne w kryptologii	44	5,0	20		24 +			44 x	5					WCY-IMK	(*)
	D. Grupa treści wybieralnych	**430**	**38,0**	**152,0**	**20,0**	**190**	**68**				**340**	**30,0**	**90**	**8,0**		
1	Bazy danych NoSQL	30	3	6		24 +					30 +	3			WCY-ISI	(*)
2	Modelowanie i analiza sieci złożonych	44	4	18	10 +	16 +					44 x	4			WCY-ISI	(*)
3	Zarządzanie projektami	30	3	14		16 +					30 +	3			WCY-ISI	(*)
4	Zaawansowane metody uczenia maszynowego	30	3	14		16 +					30 x	3			WCY-ISI	(*)
5	Bussines modeling in UML	30	3	10		20 +							30 +	3	WCY-ISI	(*)
6	Rozproszone przetwarzanie danych	44	4	16		28 +					44 x	4			WCY-ISI	(*)
7	Podstawy kryptologii współczesnej	30	3	14		16 +					30 +	3			WCY-IMK	(*)
8	Przetwarzanie języka naturalnego	44	3	18	10 +	16 +					44 +	3			WCY-ISI	(*)
9	Big data - projekt z zakresu bezpieczeństwa informacji	44	4				44 +				44 x	4			WCY-ISI	(*)
10	Zarządzanie wiedzą	44	3	12		8 +	24 +				44 +	3			WCY-ISI	(*)
11	Ilościowe metody oceny bezpieczeństwa systemów teleinformaty	30	3	14		16 +							30 x	3	WCY-ISI	(*)
12	Teoria wojny informacyjnej	30	2	16		14 +							30 +	2	WCY-ISI	(*)
	E. Praca dyplomowa	**44**	**22,0**					**44**					**44**	**22**		
1	Seminarium dyplomowe	44	2					44					44 +	2	WCY	(*)
2	Praca dyplomowa		20										x	20	WCY	(*)
	OGÓŁEM GODZIN/pkt. ECTS	**802**	**90**	**304**	**82**	**282**	**90**	**44**	**328**	**30,0**	**340**	**30,0**	**134**	**30,0**		
	dopuszczalny deficyt pkt. ECTS								15		15					Łącznie nie więcej niż 30
	Rodzaje i liczba rygorów w semestrze: liczba egzaminów x								2		4		2			
	liczba zaliczeń +								8		5		3			
	liczba projektów przejściowych															

(*)Możliwa realizacja oraz ocena metodami i technikami kształcenia na odległość. Informacje szczegółowe w karcie informacyjnej przedmiotu.

Wojskowa Akademia Techniczna

PLAN STACJONARNYCH STUDIÓW DRUGIEGO STOPNIA "MAGISTERSKICH" O PROFILU OGÓLNOAKADEMICKIM

DYSCYPLINA NAUKOWA: INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA

KIERUNEK STUDIÓW: KRYPTOLOGIA I CYBERBEZPIECZEŃSTWO

Załącznik nr 7d

Specjalność profilowana przedmiotami wybieralnymi: Bezpieczeństwo systemów informatyczny

początek 2023 rok

	GRUPY ZAJĘĆ / PRZDMIOTY	ogółem godzin/ pkt ECTS		w tym godzin:					liczba godzin/rygor/pkt ECTS w semestrze: I						jednostka organizacyjna administrująca odpowiedzialna za przedmiot	Uwagi
									I		II		III			
		l. godz	ECTS	wykł.	ćwicz.	lab.	projekt	semin.	godz.	ECTS	godz.	ECTS	godz.	ECTS		
	A.Grupa treści kształcenia ogólnego	**34**	**2,0**	**4**	**30**				**34**	**2,0**						
1	Bezpieczeństwo i higiena pracy	**4**		4					4 +						ZBHP	(*)
2	Język obcy	**30**	**2,0**		30 +				30 +	2					SJO	(*)
	B. Grupa treści kształcenia podstawowego	**90**	**8,0**	**58**	**32**				**90**	**8,0**						
1	Nowoczesne metody i techniki zarządzania	**20**	**2,0**	14	6				20 +	2					WBL/IOZ	(*)
2	Procesy stochastyczne	**30**	**3,0**	16	14 +				30 +	3					WCY/IMK	(*)
3	Ekonomia	**20**	**2,0**	14	6				20 +	2					WBL/IOZ	(*)
4	Socjologia	**20**	**1,0**	14	6				20 +	1					WBL/IOZ	(*)
	C. Grupa treści kształcenia kierunkowego	**204**	**20,0**	**90,0**		**92**	**22**		**204**	**20,0**						
1	Bezpieczeństwo baz danych	**30**	**3,0**	14		16 +			30 +	3					WCY/ISI	(*)
2	Steganografia	**30**	**3,0**	16		14 +			30 +	3					WCY/IMK	(*)
3	Diagnostyka i tolerowanie uszkodzeń	**40**	**4,0**	16		10 +	14 +		40 x	4					WCY/ITC	(*)
4	Wirtualizacja systemów IT	**30**	**2,0**	10		12 +	8 +		30 +	2					WCY-ITC	(*)
5	Techniki algorytmiczne	**30**	**3,0**	14		16			30 +	3					WCY-ISI	(*)
6	Metody numeryczne w kryptologii	**44**	**5,0**	20		24 +			44 x	5					WCY-IMK	(*)
	D. Grupa treści wybieralnych	**430**	**38,0**	**164,0**	**20**	**178**	**68**				**340**	**30,0**	**90**	**8,0**		
1	Systemy webowe	**30**	**3**	14		16 +					30 +	3			WCY-ISI	(*)
2	Modelowanie i analiza sieci złożonych	**44**	**4**	18	10 +	16 +					44 x	4			WCY-ISI	(*)
3	Zarządzanie projektami	**30**	**3**	14		16 +					30 +	3			WCY-ISI	(*)
4	Bussines modeling in UML	**30**	**3**	10		20 +							30 +	3	WCY-ISI	(*)
5	Architektura korporacyjna	**30**	**3**	14		16 +					30 +	3			WCY-ISI	(*)
6	Podstawy kryptologii współczesnej	**30**	**3**	14		16 +					30 +	3			WCY-IMK	(*)
7	Inżynieria wsteczna systemów informatycznych	**44**	**4**	20		24 +					44 x	4			WCY-ISI	(*)
8	Niezawodność i wydajność systemów informatycznych	**44**	**3**	18	10 +	16 +					44 +	3			WCY-ISI	(*)
9	Projekt z zakresu bezpieczeństwa systemów	**44**	**4**				44 +				44 +	4			WCY-ISI	(*)
10	Inżynieria wsteczna złośliwego oprogramowania	**44**	**3**	12		8 +	24 +				44 +	3			WCY-ISI	(*)
11	Ilościowe metody oceny bezpieczeństwa systemów teleinformaty	**30**	**3**	14		16 +							30 x	3	WCY-ISI	(*)
12	Teoria wojny informacyjnej	**30**	**2**	16		14 +							30 +	2	WCY-ISI	(*)
	E. Praca dyplomowa	**44**	**22,0**					**44**					**44**	**22**		
1	Seminarium dyplomowe	44	2					44					44 +	2	WCY	(*)
2	Praca dyplomowa		20										x	20	WCY	(*)
	OGÓŁEM GODZIN/pkt. ECTS	**802**	**90**	**316**	**82**	**270**	**90**	**44**	**328**	**30,0**	**340**	**30,0**	**134**	**30,0**		
	dopuszczalny deficyt pkt. ECTS								**15**		**15**					**Łącznie nie więcej niż 30**
	Rodzaje i liczba rygorów w semestrze: liczba egzaminów x								**2**		**2**		**2**			
	liczba zaliczeń +								**8**		**7**		**3**			
	liczba projektów przejściowych															

(*)Możliwa realizacja oraz ocena metodami i technikami kształcenia na odległość. Informacje szczegółowe w karcie informacyjnej przedmiotu.

Wojskowa Akademia Techniczna

Wydział Cybernetyki

Opinia
Wydziałowej Rady ds. Kształcenia
Wydziału Cybernetyki Wojskowej Akademii Technicznej

nr 31/WRdsK/2023 z dnia 19 września 2023 r.

w sprawie projektów programów studiów stacjonarnych II stopnia 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 1/WAT/2021 z dnia 21 października 2021 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 decyzjami Dziekana WCY nr 38/WCY/2020 z dnia 20 listopada 2020 r., 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 2023/2024:

- projekty programów studiów stacjonarnych II stopnia na kierunkach:
  a) *informatyka* – stanowiący załącznik nr 1 do opinii,
  b) *kryptologia i cyberbezpieczeństwo* – stanowiący załącznik nr 2 do opinii.

PRZEWODNICZĄCY
Wydziałowej Rady ds. kształcenia
dr inż. Dariusz PIERZCHAŁA

Wojskowa Akademia Techniczna

Samorząd Studencki

Egz. nr 2

UCHWAŁA
Rady Samorządu Wydziału Cybernetyki
Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego

nr 02/RSWCY/2023 z dnia 18 września 2023 r.

w sprawie zaopiniowania programów studiów

Na podstawie § 41 Regulaminu Samorządu Studenckiego WAT, stanowiącego załącznik do uchwały Parlamentu SS WAT Nr 14/PAR/2019 z dnia 16 listopada 2019 r. (t.j. obwieszczenie Przewodniczącej SS WAT nr 1/PSS/2023 z 23 stycznia 2023 r.), uchwala się, co następuje:

§ 1

Pozytywnie opiniuje się program stacjonarnych studiów drugiego stopnia na kierunku Informatyka oraz program stacjonarnych studiów drugiego stopnia na kierunku Kryptologia i Cyberbezpieczeństwo.

§ 2

Uchwała wchodzi w życie z dniem podpisania.

Przewodniczący Rady Samorządu WCY

Piotr Gdula

Piotr Gdula

Wykonano w 2 egz.:
1) a/a
2) Prodziekan ds. kształcenia i rozwoju WCY,

Sporządził: Piotr Gdula, ☎ tel. 797-375-316, e-mail: piotr.gdula@student.wat.edu.pl