

WOJSKOWA AKADEMIA TECHNICZNA
im. Jarosława Dąbrowskiego

PROGRAM STUDIÓW

Poziom studiów: studia drugiego stopnia

Kierunek studiów: „kryptologia i cyberbezpieczeństwo” (stacjonarne)

*Uchwała Senatu Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego
nr 35/WAT/2021 z dnia 27 maja 2021r. w sprawie ustalenia programu studiów
„kryptologia i cyberbezpieczeństwo” – profil ogólnoakademicki*

Obowiązuje od roku akademickiego 2021/2022

Spis treści

1. ZAŁOŻENIA ORGANIZACYJNE	3
2. EFEKTY UCZENIA SIĘ	4
3. GRUPY PRZEDMIOTÓW I ICH OPIS.....	7
4. WERYFIKACJA I OCENA EFEKTÓW UCZENIA SIĘ	21
5. PLANY STUDIÓW	22

1. ZAŁOŻENIA ORGANIZACYJNE

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 inżynierjno-techniczne

Dyscyplina naukowa informatyka techniczna i telekomunikacja

Język studiów polski

Liczba semestrów trzy

Łączna liczba godzin

<i>W programie specjalności profilowanej przedmiotami wybieralnymi</i>	<i>Łączna liczba godzin</i>
bezpieczeństwo informacyjne	860
cyberobrona	834
systemy kryptograficzne	866
bezpieczeństwo systemów informatycznych	816

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**

<i>W programie specjalności profilowanej przedmiotami wybieralnymi</i>	<i>Liczba punktów ECTS</i>
bezpieczeństwo informacyjne	47
cyberobrona	46,5
systemy kryptograficzne	47
bezpieczeństwo systemów informatycznych	45

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

2. EFEKTY 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 inżynierskich¹

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** - Inż²_P7S_WG - kod składnika opisu charakterystyk drugiego stopnia dla kwalifikacji na poziomie 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 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
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 zidentyfikować 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 prostych 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 sieciami 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 multimedialnych 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 porozumiewanie 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	P7S_KO
K_K06	jest gotów do odpowiedzialnego pełnienia ról zawodowych z uwzględnieniem zmieniających się potrzeb społecznych, w tym: <ul style="list-style-type: none"> – rozwijania dorobku zawodu, – podtrzymywania etosu zawodu, – przestrzegania i rozwijania zasad etyki zawodowej oraz działania na rzecz przestrzegania tych zasad 	P7S_KR

3. GRUPY PRZEDMIOTÓW I ICH OPIS

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 dyscypliny	odniesienie do efektów kierunkowych
	A. Grupa treści kształcenia ogólnego	0		
A1	BEZPIECZEŃSTWO I HIGIENA PRACY <u>Treść programu ramowego:</u> 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 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.	0		K_W10
	B. Grupa treści kształcenia podstawowego	7		
B1	NOWOCZESNE METODY I TECHNIKI ZARZĄDZANIA <u>Treść programu ramowego:</u> System zarządzania organizacją. Ewolucja teorii i praktyki zarządzania. Uwarunkowania i wyzwania współczesnego zarządzania. Konceptcje zorientowane na klienta. Nowoczesny marketing. Zarządzanie 2.0: nowe paradygmaty. Orientacja organizacji na jakość. Konceptcje zarządzania jakością: TQM, ISO 9000, Six Sigma. System zrównoważonego zarządzania. Orientacje organizacji na innowacje i know-how. Zasady i błędy w przekształcania organizacji. Konceptcje optymalizujące działanie organizacji. Konceptcje zorientowane na wiedzę, człowieka i podejście zasobowe. Konceptcje organizacji uczącej się i inteligentnej. Kapitał niematerialny wybranych przedsiębiorstw – analiza porównawcza. Konceptcje 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 <u>Treść programu ramowego:</u> Ciągi losowe. Klasyfikacja i parametry procesów stochastycznych. Przykłady procesów. Łańcuchy Markowa. Procesy Markowa. Klasyfikacja stanów. Ergodyczność. Procesy zliczające. Proces urodzeń i śmierci. Systemy kolejkowe	2	M	K_W02, K_W05, K_U02, K_U14
B3	EKONOMIA <u>Treść programu ramowego:</u> 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 <u>Treść programu ramowego:</u> Zapoznanie z podstawowymi pojęciami, koncepcjami i zastosowaniami socjologii w nauce i praktyce życia społecznego.	1	NS	K_W01, K_U01, K_U14, K_K02,

	<p>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. Zbiorowości i wartości wspólnotowe (wspólno-grupowe). Wewnętrzna organizacja grupy. Relacje międzyludzkie (inscenizacja interakcji). Socjalizacja, stratyfikacja społeczna.</p>			K_K03, K_K04, K_K06
	C. Grupa treści kształcenia kierunkowego	14		
C1	<p><i>STEGANOGRAFIA</i> <u>Treść programu ramowego:</u> 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.</p>	3	ITT	K_W03, K_W04, K_W08, K_U09, K_U14, K_K01
C2	<p><i>DIAGNOSTYKA I TOLEROWANIE USZKODZEŃ</i> <u>Treść programu ramowego:</u> 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, magistrała diagnostyczna, standard IEEE 1149.x. Układy samosprawdzalne, samostępujące (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 niezdalnych 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 Lamport'a, 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: tolerowanie uszkodzeń w układach szyfratorów, detekcja ataków typu "fault injection", środki zapobiegania atakom.</p>	3	ITT	K_W06, K_U02, K_U06, K_K01, K_K05, K_K06

C3	<i>METODY I TECHNIKI SYMLACJI KOMPUTEROWEJ</i> <u>Treść programu ramowego:</u> Praktyczne wprowadzenie w metody dyskretne i quasiciągłe oraz techniki krokowe i zdarzeniowe symulacji komputerowej. Konstruowanie programowych mechanizmów symulacji dyskretnej w wybranych językach wysokiego poziomu. Algorytmy wpływu czasu i metody sterowania przebiegiem rozproszonego eksperymentu symulacyjnego. Wybrane standardy rozproszonej symulacji komputerowej (HLA, DIS).	4	ITT	K_W02, K_W05, K_U02, K_U05, K_U11, K_K01
C4	<i>BEZPIECZEŃSTWO BAZ DANYCH</i> <u>Treść programu ramowego:</u> 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.	4	ITT	K_W06, K_W08, K_U05, K_U06, K_U07, K_U11
D. Grupa treści kształcenia specjalistycznego – wybieralnego		46		
specjalność „bezpieczeństwo informacyjne”				
DB1	<i>PODSTAWY KRYPTOLOGII WSPÓŁCZESNEJ</i> <u>Treść programu ramowego:</u> 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.	4	ITT	K_W03, K_W04, K_W08, K_W09, K_W12, K_U03, K_U10, K_U12, K_U15
DB2	<i>BAZY DANYCH NOSQL</i> <u>Treść programu ramowego:</u> 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
DB3	<i>MODELOWANIE I ANALIZA SIECI ZŁOŻONYCH</i> <u>Treść programu ramowego:</u> 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
DB4	<i>IŁOŚCIOWE METODY OCENY BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH</i> <u>Treść programu ramowego:</u> 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.	4	ITT	K_W02, K_W05, K_W08, K_U02, K_U05, K_U09, K_U14, K_K01
DB5	<i>ROZPROSZONE PRZETWARZANIE DANYCH</i> <u>Treść programu ramowego:</u> Zasady dostępu i korzystania z rozproszonych baz danych, realizacja transakcji w rozproszonych bazach danych, zapytania do	4	ITT	K_W03, K_W04, K_W09, K_U03, K_U04

	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.			
DB6	ZARZĄDZANIE PROJEKTAMI <u>Treść programu ramowego:</u> 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
DB7	TECHNIKI ALGORYTMICZNE <u>Treść programu ramowego:</u> 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
DB8	ZAAWANSOWANE METODY UCZENIA MASZYNOWEGO <u>Treść programu ramowego:</u> 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
DB9	TEORIA WOJNY INFORMACYJNEJ <u>Treść programu ramowego:</u> 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
DB10	TECHNOLOGIE INTERNETU RZECZY <u>Treść programu ramowego:</u> Wprowadzenie w terminologię i główne definicje Internetu rzeczy (przedmiotów), główne założenia i perspektywy. Platformy dla urządzeń Internetu rzeczy, z wyszczególnieniem ich architektury z wyróżnieniem warstwy fizycznej i logicznej. Konwencjonalne i odnawialne źródła energii dla urządzeń o ograniczonych zasobach.	3	ITT	K_W03, K_W04, K_W09, K_U03, K_U04

	Systemy operacyjne dla urządzeń o ograniczonych zasobach. Technologie warstwy łącza danych dla IRze-IoT z uwzględnieniem technologii komunikacji bezprzewodowej i przewodowej, sieci Manet. Specyfika warstwy sieciowa dla IRze-IoT. Protokoły komunikacyjne dla IRze-IoT: protokoły SOA zorientowane na usługi (COAP), protokoły komunikacyjne oparte na wymianie komunikatów (MQTT), protokoły identyfikacji, wykrywania i rozpoznawania usług. Technologie i algorytmy wykorzystywane w przetwarzaniu danych dla IRze-IoT: organizacja przetwarzania danych dla Internetu rzeczy, idea i środowiska cloud computing. Aplikacje – Internet of Military Things, idea zastosowania IRze-IoT w działaniach militarnych i zarządzaniu kryzysowym. Idea i koncepcje Smart City oraz Smart Grid. Smart Home, Home Automation, Automatyka domowa. Automatyka samochodowa i odbiór danych z sensorów i systemów pokładowych pojazdów (monitoring systemów uzbrojenia).			
DB11	<i>PRZETWARZANIE JĘZYKA NATURALNEGO</i> <u>Treść programu ramowego:</u> 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.	4	ITT	K_W03, K_W04, K_W09, K_U03, K_U04
DB12	<i>BIG DATA – PROJEKT Z ZAKRESU BEZPIECZEŃSTWA INFORMACJI</i> <u>Treść programu ramowego:</u> 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 zadania 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
DB13	<i>BUSSINES MODELING IN UML (w języku angielskim)</i> <u>Treść programu ramowego:</u> 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.	2	ITT	K_W09, K_U10, K_U13
DB14	<i>ZARZĄDZANIE WIEDZĄ</i> <u>Treść programu ramowego:</u> 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	3	ITT	K_W03, K_W04, K_W05, K_U03, K_U10

	wnioskowania. Ontologie a bazy danych. Systemy rekomendacji. Semantyczne wyszukiwanie informacji. Wprowadzenie do analizy źródeł tekstowych. Kontrolowany język naturalny (idea i zastosowania, algorytmy).			
specjalność „bezpieczeństwo systemów informatycznych				
DS1	<i>PODSTAWY KRYPTOLOGII WSPÓŁCZESNEJ</i> <u>Treść programu ramowego:</u> 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.	4	ITT	K_W03, K_W04, K_W08, K_W09, K_W12, K_U03, K_U10, K_U12, K_U15
DS2	<i>SYSTEMY WEBOWE</i> <u>Treść programu ramowego:</u> 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.	3	ITT	K_W03, K_W08, K_U05, K_U09
DS3	<i>MODELOWANIE I ANALIZA SIECI ZŁOŻONYCH</i> <u>Treść programu ramowego:</u> 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.	5	ITT	K_W02, K_W04, K_W05, K_U02, K_U05, K_U14
DS4	<i>IŁOŚCIOWE METODY OCENY BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH</i> <u>Treść programu ramowego:</u> 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.	4	ITT	K_W02, K_W05, K_W08, K_U02, K_U05, K_U09, K_U14, K_K01
DS5	<i>ARCHITEKTURA KORPORACYJNA</i> <u>Treść programu ramowego:</u> 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	<i>ZARZĄDZANIE PROJEKTAMI</i> <u>Treść programu ramowego:</u> 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	4	ITT	K_W03, K_W04, K_U03, K_U04, K_K01, K_KK06

	metodyki prince2. Analiza jakościowa projektu. Tendencje rozwojowe zarządzania projektami.			
DS7	<p><i>TECHNIKI ALGORYTMICZNE</i></p> <p><u>Treść programu ramowego:</u> 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.</p>	4	ITT	K_W03, K_W04, K_W09, K_U03, K_U04
DS8	<p><i>TEORIA WOJNY INFORMACYJNEJ</i></p> <p><u>Treść programu ramowego:</u> 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.</p>	2	ITT	K_W01, K_W02, K_W04, K_W05, K_U01, K_U02, K_U05, K_U14
DS9	<p><i>INŻYNIERIA WSTECZNA SYSTEMÓW INFORMATYCZNYCH</i></p> <p><u>Treść programu ramowego:</u> 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.</p>	4	ITT	K_W03, K_W08, K_U05, K_U09
DS10	<p><i>NIEZAWODNOŚĆ I WYDAJNOŚĆ SYSTEMÓW INFORMATYCZNYCH</i></p> <p><u>Treść programu ramowego:</u> Modele niezawodnościowe systemów komputerowych. Modele niezawodnościowe oprogramowania. Model niezawodnościowe systemów informatycznych. Zastosowanie systemów kolejkowych do oceny wydajności systemów informatycznych.</p>	4	ITT	K_W02, K_W05, K_U02, K_U5, K_U14
DS11	<p><i>PROJEKT Z ZAKRESU BEZPIECZEŃSTWA SYSTEMÓW</i></p> <p><u>Treść programu ramowego:</u> 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.</p>	4	ITT	K_W06, K_W09, K_W11, K_U03, K_U04, K_U05, K_U06, K_U12, K_K02, K_K03
DS12	<p><i>BUSSINES MODELING IN UML (w języku angielskim)</i></p> <p><u>Treść programu ramowego:</u> 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</p>	2	ITT	K_W09, K_U10, K_U13, K_U13

	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.			
DS13	<i>INŻYNIERIA WSTECZNA ZŁOŚLIWEGO OPROGRAMOWANIA</i> <u>Treść programu ramowego:</u> 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, dekompiletory, deobfuskatory. Badanie zachowania się i komunikacji. Analiza dynamiczna. Usługi internetowe badania kodu wykonywalnego.	3	ITT	K_W03, K_W08, K_U05, K_U09
specjalność „cyberobrona”				
DC1	<i>MODELOWANIE SYSTEMÓW TELEINFORMATYCZNYCH</i> <u>Treść programu ramowego:</u> Tematyka wykładów: Inżynieria oparta na modelach, formalna weryfikacja. Podstawy modelowania ST w języku UML. Modelowanie wymagań na system teleinformatyczny. Modelowanie architektury i zachowania ST. Diagramy interakcji, diagram maszyny stanów. Rozszerzenia języka UML do modelowania protokołów, aplikacji i usług sieciowych. Modelowanie protokołów: diagramy przepływu wywołań, przekształcanie diagramów wywołań do diagramu maszyny stanów. Podstawy weryfikacji systemu teleinformatycznego w oparciu o modele formalne: weryfikacja modelu, modele systemów równoległych, 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 uwarunkowanych 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. Modelowanie systemów równoległych z wykorzystaniem kolorowanych sieci Petriego. Modelowanie ST uwarunkowanych czasowo z wykorzystaniem czasowych sieci Petriego. Modelowanie i weryfikacja ST uwarunkowanych czasowo z wykorzystaniem automatów czasowych. Tematyka zajęć projektowych: Wydanie i omówienie zadań projektowych z zakresu modelowania ST. Realizacja zadań projektowych według indywidualnego planu. Prezentacja rozwiązań i rozliczenie projektów.	3	ITT	K_W04, K_W05, K_U03, K_K04, K_K05, K_K06

DC2	<p><i>BEZPIECZEŃSTWO SIECI IPv6</i></p> <p><u>Treść programu ramowego:</u> 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.</p>	4	ITT	K_W07, K_W08, K_U09, K_K03, K_K06
DC3	<p><i>SYSTEMY ROZPROSZONE</i></p> <p><u>Treść programu ramowego:</u> 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.</p>	3	ITT	K_W04, K_U11, K_K05, K_K06
DC4	<p><i>ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI</i></p> <p><u>Treść programu ramowego:</u> Wprowadzenie do bezpieczeństwa informacyjnego – Podstawowe Twierdzenie Bezpieczeństwa. Modele formalne: Belli-LaPaduli, Biby. Modele 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.</p>	4	ITT	K_W03, K_W08, K_U10
DC5	<p><i>TRENDS IN COMPUTER TECHNOLOGY</i> <i>(w języku angielskim)</i></p> <p><u>Treść programu ramowego:</u> 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.</p>	2	ITT	K_W03, K_U08, K_K01, K_K06, K_U13
DC6	<p><i>ERGONOMIA SYSTEMÓW INTERAKTYWNYCH</i></p> <p><u>Treść programu ramowego:</u> Zasady projektowania i oceny dialogu poprzez terminale obrazowania. Metody i techniki realizacji dialogu człowiek-komputer. Model działania użytkownika w systemie interaktywnym. Charakterystyki jakości działania użytkownika w systemie interaktywnym. Testy oceny jakości działania użytkownika. Standard ISO-9241. Graficzny interfejs użytkownika w systemach interaktywnych. Zasady obrazowej prezentacji informacji w dialogu użytkownika. Zasady projektowania interakcji w interfejsie użytkownika. Projektowanie graficznego interfejsu użytkownika w systemie interaktywnym.</p>	2	ITT	K_W02, K_W04, K_U02, K_U12

DC7	<i>TECHNOLOGIE MOBILNE</i> <u>Treść programu ramowego:</u> 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
DC8	<i>PROJEKTOWANIE SYSTEMÓW BEZPIECZEŃSTWA INFORMACJI</i> <u>Treść programu ramowego:</u> 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
DC9	<i>ANALIZA I PROJEKTOWANIE SYSTEMÓW TELEINFORMATYCZNYCH</i> <u>Treść programu ramowego:</u> Paradygmaty modelowania systemów informatycznych (ST). Cykle życiowe; przegląd i klasyfikacja metodyk zarządzania 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
DC10	<i>WIRTUALIZACJA SYSTEMÓW IT</i> <u>Treść programu ramowego:</u> 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.	2	ITT	K_W05, K_U08, K_K01, K_K06
DC11	<i>TECHNIKI DOCHODZENIOWE I ŚLEDZCZE</i> <u>Treść programu ramowego:</u> 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
DC12	<i>ZARZĄDZANIE SIECIAMI TELEINFORMATYCZNYMI</i> <u>Treść programu ramowego:</u> Wprowadzenie do administrowania siecią: monitorowanie ruchu sieciowego w sieci przełączników warstwy II, protokół SNMP a monitorowanie urządzeń sieciowych, protokół NetFlow – zasady	4	ITT	K_W03, K_W07, K_U07, K_K03, K_K06

	<p>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.</p> <p>Sieci prywatne VPN.</p>			
DC13	<p><i>TECHNOLOGIE INTERNETU RZECZY</i> <u>Treść programu ramowego:</u> 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.</p>	3	ITT	K_W05, K_W07, K_U08, K_K04, K_K06
DC14	<p><i>STUDIUM ATAKÓW I INCYDENTÓW</i> <u>Treść programu ramowego:</u> Przegląd: słabości zasobów teleinformatycznych i sposoby ich wykorzystywania; typowe techniki ataków; metody 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.</p>	3	ITT	K_W03, K_W08, K_U09, K_K03, K_K06
DC15	<p><i>WALKA W CYBERPRZESTRZENI</i> <u>Treść programu ramowego:</u> 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. Cyberoddziaływanie skombinowane w działaniach w innych domenach. Zapewnianie cyberbezpieczeństwa: rozpoznawanie oszustw, ochrona zasobów informacyjnych, zapewnianie poufności i prywatności zasobów informacyjnych i komunikacji.</p>	3	ITT	K_W03, K_W08, K_U09, K_K04, K_K06
	specjalność „systemy kryptograficzne”			
DK1	<p><i>ATAKI ALGEBRAICZNE</i> <u>Treść programu ramowego:</u> Metody rozwiązywania układów równań liniowych. Metody rozwiązywania układów równań nieliniowych. Atak kostek.</p>	3	ITT	K_W02, K_U02, K_U09

	Odporność algebraiczna funkcji boolowskich. Zastosowanie metod optymalizacji. SAT Solvers i ich zastosowania.			
DK2	<i>ELEMENTY ALGEBRAICZNEJ TEORII LICZB</i> <u>Treść programu ramowego:</u> Aksjomaty teorii mnogości. Konstrukcja zbioru liczb naturalnych. Monoid liczb naturalnych. Konstrukcja zbioru liczb całkowitych i wymiernych. Własności działań w zdefiniowanych zbiorach. Pierścienie liczb całkowitych i ciało liczb wymiernych. Ciało liczb rzeczywistych. Definicje działań na liczbach. Pierścień wielomianów nad C . Zasadnicze twierdzenie algebry i wnioski z niego wynikające. Ciało algebraicznie domknięte. Ciało liczb zespolonych. Liczby algebraiczne i przestępne. Liczby algebraiczne i przestępne, ciało liczb algebraicznych. Liczby algebraiczne. Ciało liczb algebraicznych. Liczby przestępne, liczby "e" i "pi".	2	M	K_W02, K_U02
DK3	<i>GENERACJA I TESTOWANIE LOSOWOŚCI</i> <u>Treść programu ramowego:</u> 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.	3	ITT	K_W02, K_U02
DK4	<i>TEORIA CIAŁ SKOŃCZONYCH</i> <u>Treść programu ramowego:</u> 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
DK5	<i>ELEMENTS OF PUBLIC-KEY CRYPTOLOGY</i> <i>(w języku angielskim)</i> <u>Treść programu ramowego:</u> 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.	3	ITT	K_W02, K_U09, K_U13
DK6	<i>QUANTUM AND POST-QUANTUM CRYPTOLOGY</i> <i>(w języku angielskim)</i> <u>Treść programu ramowego:</u> 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	<i>KRYPTOANALIZA ALGORYTMÓW BLOKOWYCH</i> <u>Treść programu ramowego:</u> 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	<i>KRYPTOANALIZA ALGORYTMÓW STRUMIENIOWYCH</i> <u>Treść programu ramowego:</u>	3	ITT	K_W03, K_W04, K_W08, K_U09, K_U14, K_K01

	Podstawy kryptoanalizy szyfrów strumieniowych. Atak na złożoność liniową generatora. Kryptoanalityczne modele generatora klucza. Podstawy ataków korelacyjnych. Podstawowy atak korelacyjny Sigenhalera. 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.			
DK9	<i>PROJEKT Z ZAKRESU MATEMATYCZNYCH I INFORMATYCZNYCH PODSTAW KRYPTOLOGII</i> <u>Treść programu ramowego:</u> 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.	3	ITT	K_W02, K_W03, K_W04, K_W02, K_U08, K_U09, K_U14, K_K01
DK10	<i>METODY NUMERYCZNE W KRYPTOLOGII</i> <u>Treść programu ramowego:</u> Podstawowe pojęcia analizy numerycznej. Arytmetyka stałoprzecinkowa. Arytmetyka zmiennoprzecinkowa i błędy zaokrążeń 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	4	M	K_W02, K_U02
DK11	<i>CERTYFIKACJA URZĄDZEŃ KRYPTOGRAFICZNYCH</i> <u>Treść programu ramowego:</u> Ogólne zasady konstrukcji systemów kryptograficznych. Konstrukcja kryptosystemu dla wybranego systemu informacyjnego. Ogólne zasady konstrukcji urządzeń kryptograficznych. Opracowanie zasady działania przykładowego urządzenia kryptograficznego. Formalne metody weryfikacji bezpieczeństwa systemów teleinformatycznych: CommonCriteria (norma PN-ISO/IEC 15408-1).	2	ITT	K_W23, K_U11, K_U19
DK12	<i>KRZYWE HIPERELIPTYCZNE W KRYPTOLOGII</i> <u>Treść programu ramowego:</u> 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

DK13	<p>PROJEKTOWANIE KRYPTOGRAFICZNYCH UKŁADÓW CYFROWYCH II</p> <p><u>Treść programu ramowego:</u> 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 koprocatora kryptoGRAFICZNEGO dla algorytmu AES.</p>	5	ITT	K_W03, K_W04, K_W08, K_U09, K_U11, K_U14, K_K01
DK14	<p>AKREDYTACJA SYSTEMÓW TELEINFORMATYCZNYCH</p> <p><u>Treść programu ramowego:</u> 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.</p>	5	ITT	K_W03, K_W07, K_U07, K_U14, K_K01 K_K03, K_K06
	Przedmioty dyplomowania	23		
E1	<p>SEMINARIUM DYPLMOWE</p> <p><u>Treść programu ramowego:</u> Seminarium uzupełnia konsultacje studenta z promotorem podczas przygotowywania pracy dyplomowej i przygotowuje go do egzaminu dyplomowego.</p>	3	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
E2	<p>PRACA DYPLMOWA</p> <p><u>Treść programu ramowego:</u> W ramach programu studiów II stopnia, student realizują 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.</p>	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		

4. WERYFIKACJA I OCENA EFEKTÓW UCZENIA SIĘ

Sposoby weryfikacji i oceny efektów uczenia się³ 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 poprzedzone sprawdzeniem wiedzy studentów w zakresie zagadnień związanych z danym tematem. Po wykonaniu ćwiczenia studenci mogą wykonywać sprawozdania, w których muszą się wykazać umiejętność 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.

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.

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

5. PLANY STUDIÓW

Plany studiów:

1. Plan studiów stacjonarnych I stopnia dla specjalności *Systemy kryptograficzne* – Załącznik nr 1a
2. Plan studiów stacjonarnych I stopnia dla specjalności *Cyberobrona* – Załącznik nr 2a
3. Plan studiów stacjonarnych I stopnia dla specjalności *Bezpieczeństwo informacyjne* – Załącznik nr 3a
4. Plan studiów stacjonarnych I stopnia dla specjalności *Bezpieczeństwo systemów informatycznych* – Załącznik nr 4a



GRUPY ZAJĘĆ / PRZDMIOTY	Dyscyplina naukowa	ogółem godzin/ pkt ECTS		ECTS / kształt. umiejętności praktyczne	ECTS / kształt. umiejętności naukowe	ECTS udział NA	w tym godzin:					liczba godzin/rygor/pkt ECTS w semestrze:						jednostka organizacyjna administrująca odpowiedzialna za przedmiot	Uwagi
		i. godz	ECTS									I		II		III			
							wykl.	ćwicz.	lab.	projekt	semin.	godz.	ECTS	godz.	ECTS	godz.	ECTS		
A. Grupa treści kształcenia ogólnego		4					4					4							
1	Bezpieczeństwo i higiena pracy	4					4					4	+						ZBHP
B. Grupa treści kształcenia podstawowego		90	7,0	3,0	4,0	4,0	58	32				50	4,0	20	2,0	20	1,0		
1	Nowoczesne metody i techniki zarządzania	NZJ	20	2,0	1	1	14	6				20	+	2					WBL/IOZ
2	Procesy stochastyczne	M	30	2,0		2	16	14	+			30	+	2					WCY/IMK
3	Ekonomia	EF	20	2,0	1	1	14	6						20	+	2			WBL/IOZ
4	Sociologia	NS	20	1,0	1		14	6								20	+	1	WBL/IOZ
C. Grupa treści kształcenia kierunkowego		162	14,0	8,0	8,0	14,0	56	8	68	30		88	8,0	74	6,0				
1	Steganografia	ITT	30	3,0	1,0	2	3	16		14	+			30	+	3			WCY/IMK
2	Diagnostyka i tolerowanie uszkodzeń	ITT	44	3,0	1,5	2	3	16		12	+	16	+	44	x	3			WCY/ITC
3	Metody i techniki symulacji komputerowej	ITT	44	4,0	3	2	4	10		20	+	14	+	44	x	4			WCY/ISI
4	Bezpieczeństwo baz danych	ITT	44	4,0	2,5	2	4	14	8	22	+			44	+	4			WCY/ISI
D. Grupa treści wybieralnych		566	46,0	21,5	46,0	26,0	270	54	198	44		224	18,0	282	22,0	60	6,0		
1	Ataki algebraiczne	ITT	30	3	1,0	3,0	1,5	20		10	+			30	+	3			WCY-IMK
2	Elementy algebraicznej teorii liczb	M	30	2	1,0	2,0	1,5	14	16	+				30	+	2			WCY-IMK
3	Generacja i testowanie losowości	ITT	44	3	1,5	3,0	2,0	20	10	+	14	+		44	x	3			WCY-IMK
4	Teoria ciał skończonych	M	30	3	1,0	3,0	1,5	20	10	+				30	+	3			WCY-IMK
5	Elements of Public-Key Cryptology	ITT	30	3	1,0	3,0	1,5	20		10	+					30	x	3	WCY-IMK
6	Quantum and Post-Quantum Cryptology	ITT	44	4	1,0	4,0	2,0	30	14	+				44	x	4			WCY-IMK
7	Kryptoanaliza algorytmów blokowych	ITT	30	3	1,0	3,0	1,5	20	4	+	6	+		30	+	3			WCY-IMK
8	Kryptoanaliza algorytmów strumieniowych	ITT	44	3	1,0	3,0	2,0	24		20	+			44	+	3			WCY-IMK
9	Projekt z zakresu matematycznych i informatycznych podstaw kry	ITT	30	3	2,5	3,0	1,5	2			28	+				30	+	3	WCY-IMK
10	Metody numeryczne w kryptologii	M	60	4	2,0	4,0	2,5	30		30	+			60	x	4			WCY-IMK
11	Certyfikacja urządzeń kryptograficznych	ITT	30	2	1,0	2,0	1,5	10		20	+		30	+	2				WCY-IMK
12	Krzywe hipereliptyczne w kryptologii	ITT	44	3	1,5	3,0	2,0	16	12	+	16	+		44	+	3			WCY-IMK
13	Projektowanie kryptograficznych układów cyfrowych II	ITT	60	5	3,0	5,0	2,5	24		36	+		60	x	5				WCY-IMK
14	Akredytacja systemów teleinformatycznych	ITT	60	5	3,0	5,0	2,5	20		40	+		60	x	5				WCY-IMK
E. Praca dyplomowa		44	23,0	8,0	11,0	3					44					44	23		
1	Seminarium dyplomowe	ITT	44	3	2	1	1				44					44	+	3	WCY
2	Praca dyplomowa	ITT		20	6	10	2										x	20	WCY
OGÓŁEM GODZIN/pkt. ECTS		866	90	40,5	69,0	47,0	388	94	266	74	44	366	30,0	376	30,0	124	30,0		
dopuszczalny deficyt pkt. ECTS												10		10		10			
Rodzaje i liczba rygorów w semestrze:												liczba egzaminów x	4	liczba zaliczeń +	3	liczba projektów przejściowych	2		
													5		7		3		



PLAN STACJONARNYCH STUDIÓW DRUGIEGO STOPNIA "MAGISTERSKICH" O PROFILU OGÓLNOAKADEMICKIM

DYSCYPLINA NAUKOWA: INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA

KIERUNEK STUDIÓW: KRYPTOLOGIA I CYBERBEZPIECZEŃSTWO

Specjalność profilowana przedmiotami wybieranymi: Cyberbrona

początek 2021 rok

GRUPY ZAJĘĆ / PRZDMIOTY	Dyscyplina naukowa	ogółem godzin/ pkt ECTS		ECTS / kształt. umiejętności praktyczne	ECTS / kształt. umiejętności naukowe	ECTS udział NA	w tym godzin:					liczba godzin/rygor/pkt ECTS w semestrze:						jednostka organizacyjna administrująca odpowiedzialna za przedmiot	Uwagi
		i. godz	ECTS				wykl.	ćwicz.	lab.	projekt	semin.	I		II		III			
												godz.	ECTS	godz.	ECTS	godz.	ECTS		
A. Grupa treści kształcenia ogólnego		4					4					4							
1	Bezpieczeństwo i higiena pracy	4					4					4	+						ZBHP
B. Grupa treści kształcenia podstawowego		90	7,0	3,0	4,0	4,0	58	32				50	4,0	20	2,0	20	1,0		
1	Nowoczesne metody i techniki zarządzania	NZJ	20	2,0	1	1	14	6				20	+	2					WBL/IOZ
2	Procesy stochastyczne	M	30	2,0		2	16	14	+			30	+	2					WCY/IMK
3	Ekonomia	EF	20	2,0	1	1	14	6						20	+	2			WBL/IOZ
4	Socjologia	NS	20	1,0	1		14	6								20	+	1	WBL/IOZ
C. Grupa treści kształcenia kierunkowego		162	14,0	8,0	8,0	14,0	56	8	68	30		88	8,0	74	6,0				
1	Steganografia	ITT	30	3,0	1,0	2	3	16		14	+			30	+	3			WCY/IMK
2	Diagnostyka i tolerowanie uszkodzeń	ITT	44	3,0	1,5	2	3	16		12	+	16	+	44	x	3			WCY/ITC
3	Metody i techniki symulacji komputerowej	ITT	44	4,0	3	2	4	10		20	+	14	+	44	x	4			WCY/ISI
4	Bezpieczeństwo baz danych	ITT	44	4,0	2,5	2	4	14	8	22	+			44	+	4			WCY/ISI
D. Grupa treści wybieralnych		534	46,0	24,0	46,0	25,5	224	10	202	98		222	18,0	252	22,0	60	6,0		
1	Modelowanie systemów teleinformatycznych	ITT	44	3	1,5	3,0	2,0	16		12	+	16	+	44	+	3			WCY-ITC
2	Bezpieczeństwo sieci IPv6	ITT	44	4	2,5	4,0	2,0	12		20	+	12	+	44	x	4			WCY-ITC
3	Systemy rozproszone	ITT	30	3	1,0	3,0	1,5	20				10	+	30	x	3			WCY-ITC
4	Zarządzanie bezpieczeństwem informacji	ITT	44	4	1,5	4,0	2,0	24	10	+	10	+			44	x	4		WCY-ITC
5	Trends in computer technology	ITT	30	2	0,5	2,0	1,5	20		10				30	+	2			WCY-ITC
6	Ergonomia systemów interaktywnych	ITT	30	2	1,0	2,0	1,5	14		16	+			30	+	2			WCY-ITC
7	Technologie mobilne	ITT	30	2	1,0	2,0	1,5	14		16	+					30	+	2	WCY-ITC
8	Projektowanie systemów bezpieczeństwa informacji	ITT	44	4	2,5	4,0	2,0	14		16	+	14	+	44	x	4			WCY-ITC
9	Analiza i projektowanie systemów teleinformatycznych	ITT	44	4	2,5	4,0	2,0	16		14	+	14	+	44	x	4			WCY-ITC
10	Wirtualizacja systemów IT	ITT	30	2	1,0	2,0	1,5	10		12	+	8	+	30	+	2			WCY-ITC
11	Techniki dochodzeniowe i śledcze	ITT	30	3	2,0	3,0	1,5	10		20	+			30	+	3			WCY-ITC
12	Zarządzanie sieciami teleinformatycznymi	ITT	44	4	2,5	4,0	2,0	14		20	+	10	+	44	x	4			WCY-ITC
13	Technologie Internetu Rzeczy	ITT	30	3	1,0	3,0	1,5	16				14	+			30	+	3	WCY-ITC
14	Studium ataków i incydentów	ITT	30	3	1,5	3,0	1,5	14		16	+			30	+	3			WCY-ITC
15	Walka w cyberprzestrzeni	ITT	30	3	2,0	3,0	1,5	10		20	+					30	x	3	WCY-ITC
E. Praca dyplomowa		44	23,0	8,0	11,0	3					44					44	23		
1	Seminarium dyplomowe	ITT	44	3	2	1	1				44					44	+	3	WCY
2	Praca dyplomowa	ITT		20	6	10	2										x	20	WCY
OGÓŁEM GODZIN/pkt. ECTS		834	90	43,0	69,0	46,5	342	50	270	128	44	364	30,0	346	30,0	124	30,0		
dopuszczalny deficyt pkt. ECTS												10		10		10			
Rodzaje i liczba rygorów w semestrze:												liczba egzaminów x		4	4	2			
												liczba zaliczeń +		6	6	3			
												liczba projektów przejściowych							



PLAN STACJONARNYCH STUDIÓW DRUGIEGO STOPNIA "MAGISTERSKICH" O PROFILU OGÓLNOAKADEMICKIM

DYSCYPLINA NAUKOWA: INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA

KIERUNEK STUDIÓW: KRYPTOLOGIA I CYBERBEZPIECZEŃSTWO

Specjalność profilowana przedmiotami wybieranymi: Bezpieczeństwo informacyjne

początek 2021 rok

GRUPY ZAJĘĆ / PRZDMIOTY	Dyscyplina naukowa	ogółem godzin/ pkt ECTS		ECTS / kształt. umiejętności praktyczne	ECTS / kształt. umiejętności naukowe	ECTS udział NA	w tym godzin:					liczba godzin/rygor/pkt ECTS w semestrze:						jednostka organizacyjna administrująca odpowiedzialna za przedmiot	Uwagi	
		i. godz	ECTS				wykl.	ćwicz.	lab.	projekt	semin.	I		II		III				
												godz.	ECTS	godz.	ECTS	godz.	ECTS			
A. Grupa treści kształcenia ogólnego		4					4					4								
1	Bezpieczeństwo i higiena pracy	4					4					4	+						ZBHP	
B. Grupa treści kształcenia podstawowego		90	7,0	3,0	4,0	4,0	58	32				50	4,0	20	2,0	20	1,0			
1	Nowoczesne metody i techniki zarządzania	NZJ	20	2,0	1	1	14	6				20	+	2					WBL/IOZ	
2	Procesy stochastyczne	M	30	2,0		2	16	14	+			30	+	2					WCY/IMK	
3	Ekonomia	EF	20	2,0	1	1	14	6						20	+	2			WBL/IOZ	
4	Socjologia	NS	20	1,0	1		14	6								20	+	1	WBL/IOZ	
C. Grupa treści kształcenia kierunkowego		162	14,0	8,0	8,0	14,0	56	8	68	30		88	8,0	74	6,0					
1	Steganografia	ITT	30	3,0	1,0	2	3	16		14	+			30	+	3			WCY/IMK	
2	Diagnostyka i tolerowanie uszkodzeń	ITT	44	3,0	1,5	2	3	16		12	+	16	+	44	x	3			WCY/ITC	
3	Metody i techniki symulacji komputerowej	ITT	44	4,0	3	2	4	10		20	+	14	+	44	x	4			WCY/ISI	
4	Bezpieczeństwo baz danych	ITT	44	4,0	2,5	2	4	14	8	22	+			44	+	4			WCY/ISI	
D. Grupa treści wybieralnych		560	46,0	27,0	46,0	26,0	194	68	230	68		222	18,0	264	22,0	74	6,0			
1	Podstawy kryptologii współczesnej	ITT	44	4	2,5	4,0	2,0	16	12	+	16	+			44	+	4		WCY-IMK	
2	Bazy danych NoSQL	ITT	30	3	2,0	3,0	1,5	6		24	+			30	+	3			WCY-ISI	
3	Modelowanie i analiza sieci złożonych	ITT	44	4	2,0	4,0	2,0	18	10	+	16	+			44	x	4		WCY-ISI	
4	Ilościowe metody oceny bezpieczeństwa systemów teleinformatycznych	ITT	44	4	2,0	4,0	2,0	18	12	+	14	+					44	x	4	WCY-ISI
5	Rozproszone przetwarzanie danych	ITT	44	4	2,5	4,0	2,0	16		28	+			44	x	4			WCY-ISI	
6	Zarządzanie projektami	ITT	44	3	1,5	3,0	2,0	16	14	+	14	+			44	+	3		WCY-ISI	
7	Techniki algorytmiczne	ITT	44	3	2,0	3,0	2,0	14	10	20				44	3				WCY-ISI	
8	Zaawansowane metody uczenia maszynowego	ITT	30	3	1,5	3,0	1,5	14		16	+			30	x	3			WCY-ISI	
9	Teoria wojny informacyjnej	ITT	30	2	0,5	2,0	1,5	16		14	+					30	+	2	WCY-ISI	
10	Technologie internetu rzeczy	ITT	44	3	1,5	3,0	2,0	20		24	+			44	x	3			WCY-ISI	
11	Przetwarzanie języka naturalnego	ITT	44	4	2,0	4,0	2,0	18	10	+	16	+			44	+	4		WCY-ISI	
12	Big data - projekt z zakresu bezpieczeństwa informacji	ITT	44	4	4,0	4,0	2,0			44	+			44	x	4			WCY-ISI	
13	Bussines modeling in UML	ITT	30	2	1,0	2,0	1,5	10		20	+			30	+	2			WCY-ISI	
14	Zarządzanie wiedzą	ITT	44	3	2,0	3,0	2,0	12		8	+	24	+			44	+	3		WCY-ISI
E. Praca dyplomowa		44	23,0	8,0	11,0	3					44					44	23			
1	Seminarium dyplomowe	ITT	44	3	2	1	1				44					44	+	3	WCY	
2	Praca dyplomowa	ITT		20	6	10	2										x	20	WCY	
OGÓŁEM GODZIN/pkt. ECTS		860	90	46,0	69,0	47,0	312	108	298	98	44	364	30,0	358	30,0	138	30,0			
dopuszczalny deficyt pkt. ECTS												10		10		10				
Rodzaje i liczba rygorów w semestrze:												liczba egzaminów x	3	4	2					
												liczba zaliczeń +	6	5	3					
												liczba projektów przejściowych								



PLAN STACJONARNYCH STUDIÓW DRUGIEGO STOPNIA "MAGISTERSKICH" O PROFILU OGÓLNOAKADEMICKIM

DYSCYPLINA NAUKOWA: INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA

KIERUNEK STUDIÓW: KRYPTOLOGIA I CYBERBEZPIECZEŃSTWO

Specjalność profilowana przedmiotami wybieranymi: Bezpieczeństwo systemów informatycznych

GRUPY ZAJĘĆ / PRZDMIOTY	Dyscyplina naukowa	ogółem godzin/ pkt ECTS		ECTS / kształt. umiejętności praktyczne	ECTS / kształt. umiejętności naukowe	ECTS udział NA	w tym godzin:					liczba godzin/rygor/pkt ECTS w semestrze:						jednostka organizacyjna administrująca odpowiedzialna za przedmiot	Uwagi	
		i. godz	ECTS				wykl.	ćwicz.	lab.	projekt	semin.	I		II		III				
												godz.	ECTS	godz.	ECTS	godz.	ECTS			
A. Grupa treści kształcenia ogólnego		4					4					4								
1	Bezpieczeństwo i higiena pracy	4					4					4	+						ZBHP	
B. Grupa treści kształcenia podstawowego		90	7,0	3,0	4,0	4,0	58	32				50	4,0	20	2,0	20	1,0			
1	Nowoczesne metody i techniki zarządzania	NZJ	20	2,0	1	1	14	6				20	+	2					WBL/IOZ	
2	Procesy stochastyczne	M	30	2,0		2	16	14	+			30	+	2					WCY/IMK	
3	Ekonomia	EF	20	2,0	1	1	14	6						20	+	2			WBL/IOZ	
4	Socjologia	NS	20	1,0	1		14	6								20	+	1	WBL/IOZ	
C. Grupa treści kształcenia kierunkowego		162	14,0	8,0	8,0	14,0	56	8	68	30		88	8,0	74	6,0					
1	Steganografia	ITT	30	3,0	1,0	2	3	16		14	+			30	+	3			WCY/IMK	
2	Diagnostyka i tolerowanie uszkodzeń	ITT	44	3,0	1,5	2	3	16		12	+	16	+	44	x	3			WCY/ITC	
3	Metody i techniki symulacji komputerowej	ITT	44	4,0	3	2	4	10		20	+	14	+	44	x	4			WCY/ISI	
4	Bezpieczeństwo baz danych	ITT	44	4,0	2,5	2	4	14	8	22	+			44	+	4			WCY/ISI	
D. Grupa treści wybieralnych		516	46,0	27,0	46,0	24,0	186	68	194	68		192	18,0	250	22,0	74	6,0			
1	Podstawy kryptologii współczesnej	ITT	44	4	2,5	4,0	2,0	16	12	+	16	+			44	+	4		WCY-IMK	
2	Systemy webowe	ITT	30	3	1,5	3,0	1,5	14						30	+	3			WCY-ISI	
3	Modelowanie i analiza sieci złożonych	ITT	44	5	3,0	5,0	2,0	18	10	+	16	+			44	x	5		WCY-ISI	
4	Ilościowe metody oceny bezpieczeństwa systemów teleinformatycznych	ITT	44	4	2,0	4,0	2,0	18	12	+	14	+					44	x	4	WCY-ISI
5	Architektura korporacyjna	ITT	30	3	1,5	3,0	1,5	14						30	+	3			WCY-ISI	
6	Zarządzanie projektami	ITT	44	4	2,5	4,0	2,0	16	14	+	14	+			44	+	4		WCY-ISI	
7	Techniki algorytmiczne	ITT	44	4	2,5	4,0	2,0	14	10		20	+			44	+	4		WCY-ISI	
8	Teoria wojny informacyjnej	ITT	30	2	0,5	2,0	1,5	16			14	+					30	+	2	WCY-ISI
9	Inżynieria wsteczna systemów informatycznych	ITT	44	4	2,0	4,0	2,0	20			24	+			44	x	4		WCY-ISI	
10	Niezawodność i wydajność systemów informatycznych	ITT	44	4	2,0	4,0	2,0	18	10	+	16	+			44	+	4		WCY-ISI	
11	Projekt z zakresu bezpieczeństwa systemów	ITT	44	4	4,0	4,0	2,0				44	+			44	+	4		WCY-ISI	
12	Bussines modeling in UML	ITT	30	2	1,0	2,0	1,5	10			20	+			30	+	2		WCY-ISI	
13	Inżynieria wsteczna złożonego oprogramowania	ITT	44	3	2,0	3,0	2,0	12			8	+	24	+	44	+	3		WCY-ISI	
E. Praca dyplomowa		44	23,0	8,0	11,0	3					44				44	23				
1	Seminarium dyplomowe	ITT	44	3	2	1	1				44				44	+	3		WCY	
2	Praca dyplomowa	ITT		20	6	10	2									x	20		WCY	
OGÓŁEM GODZIN/pkt. ECTS		816	90	46,0	69,0	45,0	304	108	262	98	44	334	30,0	344	30,0	138	30,0			
dopuszczalny deficyt pkt. ECTS												10		10		10				
Rodzaje i liczba rygorów w semestrze:												liczba egzaminów x	2	2	2					
												liczba zaliczeń +	7	7	3					
												liczba projektów przejściowych								

Mateusz Runiewicz

Warszawa 05.05.2021 r.

mateusz.runiewicz@student.wat.edu.pl

Ul. Rajskiej Jabłoni 7

05-500 Józefosław

+48 698 115 730

OPINIA

Dotyczy Programów studiów rozpoczynających się od 2021 r.

Wydziałowa Rada Samorządu Studenckiego na posiedzeniu w dniu 05.05.2021 rozpatrzyła propozycje programów studiów rozpoczynających się od roku akademickiego 2021/2022.

Rada pozytywnie opiniuje niżej wymienione programy:

1. Program jednolitych studiów magisterskich na kierunku „Informatyka”;
2. Program jednolitych studiów magisterskich na kierunku „Kryptologia i cyberbezpieczeństwo”;
3. Program studiów I i II stopnia, studia stacjonarne i niestacjonarne, na kierunku „Informatyka”;
4. Program studiów I i II stopnia, studia stacjonarne i niestacjonarne, na kierunku „Kryptologia i cyberbezpieczeństwo”

Podpis



Przewodniczący RS WCY

Mateusz Runiewicz



Wojskowa
Akademia
Techniczna

Wydział
Cybernetyki



**Opinia
Wydziałowej Rady ds. Kształcenia
Wydziału Cybernetyki Wojskowej Akademii Technicznej**

nr 24/WRdsK/2020 z dnia 27 kwietnia 2021 r.

**w sprawie przyjęcia projektów programów studiów
I, II stopnia i jednolitych studiów magisterskich 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 (t.j. obwieszczenie Rektora WAT nr 2/WAT/2019 z dnia 9 października 2019 r.) oraz § 17 ust. 1 pkt. 1 *Regulaminu Wydziałowej Rady do spraw Kształcenia Wydziału Cybernetyki Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego* postanawia się, co następuje

§ 1

Przyjmuje się projekty niżej wymienionych programów studiów dla studiów rozpoczynających się od roku akademickiego 2021/2022:

- 1) projekty programów studiów stacjonarnych i niestacjonarnych I i II stopnia na kierunkach:
 - a) *informatyka* – stanowiące załączniki nr 1-3 do stanowiska,
 - b) *kryptologia i cyberbezpieczeństwo* – stanowiące załączniki nr 4-6 do stanowiska,
- 2) projekty programów jednolitych studiów magisterskich, dla kandydatów na żołnierzy zawodowych na kierunkach:
 - a) *informatyka* – stanowiący załącznik nr 7 do stanowiska,
 - b) *kryptologia i cyberbezpieczeństwo* – stanowiący załącznik nr 8 do stanowiska.

§ 2

Projekty programów studiów, o których mowa w § 1, zostaną przekazane dziekanowi WCY do dalszego procedowania.

PRZEWODNICZĄCY
Wydziałowej Rady ds. kształcenia


dr inż. Dariusz PIERZCHAŁA



Wojskowa
Akademia
Techniczna

**Uchwała
Rady Dyscypliny Naukowej
Informatyka Techniczna i Telekomunikacja
Wojskowej Akademii Technicznej
im. Jarosława Dąbrowskiego**

nr 38/RDN ITiT/2021 z dnia 11 maja 2021 r.

**w sprawie zaopiniowania programów studiów I, II stopnia
i jednolitych studiów magisterskich
przydzielonych do dyscypliny
Informatyka Techniczna i Telekomunikacja**

Na podstawie § 25 ust. 1 pkt 13 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 (t.j. obwieszczenie Rektora WAT nr 2/WAT/2019 z dnia 9 października 2019 r.) uchwała się, co następuje:

§ 1

Pozytywnie opiniuje się niżej wymienione programy studiów, dla studiów rozpoczynających się od roku akademickiego 2021/2022:

- 1) programy studiów stacjonarnych i niestacjonarnych I i II stopnia na kierunkach:
 - a) *informatyka* – stanowiące załączniki nr 1, 2, 3 do uchwały,
 - b) *kryptologia i cyberbezpieczeństwo* – stanowiące załączniki nr 4, 5, 6 do uchwały,
- 2) programy jednolitych studiów magisterskich, dla kandydatów na żołnierzy zawodowych na kierunkach:
 - a) *informatyka* – stanowiący załącznik nr 7 do uchwały,
 - b) *kryptologia i cyberbezpieczeństwo* – stanowiący załącznik nr 8 do uchwały.

§ 2

Uchwała wchodzi w życie z dniem podjęcia.

PRZEWODNICZĄCY
Rady Dyscypliny Naukowej
"Informatyka Techniczna i Telekomunikacja"

dr hab. inż. Zbigniew TARAPATA, prof. WAT