Załącznik nr 4
do uchwały Senatu WAT nr 32/WAT/2019
z dnia 30.05.2019 r.

WOJSKOWA AKADEMIA TECHNICZNA
im. Jarosława Dąbrowskiego

Wydział Cybernetyki
(nazwa podstawowej jednostki organizacyjnej WAT prowadzącej studia)

PROGRAM STUDIÓW

Poziom studiów: drugi

Kierunek studiów: „kryptologia i cyberbezpieczeństwo" – profil ogólnoakademicki

Uchwała Senatu Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego nr 32/WAT/2019 z dnia 30 maja 2019 r. w sprawie ustalenia programu studiów „kryptologia i cyberbezpieczeństwo" – profil ogólnoakademicki

Obowiązuje od roku akademickiego 2019/2020

Warszawa 2019

Spis treści

1. ZAŁOŻENIA ORGANIZACYJNE

Poziom studiów drugi

Profil studiów ogólnoakademicki

Formy studiów stacjonarna i niestacjonarna

Tytuł zawodowy nadawany absolwentowi magister inżynier

Poziom Polskiej Ramy Kwalifikacji siódmy (7)

Przyporządkowanie kierunku studiów:

Dziedzina nauki inżynieryjno-techniczne

dyscyplina naukowa informatyka techniczna i telekomunikacja

Język studiów polski

Liczba semestrów trzy

Liczba punktów ECTS konieczna do uzyskania kwalifikacji - 90

Łączna liczba godzin

w programie specjalności profilowanej przedmiotami wybieralnymi	*łączna liczba godzin*
bezpieczeństwo informacyjne	**830**
cyberobrona	**834**
systemy kryptograficzne	**850**

Łączna liczba punktów ECTS, którą student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia

w programie specjalności profilowanej przedmiotami wybieralnymi	*łączna liczba godzin*
bezpieczeństwo informacyjne	**60**
cyberobrona	**61**
systemy kryptograficzne	**61**

Łączna liczba punktów ECTS, którą student musi uzyskać w ramach zajęć z dziedziny nauk humanistycznych lub nauk społecznych - 5

Wymiar, liczba punktów ECTS, zasady i forma odbywania praktyk zawodowych

Na studiach drugiego stopnia na kierunku „kryptologia i cyberbezpieczeństwo” nie przewiduje się odbywania praktyk zawodowych.

2. 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,

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 i kompetencji społecznych;
  - 01, 02, 03, ... - numer efektu uczenia się;
- w kolumnie ***kod składnika opisu*** - Inż_P7S_WG - kod składnika opisu charakterystyk drugiego stopnia dla kwalifikacji na poziomie szóstym 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
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 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 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	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	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 dyscy-pliny	odniesienie do efektów kierunkowych
	A. Grupa treści kształcenia ogólnego	**0**		
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 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	**15**		
B1	***METODY I TECHNIKI SYMULACJI KOMPUTEROWEJ*** Treść programu ramowego: Wprowadzenie do modelowania symulacyjnego. Podstawowe pojęcia, klasyfikacja i założenia metod symulacji komputerowej oraz komputerowych generatorów liczb i procesów losowych. Metody i techniki symulacji dyskretnej krokowej, zdarzeniowej i zorientowanej na procesy. Wybrane języki programowania symulacji dyskretnej. Podstawy wielowątkowości i synchronizacji w języku Java / C#. Konstruowanie programowych mechanizmów symulacji dyskretnej w wybranych językach wysokiego poziomu. Wybrane standardy rozproszonej symulacji komputerowej. Algorytmy upływu czasu i metody sterowania przebiegiem rozproszonego eksperymentu symulacyjnego.	**4**	ITT	K_W02, K_W05, K_U02, K_U05, K_U14, K_K01
B2	***PROCESY STOCHASTYCZNE*** Treść programu ramowego: Ciągi losowe. Klasyfikacja i parametry procesów stochastycznych. Przykłady procesów Łańcuchy Markowa. Procesy Markowa. Ergodyczność. Procesy zliczające. Proces urodzeń i śmierci. Systemy kolejkowe	**2**	M	K_W02, K_W05, K_U02, K_U14
B3	***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.	**4**	ITT	K_W03, K_W04, K_U03, K_U04, K_U11, K_U14
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 ak-	**1**	NS	K_W01, K_U01, K_U14, K_K02, K_K03, K_K04, K_K06

	tywnego 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.			
B5	***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,
B6	***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
	C. Grupa treści kształcenia kierunkowego	**6**		
C1	***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
C2	***DIAGNOSTYKA I TOLEROWANIE USZKODZEŃ*** Treść programu ramowego: Pojęcia podstawowe z zakresu diagnostyki systemów komputerowych. Testowanie i niezawodność układów cyfrowych. Techniki testowania i diagnozowania systemów komputerowych. Testowanie i niezawodność oprogramowania. Diagnostyka systemowa, diagnostyka systemowa sieci teleinformatycznych, Diagnostyka symptomowa sieci teleinformatycznych. Wyznaczanie testów kontrolnych i lokalizacyjnych. Testowanie układów cyfrowych i podzespołów systemu komputerowego. Testowanie systemu z wykorzystaniem magistrali diagnostycznej. Badanie własności struktur opiniowania diagnostycznego i struktur porównawczych. Wyznaczanie diagnozowalności wybranych sieci procesorowych. Wyznaczanie charakterystyk bazowych sieci komputerowej.	**3**	ITT	K_W06, K_U02, K_U06, K_K01, K_K05, K_K06

	D. Grupa treści kształcenia specjalistycznego – wybieralnego	**46**		
	specjalność „bezpieczeństwo informacyjne”			
DB1	***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.	**4**	ITT	K_W03, K_W04, K_W08, K_W09, K_W12, K_U03, K_U10, K_U12, K_U15
DB2	***ZAAWANSOWANE TECHNOLOGIE USŁUGOWE I MOBILNE*** Treść programu ramowego: Zagadnienia projektowania systemów usługowych. Architektury i stosy technologiczne SOA. Zagadnienia konstrukcji architektur SOA w technologiach korporacyjnych. Praktyczne aspekty implementacji bezpiecznych systemów wykorzystujących podejście SOA. Zagadnienia projektowania oprogramowania mobilnego. Architektury systemów mobilnych. Dobre praktyki konstrukcji aplikacji mobilnych dla platformy Android i Windows Phone. Technologie międzyplatformowe wytwarzania oprogramowania mobilnego. Aspekty bezpieczeństwa platform i oprogramowania mobilnego.	**3**	ITT	K_W03, K_W04, K_U03, K_U04, K_U08, K_U14
DB3	***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.	**5**	ITT	K_W02, K_W04, K_W05, K_U02, K_U05, K_U14
DB4	***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.	**4**	ITT	K_W02, K_W05, K_W08, K_U02, K_U05, K_U09, K_U14, K_K01
DB5	***PROJEKTOWANIE BEZPIECZNYCH SYSTEMÓW*** Treść programu ramowego: Podstawowe pojęcia związane z bezpieczeństwem systemów TI. Obowiązujące normy i standardy. Proces prowadzenia projektu teleinformatycznego zorientowany na zasady wytwarzania bezpiecznych aplikacji oraz systemów teleinformatycznych uwzględniające obowiązujące normy prawne i standardy. Metodyki wytwarzania bezpiecznych systemów teleinformatycznych. Projektowanie i optymalizacja bezpiecznych baz danych. Projektowanie bezpiecznych aplikacji i systemów teleinformatycznych.	**4**	ITT	K_W03, K_W08, K_W10, K_W12, K_U03, K_U04, K_U09, K_U14, K_U15

DB6	***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.	**4**	ITT	K_W03, K_W04, K_U03, K_U04, K_K01, K_KK06
DB7	***ZAAWANSOWANE METODY EKSPLORACJI DANYCH*** Treść programu ramowego: Modele i analiza szeregów czasowych. Sieci bayesowskie. Ukryte łańcuchy Markowa. Fuzja danych. Metody Big data. Klasyfikatory złożone: bagging, boosting. Textminning. Wykorzystanie metod eksploracji danych do analizy bezpieczeństwa systemów teleinformatycznych.	**4**	ITT	K_W02, K_W05, K_U02, K_U05, K_U14
DB8	***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.	**2**	ITT	K_W01, K_W02, K_W04, K_W05, K_U01, K_U02, K_U05, K_U14
DB9	***ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI*** Treść programu ramowego: Pojęcie informacji, rola i znaczenie informacji w organizacji, piramida informacji, kryteria klasyfikacji informacji, podstawowe atrybuty bezpieczeństwa informacji, polityka bezpieczeństwa informacji, model PDCA. Normy i standardy z zakresu bezpieczeństwa informacyjnego. Zarządzanie ryzykiem na potrzeby bezpieczeństwa informacyjnego. Etapy budowy i wdrażania systemu zarządzania bezpieczeństwem informacji. Dokumentacja systemu zarządzania bezpieczeństwem informacji.	**3**	ITT	K_W08, K_W09, K_W10, K_U09, K_U10, K_U14, K_K_01, K_K06
DB10	***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.	**4**	ITT	K_W02, K_W05, K_U02, K_U5, K_U14
DB11	***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
DB12	***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 podstawo-	**2**	ITT	K_W09, K_U10, K_U13, K_U13

	wych tekstów pisemnych w zakresie: informatycznych systemów zarządzania, technik algorytmicznych, niezawodności programowania, architektury korporacyjnej.			
DB13	***INŻYNIERIA WSTECZNA ZŁOŚLIWEGO OPROGRAMOWANIA*** Treść programu ramowego: Podstawowe ataki teleinformatyczne; narzędzia ataków i testów penetracyjnych; wybrane, reprezentatywne techniki ataków; malware: klasyfikacja, zasady budowy i działania; użycie, rozpoznawanie i zasady analizy malware. Rozpoznawanie rodzajów ataków. Metody odtwarzania kodu złośliwego oprogramowania.	**3**	ITT	K_W03, K_W08, K_U05, K_U09
	specjalność „cyberobrona”			
DC1	***MODELOWANIE SYSTEMÓW TELEINFORMATYCZNYCH*** Treść programu ramowego: Podstawy modelowania systemu teleinformatycznego (ST) w języku UML. Modelowanie wymagań na system teleinformatyczny, architektury i zachowania ST. Diagramy interakcji, diagram maszyny stanów. Modelowanie protokołów: diagramy przepływu wywołań, przekształcanie diagramów wywołań do diagramu maszyny stanów. Modele formalne: weryfikacja modelu, modele systemów równoległych, własności liniowo-czasowe, bezpieczeństwo i żywotność. Sieci Petriego (SP): definicja, własności modelu, drzewo osiągalności, wybrane rodzaje sieci Petriego. Modelowanie ST uwarunkowanych czasowo; automaty czasowe. Przykładowe zadania modelowania systemów teleinformatycznych: badanie własności systemu na podstawie modelu. Zapoznanie ze środowiskiem narzędziowym. Budowa modelu przypadków użycia dla przykładowego systemu teleinformatycznego. Modelowanie struktury i zachowania ST z wykorzystaniem RSA. Modelowanie protokołów z wykorzystaniem diagramów interakcji i diagramów wywołań. Transformacja modelu zachowania do modelu sieci Petriego. Modelowanie ST uwarunkowanych czasowo z wykorzystaniem czasowych SP.	**3**	ITT	K_W04, K_W05, K_U03, K_K04, K_K05, K_K06
DC2	***BEZPIECZEŃSTWO SIECI IPv6*** Treść programu ramowego: Charakterystyka protokołu IPv6.Adresacja IPv6 - formaty zapisu, rodzaje i przezna-czenie 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.	**4**	ITT	K_W07, K_W08, K_U09, K_K03, K_K06
DC3	***SYSTEMY ROZPROSZONE*** Treść programu ramowego: Podstawowe pojęcia przetwarzania rozproszonego. Synchronizacja w środowisku rozpro-szonym. 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.	**3**	ITT	K_W04, K_U11, K_K05, K_K06

DC4	***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, K_K03, K_K06
DC5	***TRENDS IN COMPUTER TECHNOLOGY (w języku angielskim)*** Treść programu ramowego: Rys historyczny rozwoju technologii komputerowych. Architektura współczesnych komputerów osobistych oraz serwerów. Trendy rozwoju podstawowych elementów: płyta główna, procesor, pamięć operacyjna, napędy magnetyczne i optyczne. Magistrale współczesnych komputerów: PCI-E, SATA, HyperTransport, QPI. Analiza rynku komputerów osobistych i serwerów. Najnowsze trendy rozwoju technologii komputerowych i rynku IT.	**2**	ITT	K_W03, K_U08, K_K01, K_K06, K_U13
DC6	***ERGONOMIA SYSTEMÓW INTERAKTYWNYCH*** Treść programu ramowego: Wymagania ergonomiczne na interfejs użytkownika w systemach interaktywnych. 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 projektowania interakcji w interfejsie użytkownika. Projektowanie graficznego interfejsu użytkownika w systemie interaktywnym. Ocena jakości użytkowej interfejsu użytkownika aplikacji. Heurystyki Nielsena i Molicha.	**2**	ITT	K_W02, K_W04, K_W05, K_U02, K_U12, K_K04, K_K06
DC7	***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
DC8	***PROJEKTOWANIE SYSTEMÓW BEZPIECZEŃSTWA INFORMACJI*** 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_W03, K_W08, K_U04, K_K03, K_K06
DC9	***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 sys-	**4**	ITT	K_W04, K_W09, K_U03, K_U04, K_U10, K_K04, K_K06

	temów 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.			
DC10	***WIRTUALIZACJA SYSTEMÓW IT*** Treść programu ramowego: 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	***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
DC12	***ZARZĄDZANIE SIECIAMI TELEINFORMATYCZNYMI*** Treść programu ramowego: 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.	**4**	ITT	K_W03, K_W07, K_U07, K_K03, K_K06
DC13	***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	**3**	ITT	K_W05, K_W07, K_U08, K_K04, K_K06

	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.			
DC14	***STUDIUM ATAKÓW I INCYDENTÓW*** Treść programu ramowego: Słabości zasobów teleinformatycznych i sposoby ich wykorzystywania - przegląd zagrożeń. Typowe techniki ataków. Metodyki i narzędzia badań technicznych bezpieczeństwa – testy penetracyjne. Wybrane narzędzia ataków teleinformatycznych. Złożone metody atakowania systemów teleinformatycznych. Warunki powodzenia. brona. Rozpoznawanie symptomów działań nieuprawnionych. Włamanie, studium przypadku. Techniki śledcze. Analiza powłamaniowa. Zarządzanie incydentami. Aktualne trendy.	**3**	ITT	K_W03, K_W08, K_U09, K_K03, K_K06
DC15	***WALKA W CYBERPRZESTRZENI*** Treść programu ramowego: Podstawowe pojęcia cyberbezpieczeństwa. Sieć rozległa i organizacja Internetu. Cele w cyberprzestrzeni (infrastruktura krytyczna, zasoby korporacyjne, media społecznościowe, urządzenia prywatne). Rodzaje ataków i metody obrony. Malware i botnety. Zapewnianie własnego 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	***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
DK2	***ELEMENTY ALGEBRAICZNEJ TEORII LICZB*** Treść programu ramowego: Aksjomaty teorii mnogości. Konstrukcja zbioru liczb naturalnych. Monoid liczb naturalnych. Konstrukcja zbioru liczb całkowitych i wymiernych. Własności działań w zdefiniowanych zbiorach. pierścień 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".	**3**	M	K_W02, K_U02
DK3	***GENERACJA I TESTOWANIE LOSOWOŚCI*** Treść programu ramowego: Pojęcie losowości. Test statystyczny. 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	***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
DK5	***METODY STATYSTYCZNE W KRYPTOLOGII II*** Treść programu ramowego: Przedmiot służy do poznania i zrozumienia przez studentów podstawowych pojęć i twierdzeń metod statystycznych w kryptologii, oraz opanowania umiejętności wnioskowania dla dużych prób oraz badania własności generatorów liczb losowych. Analiza danych statystycznych. Losowe ciągi binarne. Testy statystyczne: parametryczne i nieparametryczne. Test momentów. Testy porównujące parametry. Testy zgodności. Testy losowości: test pokerowy, test kolekcjonera, test permutacji. Probabilistyczny test dla liczb pierwszych.	**2**	M	K_W02, K_U02
DK6	***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
DK7	***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.	**3**	ITT	K_W03, K_W04, K_W08, K_U09, K_U14, K_K01
DK8	***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
DK9	***KRYPTOANALIZA ALGORYTMÓW STRUMIENIOWYCH*** Treść programu ramowego: Podstawy kryptoanalizy szyfrów strumieniowych. Atak na złożoność liniową generatora. Kryptoanalityczne modele generatora klucza. Podstawy ataków korelacyjnych. Szybkie ataki korelacyjne. Atak na generator z filtrem. Atak na generator sumacyjny. Atak na generatory z kontrolowanym zegarem. Kryptoanaliza wybranych algorytmów strumieniowych.	**4**	ITT	K_W03, K_W04, K_W08, K_U09, K_U14, K_K01

DK10	***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.	**3**	ITT	K_W02, K_W03, K_W04, K_W02, K_U08, K_U09, K_U14, K_K01
DK11	***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. Liniowe zadanie najmniejszych kwadratów w postaci algebraicznej. Zadanie nadokreślone z macierzą pełnego rzędu. Algorytm z równaniem normalnym. Uwarunkowanie zadania. Rozkład macierzy według wartości szczególnych. Iteracyjne metody rozwiązywania układów liniowych równań algebraicznych	**3**	M	K_W02, K_U02
DK12	***SYSTEMY KLUCZA PUBLICZNEGO II*** Treść programu ramowego: Problemy trudne obliczeniowo i ich zastosowania w kryptografii. Problem faktoryzacji. Problem logarytmu dyskretnego. Inne problemy trudne obliczeniowo. Kryptosytem RSA: specyfikacja algorytmu, podstawy matematyczne, bezpieczeństwo, implementacja. Kryptosytem ElGamala: specyfikacja algorytmu, podstawy matematyczne, bezpieczeństwo, implementacja. Protokół Diffie-Hellmana: specyfikacja algorytmu, podstawy matematyczne, bezpieczeństwo, implementacja. Algorytmy faktoryzacji. Złożoność podwykładnicza. Podstawy matematyczne. Implementacja. Algorytmy obliczania logarytmów dyskretnych Złożoność podwykładnicza. Podstawy matematyczne. Implementacja. Problem plecakowy. Kryposystemy klucza publicznego oparte na problemie plecakowym. Kryptosystemy klucza publicznego oparte na problemach trudnych obliczeniowo z teorii krat. Kryptosystemy oparte na teorii funkcji wielu zmiennych. Elementy kryptografii kwantowej.	**3**	ITT	K_W03, K_W04, K_W08, K_U09, K_U14, K_K01
DK13	***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_U02

DK14	***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.	**4**	ITT	K_W03, K_W04, K_W08, K_U09, K_U11, K_U14, K_K01
DK15	***AKREDYTACJA SYSTEMÓW TELEINFORMATYCZNYCH*** Treść programu ramowego: Zasady ogólne konstrukcji zabezpieczeń dla systemów przetwarzających informacje klasyfikowane: analiza systemu informatycznego, metody oceny zasobów istotnych, metody analizy ryzyka. Metody projektowania zabezpieczeń technicznych, organizacyjnych, fizycznych. Zasady konstruowania polityki bezpieczeństwa. Zasady konstruowania dokumentacji akredytacyjnej dla systemów przetwarzających informacje klasyfikowane. Aktualne normy w dziedzinie konstruowania systemów ochrony danych: normy ISO z grupy 270xx, normy amerykańskie.	**3**	ITT	K_W03, K_W07, K_U07, K_U14, K_K01 K_K03, K_K06
	Przedmioty dyplomowania	**23**		
E1	***SEMINARIUM DYPLOMOWE*** Treść programu ramowego: Seminarium uzupełnia konsultacje studenta z promotorem podczas przygotowywania pracy dyplomowej i przygotowuje go do egzaminu dyplomowego.	**3**		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	***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**		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 się[1] osiągniętych przez studenta trakcie całego cyklu kształcenia

Wdrożenie koncepcji prowadzenia zajęć według założonych efektów kształcenia przekłada się na różnorodne formy i kryteria ewaluacji. Istotnym aspektem weryfikacji jest klarowne określenie kryteriów oceny w odniesieniu do poszczególnych efektów kształcenia. Na pierwszych zajęciach w ramach poszczególnych modułów kształcenia prowadzący zajęcia informują studentów o zakładanych przedmiotowych efektach kształcenia oraz o formach i sposobach ich weryfikacji. Sposoby weryfikacji zakładanych efektów kształcenia zależą przede wszystkim od rodzaju zajęć. Szczegółowe zasady określone są w sylabusach poszczególnych modułów kształcenia. 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 pozytywne zaliczenie wszystkich innych rygorów – ćwiczeń rachunkowych/konwersatoryjnych, ćwiczeń laboratoryjnych oraz seminarium i projektu.

Ćwiczenia laboratoryjne prowadzone są 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 przy wykorzystaniu pozyskanych umiejętności i doświadczenia.
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 prowadzone są 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.

[1] opis ogólny - szczegóły *w kartach informacyjnych przedmiotów udostępnianych studentom 30 dni przed rozpoczęciem zajęć.*

5. PLANY STUDIÓW

Plany studiów:

1. Plan studiów stacjonarnych II stopnia dla specjalności *Systemy kryptograficzne* - Załącznik nr 1a
2. Plan studiów stacjonarnych II stopnia dla specjalności *Cyberobrona* - Załącznik nr 2a
3. Plan studiów stacjonarnych II stopnia dla specjalności *Bezpieczeństwo informacyjne* - Załącznik nr 3a
4. Plan studiów niestacjonarnych II stopnia dla specjalności *Systemy kryptograficzne* - Załącznik nr 1b
5. Plan studiów niestacjonarnych II stopnia dla specjalności *Cyberobrona* - Załącznik nr 2b
6. Plan studiów niestacjonarnych II stopnia dla specjalności *Bezpieczeństwo informacyjne* - Załącznik nr 3b

Wojskowa Akademia Techniczna

PLAN STACJONARNYCH STUDIÓW DRUGIEGO STOPNIA O PROFILU OGÓLNOAKADEMICKIM
OD NABORU 2019

Załącznik 1a

Kierunek: **kryptologia i cyberbezpieczeństwo** Dyscyplina naukowa: **informatyka techniczna i telekomunikacja**

Specjalność profilowana przedmiotami wybieralnymi: **Systemy kryptograficzne** **początek 2019**

Indeks	Grupy zajęć / przedmioty	Dyscyplina naukowa	Ogółem godziny/ECTS		ECTS w zajęciach			Liczba godzin / rygor według formy zajęć										Liczba godzin /rygor / liczba punktów ECTS w semestrze										Jednostka organizacyjna odpowiedzialna za przedmiot	Uwagi
																		I			II			III					
			godziny	ECTS	kszt. um. prakt.	kszt. um. nauk.	z udz. naucz. akad.	wykłady		ćwiczenia		laboratorium		projekt		seminarium		godziny		ECTS	godziny		ECTS	godziny		ECTS			
A. Grupa treści kształcenia ogólnego			**4**	**0**		0	0	4		0		0		0		0		4		0	0		0	0		0			
A.1	Bezpieczeństwo i higiena pracy		**4**					4										4										Sekcja BHP	
B. Grupa treści kształcenia podstawowego			**178**	**15**	7	15	8,5	82		40		42		14				138		12	20		2	20		1			
B.1	Metody i techniki symulacji komputerowej	ITT	**44**	**4**	3	4	2	10	x			20	+	14	+			44	x	4								WCY-ISI	
B.2	Procesy stochastyczne	M	**30**	**2**	0,5	2	1,5	16	+	14	+							30	+	2								WCY-IMK	
B.3	Bezpieczeństwo baz danych	ITT	**44**	**4**	2,5	4	2	14	+	8	+	22	+					44	+	4								WCY-ISI	
B.4	Socjologia	NS	**20**	**1**	0	1	1	14	+	6	+													20	+	1		WCY-IOZ	
B.5	Ekonomia	EF	**20**	**2**	0,5	2	1	14	+	6	+										20	+	2					WCY-IOZ	
B.6	Nowoczesne metody i techniki zarządzania	NZJ	**20**	**2**	0,5	2	1	14	+	6	+							20	+	2								WCY-IOZ	
C. Grupa treści kształcenia kierunkowego			**74**	**6**	2,5	6	3,5	32				26		16				0		0	74		6			0			
C.1	Steganografia	ITT	**30**	**3**	1	3	1,5	16	+			14	+								30	+	3					WCY-IMK	
C.2	Diagnostyka i tolerowanie uszkodzeń	ITT	**44**	**3**	1,5	3	2	16	x			12	+	16	+						44	x	3					WCY-ITA	
D. Grupa treści kształcenia specjalistycznego			**550**	**46**	21	46	26	266		60		186		38				238		18	252		22	60		6			
D.K.1	Ataki algebraiczne	ITT	**30**	**3**	1	3	1,5	20	+			10	+								30	+	3					WCY-IMK	
D.K.2	Elementy algebraicznej teorii liczb	M	**30**	**3**	1,5	3	1,5	14	+	16	+							30	+	3								WCY-IMK	
D.K.3	Generacja I testowanie losowosci	ITT	**44**	**3**	1,5	3	2	20	x	10	+	14	+					44	x	3								WCY-IMK	
D.K.4	Teoria ciał skończonych	M	**30**	**3**	1	3	1,5	20	+	10	+							30	+	3								WCY-IMK	
D.K.5	Metody statystyczne w kryptologii II	M	**30**	**2**	1	2	1,5	10	+			20	+					30	+	2								WCY-IMK	
D.K.6	Elements of Public-Key Cryptology (w języku angielskim)	ITT	**30**	**3**	1	3	1,5	20	x			10	+											30	x	3		WCY-IMK	
D.K.7	Quantum and Post-Quantum Cryptology (w języku angielskim)	ITT	**30**	**3**	1	3	1,5	20	+	10	+										30	+	3					WCY-IMK	
D.K.8	Kryptoanaliza algorytmów blokowych	ITT	**30**	**3**	1	3	1,5	20	+	4	+	6	+								30	+	3					WCY-IMK	
D.K.9	Kryptoanaliza algorytmów strumieniowych	ITT	**44**	**4**	1,5	4	2	24	+			20	+								44	+	4					WCY-IMK	
D.K.10	Projekt z zakresu matematycznych i informatycznych podstaw kryptol	ITT	**30**	**3**	2,5	3	1,5	2	+					28	+									30	+	3		WCY-IMK	
D.K.11	Metody numeryczne w kryptologii	M	**44**	**3**	1,5	3	2	20	x			24	+								44	x	3					WCY-IMK	
D.K.12	Systemy klucza publicznego II	ITT	**44**	**3**	1,5	3	2	20	x	10	+	14	+								44	x	3					WCY-IMK	
D.K.13	Krzywe hipereliptyczne w kryptologii	ITT	**30**	**3**	1,5	3	1,5	12	+			8	+	10	+						30	+	3					WCY-IMK	
D.K.14	Projektowanie kryptograficznych ukladow cyfrowych II	ITT	**60**	**4**	2	4	2,5	24	x			36	+					60	x	4								WCY-IMK	
D.K.15	Akredytacja systemów teleinformatycznych	ITT	**44**	**3**	1,5	3	2	20	+			24	+					44	+	3								WCY-IMK	
E. Praca dyplomowa			**44**	**23**		23	23							0		44								44		23			
E.1	Seminarium dyplomowe		**44**	**3**	3	3	3									44								44	+	3		WCY	
E.2	Praca dyplomowa			**20**	20	20	20																		x	20		WCY	
ogólem godzin / punktów ECTS			**850**	**90**	30,5	90	61	384		100		254		68		44		380		30	346		30	124		30			
dopuszczalny deficyt punktów ECTS																		10			10			0					
rodzaje i liczba rygorów w semestrze:																	liczba egzaminów (x)	3			3			1					
																	liczba zaliczeń (+)	7			7			2					
																	liczba projektów przejściowych (#)	1			1			0					

Wojskowa Akademia Techniczna

PLAN STACJONARNYCH STUDIÓW DRUGIEGO STOPNIA O PROFILU OGÓLNOAKADEMICKIM
OD NABORU 2019

Załącznik 2a

Kierunek: **kryptologia i cyberbezpieczeństwo** Dyscyplina naukowa: **informatyka techniczna i telekomunikacja**

Specjalność profilowana przedmiotami wybieralnymi: **Cyberobrona** **początek 2019**

Indeks	Grupy zajęć / przedmioty	Dyscyplina naukowa	Łącznie godziny/ECTS		ECTS w zajęciach			Liczba godzin / rygor według formy zajęć										Liczba godzin /rygor / liczba punktów ECTS w semestrze									Jednostka organizacyjna odpowiedzialna za przedmiot	Uwagi
																		I			II			III				
			godziny	ECTS	kszt. um. prakt.	kszt. um. nauk.	z udz. naucz.	wykłady		ćwiczenia		laboratorium		projekt		seminarium		godziny		ECTS	godziny		ECTS	godziny		ECTS		
A. Grupa treści kształcenia ogólnego			**4**	**0**	0	0	0	4		0		0		0		0		4		0	0		0	0		0		
A.1	Bezpieczeństwo i higiena pracy		**4**					4										4									Sekcja BHP	
B. Grupa treści kształcenia podstawowego			**178**	**15**	7	15	8,5	82		40		42		14		0		138		12	20		2	20		1		
B.1	Metody i techniki symulacji komputerowej	ITT	**44**	**4**	3	4	2	10	x			20	+	14	+			44	x	4							WCY-ISI	
B.2	Procesy stochastyczne	M	**30**	**2**	0,5	2	1,5	16	+	14	+							30	+	2							WCY-IMK	
B.3	Bezpieczeństwo baz danych	ITT	**44**	**4**	2,5	4	2	14	+	8	+	22	+					44	+	4							WCY-ISI	
B.4	Socjologia	NS	**20**	**1**	0	1	1	14	+	6	+													20	+	1	WCY-IOZ	
B.5	Ekonomia	EF	**20**	**2**	0,5	2	1	14	+	6	+										20	+	2				WCY-IOZ	
B.6	Nowoczesne metody i techniki zarządzania	NZJ	**20**	**2**	0,5	2	1	14	+	6	+							20	+	2							WCY-IOZ	
C. Grupa treści kształcenia kierunkowego			**74**	**6**	2,5	6	3,5	32		0		26		16		0		0		0	74		6			0		
C.1	Steganografia	ITT	**30**	**3**	1	3	1,5	16	+			14	+								30	+	3				WCY-IMK	
C.2	Diagnostyka i tolerowanie uszkodzeń	ITT	**44**	**3**	1,5	3	2	16	x			12	+	16	+						44	x	3				WCY-ITA	
D. Grupa treści kształcenia specjalistycznego			**534**	**46**	24	46	25,5	224		10		202		98		0		222		18	252		22	60		6		
D.C.1	Modelowanie systemów teleinformatycznych	ITT	**44**	**3**	1,5	3	2	16	+			12	+	16	+			44	#	3							WCY-ITA	
D.C.2	Bezpieczeństwo sieci IPv6	ITT	**44**	**4**	2,5	4	2	12	x			20	+	12	+			44	x	4							WCY-ITA	
D.C.3	Systemy rozproszone	ITT	**30**	**3**	1	3	1,5	20	x					10	+			30	x	3							WCY-ITA	
D.C.4	Zarządzanie bezpieczeństwem informacji	ITT	**44**	**4**	1,5	4	2	24	x	10	+	10	+					44	x	4							WCY-ITA	
D.C.5	Trends in computer technology (w języku angielskim)	ITT	**30**	**2**	0,5	2	1,5	20	+			10						30	+	2							WCY-ITA	
D.C.6	Ergonomia systemów interaktywnych	ITT	**30**	**2**	1	2	1,5	14	+			16	+					30	+	2							WCY-ITA	
D.C.7	Technologie mobilne	ITT	**30**	**2**	1	2	1,5	14	+			16	+								30	+	2				WCY-ITA	
D.C.8	Projektowanie systemów bezpieczeństwa informacji	ITT	**44**	**4**	2,5	4	2	14	x			16	+	14	+						44	x	4				WCY-ITA	
D.C.9	Analiza i projektowanie systemów teleinformatycznych	ITT	**44**	**4**	2,5	4	2	16	x			14	+	14	+						44	x	4				WCY-ITA	
D.C.10	Wirtualizacja systemów IT	ITT	**30**	**2**	1	2	1,5	10	+			12	+	8	+						30	+	2				WCY-ITA	
D.C.11	Techniki dochodzeniowe i śledcze	ITT	**30**	**3**	2	3	1,5	10	+			20	+								30	+	3				WCY-ITA	
D.C.12	Zarządzanie sieciami teleinformatycznymi	ITT	**44**	**4**	2,5	4	2	14	x			20	+	10	+						44	x	4				WCY-ITA	
D.C.13	Technologie Internetu Rzeczy	ITT	**30**	**3**	1	3	1,5	16	+					14	+									30	+	3	WCY-ITA	
D.C.14	Studium ataków i incydentów	ITT	**30**	**3**	1,5	3	1,5	14	+			16	+								30	+	3				WCY-ITA	
D.C.15	Walka w cyberprzestrzeni	ITT	**30**	**3**	2	3	1,5	10	x			20	+											30	x	3	WCY-ITA	
E. Praca dyplomowa			**44**	**23**	23	23	23							500		44								44		23		
E.1	Seminarium dyplomowe		**44**	**3**	3	3	3									44								44	+	3	WCY	
E.2	Praca dyplomowa			**20**	20	20	20							500											x	20	WCY	
ogółem godzin / punktów ECTS			**834**	**90**	56,5	90	60,5	342		50		270		628		44		364		30	346		30	124		30		
dopuszczalny deficyt punktów ECTS																		10			10			0				
rodzaje i liczba rygorów w semestrze:																												
																	liczba egzaminów (x)	4			4			1				
																	liczba zaliczeń (+)	5			6			2				
																	liczba projektów przejściowych (#)	4			4			0				

Wojskowa Akademia Techniczna

PLAN STACJONARNYCH STUDIÓW DRUGIEGO STOPNIA O PROFILU OGÓLNOAKADEMICKIM Załącznik 3a
OD NABORU 2019

Kierunek: **kryptologia i cyberbezpieczeństwo** Dyscyplina naukowa: **informatyka techniczna i telekomunikacja**

Specjalność profilowana przedmiotami wybieralnymi: **Bezpieczeństwo informacyjne** **początek 2019**

Indeks	Grupy zajęć / przedmioty	Dyscyplina naukowa	Ogółem godziny/E		ECTS w zajęciach			Liczba godzin / rygor według formy zajęć										Liczba godzin /rygor / liczba punktów ECTS w semestrze									Jednostka organizacyjna odpowiedzialna za przedmiot	Uwagi
																		I			II			III				
			godziny	ECTS	kszt. um. prakt.	kszt. um. nauk.	z udz. naucz.	wykłady		ćwiczenia		laboratorium		projekt		seminarium		godziny		ECTS	godziny		ECTS	godziny		ECTS		
A. Grupa treści kształcenia ogólnego			**4**	**0**		0	0	4		0		0		0		0		4		0	0		0	0		0		
A.1	Bezpieczeństwo i higiena pracy		**4**					4										4									Sekcja BHP	
B. Grupa treści kształcenia podstawowego			**178**	**15**	7	15	8,5	82		40		42		14				138		12	20		2	20		1		
B.1	Metody i techniki symulacji komputerowej	ITT	**44**	**4**	3	4	2	10	x			20	+	14	+			44	x	4							WCY-ISI	
B.2	Procesy stochastyczne	M	**30**	**2**	0,5	2	1,5	16	+	14	+							30	+	2							WCY-IMK	
B.3	Bezpieczeństwo baz danych	ITT	**44**	**4**	2,5	4	2	14	+	8	+	22	+					44	+	4							WCY-ISI	
B.4	Socjologia	NS	**20**	**1**	0	1	1	14	+	6	+													20	+	1	WCY-IOZ	
B.5	Ekonomia	EF	**20**	**2**	0,5	2	1	14	+	6	+										20	+	2				WCY-IOZ	
B.6	Nowoczesne metody i techniki zarządzania	NZJ	**20**	**2**	0,5	2	1	14	+	6	+							20	+	2							WCY-IOZ	
C. Grupa treści kształcenia kierunkowego			**74**	**6**	2,5	6	3,5	32				26		16				0		0	74		6			0		
C.1	Steganografia	ITT	**30**	**3**	1	3	1,5	16	+			14	+								30	+	3				WCY-IMK	
C.2	Diagnostyka i tolerowanie uszkodzeń	ITT	**44**	**3**	1,5	3	2	16	x			12	+	16	+						44	x	3				WCY-ITA	
D. Grupa treści kształcenia specjalistycznego			**530**	**46**	26,5	46	24,5	198		58		206		68				192		18	264		22	74		6		
D.B.1	Podstawy kryptologii współczesnej	ITT	**44**	**4**	2,5	4	2	16	+	12	+	16	+								44	+	4				WCY-IMK	
D.B.2	Zaawansowane technologie usługowe i mobilne	ITT	**30**	**3**	1,5	3	1,5	14	+			16	+					30	+	3							WCY-ISI	
D.B.3	Modelowanie i analiza sieci złożonych	ITT	**44**	**5**	3	5	2	18	x	10	+	16	+					44	x	5							WCY-ISI	
D.B.4	Ilościowe metody oceny bezpieczeństwa systemów teleinformatyczny	ITT	**44**	**4**	2	4	2	18	x	12	+	14	+											44	x	4	WCY-ISI	
D.B.5	Projektowanie bezpiecznych systemów	ITT	**44**	**4**	2	4	2	20	x			24	+								44	x	4				WCY-ISI	
D.B.6	Zarzadzanie projektami	ITT	**44**	**4**	2,5	4	2	16	+	14	+	14	+					44	+	4							WCY-ISI	
D.B.7	Zaawansowane metody eksploracji danych	ITT	**44**	**4**	2	4	2	20	x			24	+					44	x	4							WCY-ISI	
D.B.8	Teoria wojny informacyjnej	ITT	**30**	**2**	0,5	2	1,5	16	+			14	+											30	+	2	WCY-ISI	
D.B.9	Zarządzanie bezpieczeństwem informacji	ITT	**44**	**3**	1,5	3	2	20	x			24	+								44	x	3				WCY-ISI	
D.B.10	Niezawodność i wydajność systemów informatycznych	ITT	**44**	**4**	2	4	2	18	+	10	+	16	+								44	+	4				WCY-ISI	
D.B.11	Projekt z zakresu bezpieczeństwa systemów	ITT	**44**	**4**	4	4	2		x					44	+						44	x	4				WCY-ISI	
D.B.12	Bussines modeling in UML (w języku angielskim)	ITT	**30**	**2**	1	2	1,5	10	+			20	+					30	+	2							WCY-ISI	
D.B.13	Inżynieria wsteczna złośliwego oprogramowania	ITT	**44**	**3**	2	3	2	12	+			8	+	24	+						44	+	3				WCY-ISI	
E. Praca dyplomowa			**44**	**23**	23	23	23							0		44								44		23		
E.1	Seminarium dyplomowe		**44**	**3**	3	3	3									44	+							44	+	3	WCY	
E.2	Praca dyplomowa			**20**	20	20	20																		x	20	WCY	
ogółem godzin / punktów ECTS			**830**	**90**	59	90	59,5	316		98		274		98		44		334		30	358		30	138		30		
dopuszczalny deficyt punktów ECTS																		10			10			0				
rodzaje i liczba rygorów w semestrze:																												
																	liczba egzaminów (x)	3			4			1				
																	liczba zaliczeń (+)	6			5			2				
																	liczba projektów przejściowych (#)	1			2			0				

Wojskowa Akademia Techniczna

PLAN NIESTACJONARNYCH STUDIÓW DRUGIEGO STOPNIA O PROFILU OGÓLNOAKADEMICKIM **Załącznik 1b**

OD NABORU 2019

Kierunek: **kryptologia i cyberbezpieczeństwo** Dyscyplina naukowa: **informatyka techniczna i telekomunikacja**

Specjalność profilowana przedmiotami wybieralnymi: **Systemy kryptograficzne** **początek 2019**

Indeks	Grupy zajęć / przedmioty	Dyscyplina naukowa	Ogółem godziny/ECTS		ECTS w zajęciach			Liczba godzin / rygor według formy zajęć										Liczba godzin /rygor / liczba punktów ECTS w semestrze									Jednostka organizacyjna odpowiedzialna za przedmiot	Uwagi
																		I			II			III				
			godziny	ECTS	kszt. um. prakt.	kszt. um. nauk.	z udz. naucz. akad.	wykłady		ćwiczenia		laboratorium		projekt		seminarium		godziny		ECTS	godziny		ECTS	godziny		ECTS		
A. Grupa treści kształcenia ogólnego			**4**	**0**		0	0	4		0		0		0		0		4		0	0		0	0		0		
A.1	Bezpieczeństwo i higiena pracy		**4**					4										4									Sekcja BHP	
B. Grupa treści kształcenia podstawowego			**122**	**15**	6,5	15	5,5	62		26		24		10				94		12	14		2	14		1		
B.1	Metody i techniki symulacji komputerowej	ITT	**30**	**4**	2,5	4	1,5	10	x			10	+	10	+			30	x	4							WCY-ISI	
B.2	Procesy stochastyczne	M	**20**	**2**	0,5	2	1	12	+	8	+							20	+	2							WCY-IMK	
B.3	Bezpieczeństwo baz danych	ITT	**30**	**4**	2,5	4	1,5	10	+	6	+	14	+					30	+	4							WCY-ISI	
B.4	Socjologia	NS	**14**	**1**	0	1	0,5	10	+	4	+													14	+	1	WCY-IOZ	
B.5	Ekonomia	EF	**14**	**2**	0,5	2	0,5	10	+	4	+										14	+	2				WCY-IOZ	
B.6	Nowoczesne metody i techniki zarządzania	NZJ	**14**	**2**	0,5	2	0,5	10	+	4	+							14	+	2							WCY-IOZ	
C. Grupa treści kształcenia kierunkowego			**50**	**6**	3	6	2,5	22				16		12				0		0	50		6			0		
C.1	Steganografia	ITT	**20**	**3**	1	3	1	12	+			8	+								20	+	3				WCY-IMK	
C.2	Diagnostyka i tolerowanie uszkodzeń	ITT	**30**	**3**	2	3	1,5	10	x			8	+	12	+						30	x	3				WCY-ITA	
D. Grupa treści kształcenia specjalistycznego			**394**	**46**	19,5	46	19,5	190		46		130		28				174		18	180		22	40		6		
D.K.1	Ataki algebraiczne	ITT	**20**	**3**	1	3	1	12	+			8	+								20	+	3				WCY-IMK	
D.K.2	Elementy algebraicznej teorii liczb	M	**30**	**3**	1,5	3	1,5	14	+	16	+							30	+	3							WCY-IMK	
D.K.3	Generacja I testowanie losowosci	ITT	**30**	**3**	1,5	3	1,5	14	x	6	+	10	+					30	x	3							WCY-IMK	
D.K.4	Teoria ciał skończonych	M	**20**	**3**	0,5	3	1	14	+	6	+							20	+	3							WCY-IMK	
D.K.5	Metody statystyczne w kryptologii II	M	**20**	**2**	1	2	1	8	+			12	+					20	+	2							WCY-IMK	
D.K.6	Elements of Public-Key Cryptology (w języku angielskim)	ITT	**20**	**3**	0,5	3	1	14	x			6	+											20	x	3	WCY-IMK	
D.K.7	Quantum and Post-Quantum Cryptology (w języku angielskim)	ITT	**20**	**3**	1	3	1	12	+	8	+										20	+	3				WCY-IMK	
D.K.8	Kryptoanaliza algorytmów blokowych	ITT	**20**	**3**	0,5	3	1	14	+	4	+	2	+								20	+	3				WCY-IMK	
D.K.9	Kryptoanaliza algorytmów strumieniowych	ITT	**30**	**4**	1,5	4	1,5	16	+			14	+								30	+	4				WCY-IMK	
D.K.10	Projekt z zakresu matematycznych i informatycznych podstaw krypt	ITT	**20**	**3**	2,5	3	1	2	+					18	+									20	+	3	WCY-IMK	
D.K.11	Metody numeryczne w kryptologii	M	**30**	**3**	1,5	3	1,5	14	x			16	+								30	x	3				WCY-IMK	
D.K.12	Systemy klucza publicznego II	ITT	**30**	**3**	1,5	3	1,5	14	x	6	+	10	+								30	x	3				WCY-IMK	
D.K.13	Krzywe hipereliptyczne w kryptologii	ITT	**30**	**3**	1,5	3	1,5	12	+			8	+	10	+						30	#	3				WCY-IMK	
D.K.14	Projektowanie kryptograficznych ukladow cyfrowych II	ITT	**44**	**4**	2	4	2	18	x			26	+					44	x	4							WCY-IMK	
D.K.15	Akredytacja systemów teleinformatycznych	ITT	**30**	**3**	1,5	3	1,5	12	+			18	+					30	+	3							WCY-IMK	
E. Praca dyplomowa			**44**	**23**		23	13							500		44								44		23		
E.1	Seminarium dyplomowe		**44**	**3**	3	3	3									44								44	+	3	WCY	
E.2	Praca dyplomowa			**20**	20	20	10							500											x	20	WCY	
ogółem godzin / punktów ECTS			**614**	**90**	29	90	40,5	278		72		170		50		44		272		30	244		30	98		30		
dopuszczalny deficyt punktów ECTS																		10			10			0				
rodzaje i liczba rygorów w semestrze:																												
																	liczba egzaminów (x)	3			3			1				
																	liczba zaliczeń (+)	7			6			2				
																	liczba projektów przejściowych (#)	1			2			0				

Wojskowa Akademia Techniczna

PLAN NIESTACJONARNYCH STUDIÓW DRUGIEGO STOPNIA O PROFILU OGÓLNOAKADEMICKIM
OD NABORU 2019

Załącznik 2b

Kierunek: **kryptologia i cyberbezpieczeństwo** Dyscyplina naukowa: **informatyka techniczna i telekomunikacja**

Specjalność profilowana przedmiotami wybieralnymi: **Cyberobrona** **początek 2019**

Indeks	Grupy zajęć / przedmioty	Dyscyplina naukowa	Ogółem godziny/ECTS		ECTS w zajęciach			Liczba godzin / rygor według formy zajęć										Liczba godzin /rygor / liczba punktów ECTS w semestrze									Jednostka organizacyjna odpowiedzialna za przedmiot	Uwagi
																		I			II			III				
			godziny	ECTS	kszt. um. prakt.	kszt. um. nauk.	z udz. naucz. akad.	wykłady		ćwiczenia		laboratorium		projekt		seminarium		godziny		ECTS	godziny		ECTS	godziny		ECTS		
A. Grupa treści kształcenia ogólnego			**4**	**0**	0	0	0	4		0		0		0		0		4		0	0		0	0		0		
A.1	Bezpieczeństwo i higiena pracy		**4**					4										4									Sekcja BHP	
B. Grupa treści kształcenia podstawowego			**122**	**15**	6,5	15	5,5	62		26		24		10		0		94		12	14		2	14		1		
B.1	Metody i techniki symulacji komputerowej	ITT	**30**	**4**	2,5	4	1,5	10	x			10	+	10	+			30	x	4							WCY-ISI	
B.2	Procesy stochastyczne	M	**20**	**2**	0,5	2	1	12	+	8	+							20	+	2							WCY-IMK	
B.3	Bezpieczeństwo baz danych	ITT	**30**	**4**	2,5	4	1,5	10	+	6	+	14	+					30	+	4							WCY-ISI	
B.4	Socjologia	NS	**14**	**1**	0	1	0,5	10	+	4	+													14	+	1	WCY-IOZ	
B.5	Ekonomia	EF	**14**	**2**	0,5	2	0,5	10	+	4	+										14	+	2				WCY-IOZ	
B.6	Nowoczesne metody i techniki zarządzania	NZJ	**14**	**2**	0,5	2	0,5	10	+	4	+							14	+	2							WCY-IOZ	
C. Grupa treści kształcenia kierunkowego			**50**	**6**	3	6	2,5	22		0		16		12		0		0		0	50		6			0		
C.1	Steganografia	ITT	**20**	**3**	1	3	1	12	+			8	+								20	+	3				WCY-IMK	
C.2	Diagnostyka i tolerowanie uszkodzeń	ITT	**30**	**3**	2	3	1,5	10	x			8	+	12	+						30	x	3				WCY-ITA	
D. Grupa treści kształcenia specjalistycznego			**360**	**46**	23	46	18	160		8		124		68		0		150		18	170		22	40		6		
D.C.1	Modelowanie systemów teleinformatycznych	ITT	**30**	**3**	2	3	1,5	10	+			10	+	10	+			30	+	3							WCY-ITA	
D.C.2	Bezpieczeństwo sieci IPv6	ITT	**30**	**4**	2,5	4	1,5	10	x			10	+	10	+			30	x	4							WCY-ITA	
D.C.3	Systemy rozproszone	ITT	**20**	**3**	0,5	3	1	14	x					6	+			20	x	3							WCY-ITA	
D.C.4	Zarządzanie bezpieczeństwem informacji	ITT	**30**	**4**	1,5	4	1,5	16	x	8	+	6	+					30	x	4							WCY-ITA	
D.C.5	Trends in computer technology (w języku angielskim)	ITT	**20**	**2**	0,5	2	1	14	+			6						20	+	2							WCY-ITA	
D.C.6	Ergonomia systemów interaktywnych	ITT	**20**	**2**	0,5	2	1	12	+			8	+					20	+	2							WCY-ITA	
D.C.7	Technologie mobilne	ITT	**20**	**2**	1	2	1	10	+			10	+								20	+	2				WCY-ITA	
D.C.8	Projektowanie systemów bezpieczeństwa informacji	ITT	**30**	**4**	2,5	4	1,5	10	x			12	+	8	+						30	x	4				WCY-ITA	
D.C.9	Analiza i projektowanie systemów teleinformatycznych	ITT	**30**	**4**	2,5	4	1,5	10	x			10	+	10	+						30	x	4				WCY-ITA	
D.C.10	Wirtualizacja systemów IT	ITT	**20**	**2**	1	2	1	8	+			4	+	8	+						20	+	2				WCY-ITA	
D.C.11	Techniki dochodzeniowe i śledcze	ITT	**20**	**3**	1,5	3	1	8	+			12	+								20	+	3				WCY-ITA	
D.C.12	Zarządzanie sieciami teleinformatycznymi	ITT	**30**	**4**	2,5	4	1,5	10	x			14	+	6	+						30	x	4				WCY-ITA	
D.C.13	Technologie Internetu Rzeczy	ITT	**20**	**3**	1,5	3	1	10	+					10	+									20	+	3	WCY-ITA	
D.C.14	Studium ataków i incydentów	ITT	**20**	**3**	1,5	3	1	10	+			10	+								20	+	3				WCY-ITA	
D.C.15	Walka w cyberprzestrzeni	ITT	**20**	**3**	1,5	3	1	8	x			12	+											20	x	3	WCY-ITA	
E. Praca dyplomowa			**44**	**23**	23	23	13							500		44								44		23		
E.1	Seminarium dyplomowe		**44**	**3**	3	3	3									44								44	+	3	WCY	
E.2	Praca dyplomowa			**20**	20	20	10							500											x	20	WCY	
ogółem godzin / punktów ECTS			**580**	**90**	55,5	90	39	248		34		164		90		44		248		30	234		30	98		30		
dopuszczalny deficyt punktów ECTS																		10			10			0				
rodzaje i liczba rygorów w semestrze:																												
																	liczba egzaminów (x)	4			4			1				
																	liczba zaliczeń (+)	6			6			2				
																	liczba projektów przejściowych (#)	3			4			0				

Wojskowa Akademia Techniczna

PLAN NIESTACJONARNYCH STUDIÓW DRUGIEGO STOPNIA O PROFILU OGÓLNOAKADEMICKIM
OD NABORU 2019

Załącznik 3b

Kierunek: **kryptologia i cyberbezpieczeństwo** Dyscyplina naukowa: **informatyka techniczna i telekomunikacja**

Specjalność profilowana przedmiotami wybieralnymi: **Bezpieczeństwo informacyjne** **początek 2019**

Indeks	Grupy zajęć / przedmioty	Dyscyplina naukowa	Ogółem godziny/ECTS		ECTS w zajęciach			Liczba godzin / rygor według formy zajęć												Liczba godzin /rygor / liczba punktów ECTS w semestrze										Jednostka organizacyjna odpowiedzialna za przedmiot	Uwagi
																				I			II			III					
			godziny	ECTS	kszt. um. prakt.	kszt. um. nauk.	z udz. naucz. akad.	wykłady		ćwiczenia		laboratorium		projekt		seminarium				godziny		ECTS	godziny		ECTS	godziny		ECTS			
A. Grupa treści kształcenia ogólnego			**4**	**0**		0	0	4		0		0		0		0				4		0	0		0	0		0			
A.1	Bezpieczeństwo i higiena pracy		**4**					4												4									Sekcja BHP	
B. Grupa treści kształcenia podstawowego			**122**	**15**	6,5	15	5,5	62		26		24		10						94		12	14		2	14		1			
B.1	Metody i techniki symulacji komputerowej	ITT	**30**	**4**	2,5	4	1,5	10	x			10	+	10	+					30	x	4							WCY-ISI	
B.2	Procesy stochastyczne	M	**20**	**2**	0,5	2	1	12	+	8	+									20	+	2							WCY-IMK	
B.3	Bezpieczeństwo baz danych	ITT	**30**	**4**	2,5	4	1,5	10	+	6	+	14	+							30	+	4							WCY-ISI	
B.4	Socjologia	NS	**14**	**1**	0	1	0,5	10	+	4	+															14	+	1	WCY-IOZ	
B.5	Ekonomia	EF	**14**	**2**	0,5	2	0,5	10	+	4	+												14	+	2				WCY-IOZ	
B.6	Nowoczesne metody i techniki zarządzania	NZJ	**14**	**2**	0,5	2	0,5	10	+	4	+									14	+	2							WCY-IOZ	
C. Grupa treści kształcenia kierunkowego			**50**	**6**	3	6	2,5	22				16		12						0		0	50		6			0			
C.1	Steganografia	ITT	**20**	**3**	1	3	1	12	+			8	+										20	+	3				WCY-IMK	
C.2	Diagnostyka i tolerowanie uszkodzeń	ITT	**30**	**3**	2	3	1,5	10	x			8	+	12	+								30	x	3				WCY-ITA	
D. Grupa treści kształcenia specjalistycznego			**360**	**46**	25,5	46	18	136		40		138		46						130		18	180		22	50		6			
D.B.1	Podstawy kryptologii współczesnej	ITT	**30**	**4**	2	4	1,5	12	+	8	+	10	+										30	+	4				WCY-IMK	
D.B.2	Zaawansowane technologie usługowe i mobilne	ITT	**20**	**3**	1,5	3	1	8	+			12	+							20	+	3							WCY-ISI	
D.B.3	Modelowanie i analiza sieci złożonych	ITT	**30**	**5**	3	5	1,5	12	x	8	+	10	+							30	x	5							WCY-ISI	
D.B.4	Ilościowe metody oceny bezpieczeństwa systemów teleinformatycz	ITT	**30**	**4**	2	4	1,5	12	x	8	+	10	+													30	x	4	WCY-ISI	
D.B.5	Projektowanie bezpiecznych systemów	ITT	**30**	**4**	2	4	1,5	14	x			16	+										30	x	4				WCY-ISI	
D.B.6	Zarzadzanie projektami	ITT	**30**	**4**	2	4	1,5	12	+	8	+	10	+							30	+	4							WCY-ISI	
D.B.7	Zaawansowane metody eksploracji danych	ITT	**30**	**4**	2	4	1,5	14	x			16	+							30	x	4							WCY-ISI	
D.B.8	Teoria wojny informacyjnej (cyberwojny)	ITT	**20**	**2**	0,5	2	1	12	+			8	+													20	+	2	WCY-ISI	
D.B.9	Zarządzanie bezpieczeństwem informacji	ITT	**30**	**3**	1,5	3	1,5	14	x			16	+										30	x	3				WCY-ISI	
D.B.10	Niezawodność i wydajność systemów informatycznych	ITT	**30**	**4**	2	4	1,5	12	+	8	+	10	+										30	+	4				WCY-ISI	
D.B.11	Projekt z zakresu bezpieczeństwa systemów	ITT	**30**	**4**	4	4	1,5		x					30	+								30	x	4				WCY-ISI	
D.B.12	Bussines modeling in UML (w języku angielskim)	ITT	**20**	**2**	1	2	1	6	+			14	+							20	+	2							WCY-ISI	
D.B.13	Inżynieria wsteczna złośliwego oprogramowania	ITT	**30**	**3**	2	3	1,5	8	+			6	+	16	+								30	+	3				WCY-ISI	
E. Praca dyplomowa			**44**	**23**	23	23	13							500		44										44		23			
E.1	Seminarium dyplomowe		**44**	**3**	3	3	3									44	+									44	+	3	WCY	
E.2	Praca dyplomowa			**20**	20	20	10							500													x	20	WCY	
ogółem godzin / punktów ECTS			**580**	**90**	58	90	39	224		66		178		68		44				228		30	244		30	108		30			
dopuszczalny deficyt punktów ECTS																				10			10			0					
rodzaje i liczba rygorów w semestrze:																				3			4			1					
																				6			5			2					
																				1			2			0					