Opisy przedmiotów dla specjalności *Matematyka w cyberbezpieczeństwie* (MCB) prowadzonej na studiach drugiego stopnia o profilu ogólnoakademickim na kierunku Matematyka prowadzonych na Wydziale Matematyki i Nauk informacyjnych

ALGEBRA W KRYPTOGRAFII		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	30
	Ćwiczenia	30
	Laboratorium	0
	Projekt	0
Treści kształcenia	1. Pierścienie całkowite i ich związki z ciałami. 2. Ideały w pierścieniach. Ideały główne, pierwsze, maksymalne. 3. Ciało ułamków pierścienia całkowitego. 4. Pierścienie Euklidesa. 5. Pierścienie wielomianów o współczynnikach w ciele. Wielomiany rozkładalne i nierozkładalne, pierścienie ilorazowe pierścieni wielomianów, ciało rozkładu wielomianu, ciało algebraicznie domknięte. 6. Rozszerzenia ciał, elementy algebraiczne, rozszerzenia algebraiczne. Charakterystyka ciała. Ciała proste. 7. Ciała skończone. Elementy pierwotne ciała. Podciała ciała skończonego. Reprezentacja elementów w ciałach skończonych. Obliczenia w ciałach skończonych. 8. Wielomiany minimalne, pierwiastki z jedności w ciałach skończonych. 9. Endomorfizm Frobeniousa. Grupa automorfizmów ciała skończonego. 10. Zastosowania ciał skończonych w teorii kodów korekcyjnych, kryptografii i przy projektowaniu eksperymentów.	
Liczba punktów ECTS	5	

TABELA 1. EFEKTY PRZEDMIOTOWE

1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*

Efekty uczenia się dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku *Matematyka*	Odniesienie do efektów kształcenia dla kierunku	Sposób weryfikacji
	WIEDZA		
AK_W01	Zna podstawowe własności i metody konstrukcji ciał skończonych i ich rozszerzeń.	M2MCB_W01	Egzamin pisemny, kolokwia pisemne, aktywność podczas zajęć
AK_W02	Ma wiedzę o zastosowaniach ciał skończonych w obszarze bezpieczeństwa cyfrowego.	M2_W01 M2MCB_W01	Kolokwia pisemne, aktywność podczas zajęć

UMIEJĘTNOŚCI			
AK_U01	Potrafi skonstruować ciała skończone i wykonywać w nich obliczenia.	M2MCB_U02	Egzamin pisemny, kolokwia pisemne, aktywność podczas zajęć
AK_U02	Potrafi zastosować ciała skończone do opisu wybranych zagadnień kryptograficznych.	M2MCB_U04 M2MCB_U03	Egzamin pisemny, kolokwia pisemne, aktywność podczas zajęć
KOMPETENCJE SPOŁECZNE			
AK_K01	Rozumie potrzebę wzbogacania wiedzy przez samokształcenie.	M2MCB_K02	samoocena

ALGEBRA W NAUKACH INFORMACYJNYCH		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	30
	Ćwiczenia	15
	Laboratorium	0
	Projekt	0
Treści kształcenia	1. Algebry abstrakcyjne. - Podalgebry, homomorfizmy i produkty algebr dowolnego typu. - Kongruencje i algebry ilorazowe. Twiedzenia o izomorfizmie. - Termy i równości. Algebry wolne. - Rozmaitości i inne klasy algebr. Twierdzenie Birkhoffa. 2. Półgrupy i monoidy. - Podpółgrupy i podmonoidy. Homomorfizmy i działania na zbiorach. - Półgrupy i monoidy wolne. 3. Quasigrupy i n-quasigrupy. - Izotopie, automorfizmy i grupy przekształceń quasigrup. - Szyfry quasigrupowe. - Kody liniowe oparte o kwadraty łacińskie. - n-arne quasigrupy i n-arne kody quasigrupowe. - Jednostronne quasigrupy i quandle. 4. Półkraty i kraty. - Półkraty i kraty jako zbiory uporządkowane i jako algebry abstrakcyjne. - Kraty rozdzielne. Twierdzenie o reprezentacji (skończonych) krat rozdzielnych. - Kraty zupełne. Twierdzenie Knastera-Tarskiego o punkcie stałym. - Kraty i algebry Boole'a. Wolne algebry Boole'a. Twierdzenie o reprezentacji dla skończonych algebr Boole'a. - Kraty kongruencji. - Algebry relacji.	
Liczba punktów ECTS	3	

TABELA 1. EFEKTY PRZEDMIOTOWE

1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*

ekty uczenia się dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku *Matematyka*	Odniesienie do efektów kształcenia dla kierunku	Sposób weryfikacji
	WIEDZA		
ANI_W01	Ma pogłębioną wiedzę dotyczącą wybranych struktur algebraicznych i ich zastosowań.	M2_W01, M2_W03, M2MCB_W01	Kolokwia pisemne, aktywność podczas zajęć
ANI_W02	Zna podstawowe pojęcia algebry abstrakcyjnej.	M2MCB_W01	Kolokwia pisemne, aktywność podczas zajęć

UMIEJĘTNOŚCI			
ANI_U01	Posiada umiejętność posługiwania się metodami algebraicznymi do opisu i rozwiązywania pewnych problemów z zakresu matematyki stosowanej.	M2MCB_U02	Kolokwia pisemne, aktywność podczas zajęć
ANI_U02	Posiada umiejętność posługiwania się pojęciami algebry abstrakcyjnej w zakresie bezpieczeństwa cyfrowego.	M2MCB_U02	Kolokwia pisemne, aktywność podczas zajęć
ANI_U03	Ma umiejętność dostrzeżenia struktur algebraicznych w innych dziedzinach matematyki.	M2MCB _U03	Kolokwia pisemne, aktywność podczas zajęć
KOMPETENCJE SPOŁECZNE			
ANI_K01	Rozumie potrzebę wzbogacania wiedzy przez samokształcenie.	M2MCB_K02	samoocena

ALGORYTMICZNA TEORIA LICZB	
Status przedmiotu	Obowiązkowy
Treści kształcenia	1. Elementy teorii podzielności, NWD, NWW. Algorytm Euklidesa. Obliczenia w pierścieniu Z_n. 2. Arytmetyka modularna i złożoność działań arytmetycznych. Twierdzenia Eulera i Fermata. Chińskie twierdzenie o resztach. Potęgowanie modularne. 3. Złożoność teorio liczbowych algorytmów. 4. Reszty kwadratowe, symbole Legendre'a i Jacobiego. 5. Wybrane równania diofantyczne i metody ich rozwiazywania. 6. Pierwiastki pierwotne, logarytmy dyskretne, elementy dużego rzędu mod n. 7. Liczby pierwsze i pseudopierwsze. Testy pierwszości. Rozmieszczenie liczb pierwszych. 8. Problem faktoryzacji-algorytmy faktoryzacji. 9. Znajdowanie generatorów w Z_n. 10. Logarytm dyskretny i algorytmy obliczania logarytmów dyskretnych. 11. Funkcje teorio- liczbowe i ich zachowanie asymptotyczne oraz metody obliczania. 12. Algorytm Flouda znajdowania cykli. 13. Sumy kwadratów.
Liczba punktów ECTS	4

TABELA 1. EFEKTY PRZEDMIOTOWE			
1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*			
Efekty uczenia się dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	sposób weryfikacji
WIEDZA			
ATL_W01	Zna podstawowe twierdzenia, metody badawcze oraz algorytmy związane z problemami obliczeniowymi w teorii liczb.	M2_W03 M2MCB_W15 M2MCB_W01	Kolokwium, aktywność na zajęciach
UMIEJĘTNOŚCI			
ATL_U01	Umie rozwiązywać podstawowe problemy obliczeniowej natury w teorii liczb.	M2MCB_U02 M2MCB_U04	Kolokwium, aktywność na zajęciach
KOMPETENCJE SPOŁECZNE			
ATL_K01	Rozumie przydatność nabytej wiedzy umiejętności obliczeniowych do stawiania hipotez oraz z ich weryfikacji w możliwych zastosowaniach w kryptografii.	M2MCB_K02	Kolokwium, aktywność na zajęciach

ALGORYTMY ZAAWANSOWANE		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	30
	Ćwiczenia	0
	Laboratorium	0
	Projekt	15
Treści kształcenia	Algorytmy zachłanne, kody Huffmana, matroidy, programowanie dynamiczne, mnożenie łańcucha macierzy, usuwanie rekursji, algorytmy dziel i zdobywaj, szacowanie złożoności obliczeniowej algorytmów, mnożenie liczb całkowitych, mnożenie macierzy, algorytmy geometrii obliczeniowej, znajdowanie pary najbliższych punktów, konstruowanie domknięcia wypukłego, problem wyszukiwania wzorca, algorytmy aproksymacyjne.	
Metody dydaktyczne	Wykład	
Liczba punktów ECTS	4	

TABELA 1. EFEKTY PRZEDMIOTOWE

1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*

Efekty uczenia się dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	Sposób weryfikacji
	WIEDZA		
AZ_W01	Posiada wiedzę o zaawansowanej algorytmice, strukturach danych i metodach tworzenia algorytmów.	M2_W03, M2MCB_W14	Egzamin
AZ_W02	Posiada szeroką wiedzę w zakresie teorii grafów.	M2MCB_W14	Egzamin
	UMIEJĘTNOŚCI		
AZ_U01	Potrafi projektować wydajne algorytmy i uzasadniać ich poprawność.	M2MCB_U13	Egzamin, Projekt
AZ_U02	Potrafi przeprowadzić analizę czasowej złożoności obliczeniowej algorytmu.	M2MCB_U13	Egzamin, Projekt
AZ_U03	Potrafi wykorzystać wiedzę matematyczną do analizy i optymalizacji rozwiązań informatycznych.	M2MCB_U13	Egzamin, Projekt
	KOMPETENCJE SPOŁECZNE		
AZ_K01	Rozumie przydatność nabytej wiedzy i umiejętności obliczeniowych do stawiania hipotez oraz z ich weryfikacji w możliwych zastosowaniach optymalizacji.	M2MCB_K02	Egzamin, Projekt

KODY KOREKCYJNE I TRANSMISJA DANYCH		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	30
	Ćwiczenia	30
	Laboratorium	0
	Projekt	0
Treści kształcenia	1. Kodowanie w sieciach. Idea modulacji i detekcji. 2. Kody liniowe nad dowolnymi ciałami skończonymi. Ogólne metody kodowania i dekodowania. Kody dualne. Wielkość kodów liniowych. 3. Wybrane metody konstrukcji kodów. 4. Kody doskonałe, ich parametry i związki z kombinatoryką. Kody Hamminga i kody Golay'a. 5. Kody cykliczne jako ideały w odpowiednich pierścieniach ilorazowych. Zera kodów cyklicznych. 6. Kody BCH - kody poprawiające błędy wielokrotne. Binarne kody BCH i metody ich dekodowania - wielomian lokalizacji. 7. Niebinarne kody Reeda-Solomona. 8. Kody liniowe z maksymalną odległością (rozszerzone kody RS). Cykliczne kody MDS. 9. Kody reszt kwadratowych. Dekodowanie permutacyjne. 10. Kody alternujące. Uogólnione kody RS. 11. Kody Goppa w kryptografii. System McEliece z kluczem publicznym.	
Liczba punktów ECTS	4	

TABELA 1. EFEKTY PRZEDMIOTOWE

1. Efekty kształcenia i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*

Efekty kształcenia dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	Sposób weryfikacji
	WIEDZA		
KKO_W01	Zna ogólne zasady określające kodowanie z informacją nadmiarową.	M2_W01 M2_W03	kolokwia pisemne, aktywność podczas zajęć
KKO_W02	Zna algorytmy kodowania i dekodowania dla wybranych kodów liniowych nad ciałami skończonymi.	M2_W03 M2MCB_W01 M2MCB_W03	kolokwia pisemne, aktywność podczas zajęć
	UMIEJĘTNOŚCI		
KKO_U01	Posiada umiejętność posługiwania się algorytmami kodującymi i dekodującymi dla wybranych kodów liniowych.	M2MCB_U02 M2MCB_U03 M2MCB_U04	kolokwia pisemne, aktywność podczas zajęć

KKO_U02	Posiada umiejętność zastosowania kodów korekcyjnych do szyfrowania przesyłanej informacji.	M2MCB_U04	kolokwia pisemne, aktywność podczas zajęć
KOMPETENCJE SPOŁECZNE			
KKO_K01	Rozumie przydatność nabytej wiedzy i umiejętności obliczeniowych do stawiania hipotez oraz z ich weryfikacji w możliwych zastosowaniach w teorii kodowania informacji.	M2MCB_K02	samoocena

METODY FORMALNE I WERYFIKACJA PROTOKOŁÓW KRYPTOGRAFICZNYCH		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	30
	Ćwiczenia	0
	Laboratorium	30
	Projekt	0
Treści kształcenia	1. Logika intuicjonistyczna, logika rachunku zdań, logika pierwszego rzędu: dedukcja naturalna, rachunek sekwentów, eliminacja reguły „cut". 2. (Typowany) rachunek lambda: definicje, własności. Izomorfizm Curriego-Howarda. 3. Wprowadzenie do teorii typów: definicje, własności. 4. Wprowadzenie do programowanie w Agda. 5. Dowodzenie programów w Agda w praktyce, terminacja. 6. Systemy komunikujące się: rachunek CCS, rachunek Pi i ich zastosowania w weryfikacji protokołów kryptograficznych. 7. Wstęp do systemu ProVerif.	
Liczba punktów ECTS	4	

TABELA 1. EFEKTY PRZEDMIOTOWE			
1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku Matematyka			
Efekty uczenia się dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	Sposób weryfikacji
WIEDZA			
MF_W01	Ma pogłębioną wiedzę dotyczącą modeli analitycznych, probabilistycznych, algebraicznych. Ma pogłębioną wiedzę w zakresie wybranych struktur algebraicznych występujących w matematyce i w zastosowaniach w cyberbezpieczeństwie.	M2_W01, M2MCB_W01	Kolokwium, projekt
MF_W02	Ma podstawową wiedzę dotyczącą uwarunkowań badawczych w zakresie modelowania matematycznego i posiada ogólną wiedzę o aktualnych kierunkach rozwoju i najnowszych odkryciach w zakresie matematyki.	M2_W02, M2_W03	Kolokwium, projekt
MF_W03	Zna podstawowe zagadnienia zastosowań metod formalnych w cyberbezpieczeństwie.	M2MCB_W13	Kolokwium, projekt
UMIEJĘTNOŚCI			
MF_U01	Potrafi za pomocą narzędzi metod formalnych zweryfikować poziom bezpieczeństwa systemów cyfrowych.	M2_U04	Kolokwium, projekt
KOMPETENCJE SPOŁECZNE			
MF_K01	Rozumie przydatność nabytej wiedzy i umiejętności obliczeniowych do stawiania hipotez oraz ich weryfikacji w możliwych zastosowaniach.	M2MCB_K02	Projekt

NIEPRZEMIENNE STRUKTURY ALGEBRAICZNE I ICH ZASTOSOWANIA W KRYPTOGRAFII		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	30
	Ćwiczenia	30
	Laboratorium	0
	Projekt	0
Treści kształcenia	Struktura algebry macierzy nad pierścieniem przemiennym. Konstrukcje pierścienie nieprzemiennych i przemiennych, w tym pierścienie grupowe, pierścienie z gradacją. Elementy teorii reprezentacji grup skończonych. Kraty i ich zastosowania w kryptografii. Wybrane schematy kryptograficzne.	
Liczba punktów ECTS	5	

TABELA 1. EFEKTY PRZEDMIOTOWE

1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*

Efekty uczenia się dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	Odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji (P7S_)
	WIEDZA		
NSA_W01	Zna podstawowe fakty dotyczące struktury algebr macierzy nad pierścieniem przemiennym	M2_W01	Kolokwium, egzamin
NSA_W02	Zna obszary kryptografii w których narzędziami są struktury algebraiczne. Zna związki teorii krat z zagadnieniami dotyczącymi kryptografii postkwantowej.	M2_W03, M2MCB_W01	Kolokwium, egzamin
	UMIEJĘTNOŚCI		
NSA_U01	Umie posługiwać się językiem algebraicznym w odniesieniu do zagadnień kryptograficznych.	M2_U01, M2MCB_U02	Kolokwium, egzamin
NSA_U02	Potrafi dostrzec sposób wykorzystania takich struktur algebraicznych jak grupy skończone, macierze czy kraty, w zagadnieniach kryptograficznych.	M2MCB_U03	Kolokwium, egzamin
	KOMPETENCJE SPOŁECZNE		
NSA_K01	Rozumie potrzebę uczenia się przez całe życie.	M2MCB_K02	Kolokwium, egzamin

Opis modułu			
PRACA DYPLOMOWA			
Status przedmiotu	Obowiązkowy		
Formy zajęć i ich wymiar	Wykład	0	
	Ćwiczenia	0	
	Laboratorium	0	
	Projekt	0	
Treści kształcenia	Student wykonujący dyplomową pracę magisterską ma wykazać się pogłębioną znajomością podstawowej wiedzy teoretycznej w dziedzinie matematyki oraz umiejętnością rozwiązywania problemów, wymagających stosowania nowoczesnych metod z zakresu analiz teoretycznych, badawczych, obliczeniowych i eksperymentalnych.		
Liczba punktów ECTS	20		

Efekty uczenia się dla modułu	OPIS EFEKTÓW KSZTAŁCENIA	Odniesienie do efektów kształcenia dla kierunku	Sposób weryfikacji
	WIEDZA		
W2_01	Ma pogłębioną wiedzę z matematyki i kierunków pokrewnych w zakresie tematyki przygotowywanej pracy dyplomowej.	M2_W03 M2MCB_W01	weryfikacja pracy przez promotora, recenzje pracy, ocena obrony pracy dyplomowej
W2_02	Zna zasady etyczne związane z wykonywaniem zawodu matematyka i rozumie konieczność rozważania społecznych skutków technologii informacyjnych.	M2_W04	weryfikacja pracy przez promotora, recenzje pracy, ocena obrony pracy dyplomowej
	UMIEJĘTNOŚCI		
U2_01	Potrafi pozyskiwać informacje z literatury, baz danych oraz innych źródeł, integrować je, dokonywać ich interpretacji oraz wyciągać wnioski i formułować opinie.	M2_U02 M2MCB_U14	obserwacja pracy dyplomanta przez opiekuna,
U2_02	Potrafi opracować szczegółową dokumentację wyników realizacji zadania badawczego oraz potrafi przygotować opracowanie zawierające prezentację i omówienie tych wyników raz poprowadzić dyskusję na ten temat.	M2MCB_U01 M2MCB_U14	obserwacja pracy dyplomanta przez opiekuna,
U2_03	Potrafi integrować wiedzę pochodzącą z wielu dziedzin z uwzględnieniem aspektów pozatechnicznych.	M2MCB_U02 M2MCB_U14	obserwacja pracy dyplomanta przez opiekuna,
	KOMPETECJE SPOŁECZNE		
K2_01	Jest gotów do przestrzegania zasad etyki zawodowej.	M2_K04	obserwacja pracy dyplomanta przez opiekuna,

K2_02	Posiada zdolność do kontynuacji kształcenia oraz świadomość potrzeby samokształcenia w ramach procesu kształcenia ustawicznego (studia III stopnia, studia podyplomowe, kursy i egzaminy przeprowadzane przez uczelnie, firmy i organizacje zawodowe).	M2MCB_K02	obserwacja pracy dyplomanta przez opiekuna,

PROGRAMOWANIE DYSKRETNE PROJEKT		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	0
	Ćwiczenia	0
	Laboratorium	0
	Projekt	15
Treści kształcenia	1. Analiza danego zagadnienia. 2. Stworzenie modelu oraz jego implementacja. 3. Testowanie modelu. 4. Interpretacja otrzymanego wyniku, korekta modelu. 5. Przygotowanie dokumentacji. 6. Prezentacja otrzymanych wyników oraz dyskusja. Modelowane zagadnienia będą z różnych dziedzin zastosowań, głównie przemysłowych takich jak planowanie produkcji, zagadnienie dystrybucji, projektowanie sieci.	
Liczba punktów ECTS	1	

TABELA 1. EFEKTY PRZEDMIOTOWE

1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów uczenia się kierunku *Matematyka*

Efekty uczenia się dla modułu	OPIS EFEKTÓW UCZENIA SIĘ Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów uczenia się dla kierunku	Sposób weryfikacji
	WIEDZA		
WBO_W01	Zna podstawowe metody usprawniania modeli całkowitoliczbowych.	M2_W01 M2_W 02 M2_W04 M2MCB_W12	Sprawozdanie, aktywność
	UMIEJĘTNOŚCI		
WBO_U01	Umie opisać zaawansowane zagadnienia jako model programowania liniowego całkowitoliczbowego i rozwiązać go przy pomocy solvera.	M2_U03 M2MCB_U03 M2MCB_U07 M2MCB_U09 M2MCB_U12 M2MCB_U14	Sprawozdanie, aktywność
WBO_U02	Potrafi dostosować model do możliwości obliczeniowych solvera.	M2_U03 M2MCB_U03 M2MCB_U07 M2MCB_U09 M2MCB_U12 M2MCB_U14	Sprawozdanie, aktywność
	KOMPETENCJE SPOŁECZNE		
WBO_K01	Ma umiejętność pracy w zespole.	M2MCB_K01	Sprawozdanie, aktywność
WBO_K02	Rozumie przydatność nabytej wiedzy i umiejętności obliczeniowych do stawiania hipotez oraz z ich weryfikacji w możliwych zastosowaniach optymalizacji.	M2_K01 M2_K03 M2MCB_K02	Sprawozdanie, aktywność

PROGRAMOWANIE DYSKRETNE		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	15
	Ćwiczenia	15
	Laboratorium	45
	Projekt	
Treści kształcenia	1. Programowanie dyskretne i jego zastosowania. Formułowanie modeli za pomocą zmiennych binarnych. Złożoność obliczeniowa. Unimodularność. Dualność. Zagadnienia mieszane. 2. Metody programowania dyskretnego: metody odcięć, metody podziału i ograniczeń, metody przybliżone. 3. Wybrane zagadnienia programowania dyskretnego: zagadnienia transportowe, problemy najkrótszych dróg, problem komiwojażera, zagadnienia załadunku, zagadnienia lokalizacyjne, wybrane problemy szeregowania zadań. 4. Modelowanie zagadnień praktycznych przy pomocy programowania dyskretnego: Analiza zagadnienia, stworzenie modelu oraz jego implementacja, testowanie modelu, interpretacja otrzymanego wyniku, korekta modelu. przygotowanie dokumentacji, prezentacja otrzymanych wyników oraz dyskusja.	
Liczba punktów ECTS	6	

TABELA 1. EFEKTY PRZEDMIOTOWE

1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*

Efekty uczenia się dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	Sposób weryfikacji
	WIEDZA		
PD_W01	Student posiada wiedzę dotyczącą podstawowych pojęć, metod oraz zastosowań Programowania Dyskretnego.	M2_W01 M2_W02 M2_W04 M2MCB_W12 M2MCB_W14	Aktywność na zajęciach, prace domowe, kolokwia, egzamin
PD_W02	Student posiada wiedzę o wybranych zagadnienia Programowania Dyskretnego.	M2MCB_W14	Aktywność na zajęciach, prace domowe, kolokwia, egzamin
	UMIEJĘTNOŚCI		
PD_U01	Student potrafi korzystać z podstawowych metod Programowania Dyskretnego.	M2MCB_U12, M2MCB_U13	Aktywność na zajęciach, prace domowe, kolokwia, egzamin

PD_U02	Student potrafi rozwiązywać wybrane zagadnienia Programowania Dyskretnego.	M2MCB_U12, M2MCB_U13	Aktywność na zajęciach, prace domowe, kolokwia, egzamin
PD_U03	Student potrafi zidentyfikować zagadnienie Programowania Dyskretnego w rozważanym problemie, zanalizować i rozwiązać problem przy użyciu odpowiednio dobranej metody Programowania Dyskretnego oraz oprogramowania.	M2MCB_U03 M2MCB_U09, M2MCB_U12, M2MCB_U13	Aktywność na zajęciach, prace domowe, kolokwia, egzamin
KOMPETENCJE SPOŁECZNE			
PD_K01	Student rozumie potrzebę pogłębiania wiedzy dotyczącej Programowania Dyskretnego.	M2MCB_K02	Aktywność na zajęciach, prace domowe, kolokwia, egzamin

PROGRAMOWANIE FUNKCYJNE		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	30
	Ćwiczenia	0
	Laboratorium	30
	Projekt	0
Treści kształcenia	1. Podstawowe pojęcia Lambda rachunku i teorii typów 2. Funkcje i ewaluacja w językach funkcyjnych 3. Abstrakcja w językach funkcyjnych 4. Listy w językach funkcyjnych. Rekurencja. 5. Monady i Applicative w Haskellu.	
Liczba punktów ECTS	5	

TABELA 1. EFEKTY PRZEDMIOTOWE			
1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*			
Efekty uczenia się dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	Sposób weryfikacji
WIEDZA			
PF_W01	Ma podstawową wiedzę dotyczącą paradygmatów programowania funkcyjnego.	M2MCB_W11	Projekty na laboratoriach
UMIEJĘTNOŚCI			
PF_U01	Potrafi tworzyć programy używając paradygmatów programowania funkcyjnego w jednym z wybranych języków funkcyjnych.	M2MCB_U11	Projekty na laboratoriach
KOMPETENCJE SPOŁECZNE			
PF_K01	Rozumie przydatność nabytej wiedzy i potrzebę jej pogłębiania.	M2MCB_K02	Projekty na laboratoriach

PROJEKT ZESPOŁOWY		
Status przedmiotu	Obowiązkowy	
Efekty uczenia się	Patrz TABELA 1.	
Formy zajęć i ich wymiar (semestralny)	Wykład	30
	Ćwiczenia	0
	Laboratorium	0
	Projekt	30
Treści kształcenia	1. Cykl życia projektu informatycznego 2. Wyzwania i korzyści płynące z pracy zespołowej 3. Wybrane modele wytwarzania oprogramowania 4. Planowanie i harmonogram projektu 5. Pozyskiwanie i specyfikacja wymagań 6. Elementy UML 7. Zasady tworzenia czystego kodu 8. Narzędzia wspomagające tworzenie kodu 9. Testowanie aplikacji	
Liczba punktów ECTS	4	

TABELA 1. EFEKTY PRZEDMIOTOWE

1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*

Efekty uczenia się dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	Sposób weryfikacji
	WIEDZA		
PZ_W01	Znajomość cyklu życia systemu informatycznego, podstawowych modeli wytwarzania oprogramowania oraz technik wspomagających tworzenie kodu dobrej jakości.	M2MCB_W06	Kolokwium
	UMIEJĘTNOŚCI		
PZ_U01	Umiejętność sporządzania dokumentów dokumentujących lub specyfikujących system informatyczny.	M2_U01 M2_U03 M2MCB_U07 M2MCB_U08	Projekt
PZ_U2	Umiejętność implementacji aplikacji zgodnie z wymagadniami wraz z tworzeniem stosownej dokumentacji funkcjonalnej i technicznej w dowolnym języku programowania wysokiego poziomu.	M2MCB_U13	Projekt
PZ_U03	Umiejętność wykorzystania narzędzi wspomagających estymację, organizację i monitorowanie postępów pracy zespołu nad realizacją projektu.	M2MCB_U08	Projekt
	KOMPETENCJE SPOŁECZNE		
PZ_K01	Umiejętność zarządzania własnym czasem i pracy w zespole.	M2MCB_K01 M2MCB_K02	Sprawozdanie, Projekt

SEMINARIUM		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	-
	Ćwiczenia	30
	Laboratorium	-
	Projekt	-
Treści kształcenia	1. Samodzielna praca nad dyplomem. 2. Przygotowywanie prezentacji. 3. Wygłaszanie referatów.	
Liczba punktów ECTS	2	

TABELA 1. EFEKTY PRZEDMIOTOWE			
1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*			
Efekty uczenia się dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	Sposób weryfikacji
WIEDZA			
SEM_W01	Ma podstawową wiedzę dotyczącą uwarunkowań związanych z działalnością badawczą w zakresie algebry, kombinatoryki i zastosowań matematyki w cyberbezpieczeństwie.	M2_W01-03 M2MCB_W01	Prezentacja, Aktywność
SEM_W02	Zna i rozumie uwarunkowania etyczne i prawne, związane z działalnością naukową, dydaktyczną oraz wdrożeniową.	M2_W04	Prezentacja, Aktywność
UMIEJĘTNOŚCI			
SEM_U01	Potrafi przedstawić wyniki badań w postaci samodzielnie przygotowanego referatu po polsku lub w języku obcym, zawierającego motywację, metody dochodzenia do wyników oraz ich znaczenie na tle innych podobnych wyników.	M2_U01 M2MCB_U01 M2MCB_U14	Prezentacja, Aktywność
SEM_U02	Umie posługiwać się językiem algebraicznym do interpretacji różnych zagadnień.	M2MCB_U02	Prezentacja, Aktywność
KOMPETENCJE SPOŁECZNE			
SEM_K01	Rozumie społeczne aspekty stosowania zdobytej wiedzy, jej przydatność, potrzebę uczenia się przez całe życie i podnoszenia kompetencji zawodowych.	M2_K01 M2MCB_K02	Prezentacja, Aktywność
SEM_K02	Jest gotów do przestrzegania i rozwijania zasad etyki zawodowej oraz działania na rzecz przestrzegania tych zasad.	M2_K04	Prezentacja, Aktywność

SEMINARIUM DYPLOMOWE		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	-
	Ćwiczenia	30
	Laboratorium	-
	Projekt	-
Treści kształcenia	1. Samodzielna praca nad dyplomem. 2. Przygotowywanie prezentacji. 3. Wygłaszanie referatów.	
Liczba punktów ECTS	2	

TABELA 1. EFEKTY PRZEDMIOTOWE

1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*

Efekty uczenia się dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	Sposób weryfikacji
	WIEDZA		
SEM_W01	Ma podstawową wiedzę dotyczącą uwarunkowań związanych z działalnością badawczą w zakresie algebry i kombinatoryki.	M2_W01-03 M2MCB_W01	Prezentacja, Aktywność
SEM_W02	Zna i rozumie uwarunkowania etyczne i prawne, związane z działalnością naukową, dydaktyczną oraz wdrożeniową.	M2_W04	Prezentacja, Aktywność
	UMIEJĘTNOŚCI		
SEM_U01	Potrafi przedstawić wyniki badań w postaci samodzielnie przygotowanego referatu po polsku lub w języku obcym, zawierającego motywację, metody dochodzenia do wyników oraz ich znaczenie na tle innych podobnych wyników.	M2_U01 M2MCB_U01 M2MCB_U14	Prezentacja, Aktywność
SEM_U02	Umie posługiwać się językiem algebraicznym do interpretacji różnych zagadnień.	M2MCB_U02	Prezentacja, Aktywność
	KOMPETENCJE SPOŁECZNE		
SEM_K01	Rozumie społeczne aspekty stosowania zdobytej wiedzy, jej przydatność, potrzebę uczenia się przez całe życie i podnoszenia kompetencji zawodowych.	M2_K01 M2MCB_K02	Prezentacja, Aktywność
SEM_K02	Jest gotów do przestrzegania i rozwijania zasad etyki zawodowej oraz działania na rzecz przestrzegania tych zasad.	M2_K04	Prezentacja, Aktywność

TEORIA AUTOMATÓW I JĘZYKÓW FORMALNYCH		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	30
	Ćwiczenia	15
	Laboratorium	
	Projekt	
Treści kształcenia	1. Wiadomości wstępne - przypomnienie: relacje, indukcja zupełna, języki i gramatyki. 2. Wyrażenia i języki regularne, lemat o pompowaniu, lemat Myhill-Nerode. 3. Gramatyki i języki, gramatyki i języki bezkontekstowe, lemat o pompowaniu, lemat Ogdena. 4. Gramatyki i języki kontekstowe. Gramatyki nieograniczone i języki rekurencyjnie przeliczalne. 5. Maszyny Turinga i ich odmiany, języki rekurencyjnie przeliczalne i rekurencyjne. 6. Automaty liniowo ograniczone i języki kontekstowe. 7. Automaty ze stosem i języki bezkontekstowe. 8. Automaty skończone i języki regularne, twierdzenie Myhill-Nerode. 9. Hierarchia Chomsky'ego języków, uwagi o rozstrzygalności.	
Liczba punktów ECTS	4	

TABELA 1. EFEKTY PRZEDMIOTOWE

1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*

Efekty uczenia się dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów pierwszego / drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	Sposób weryfikacji
	WIEDZA		
TAJF_W01	Zna podstawowe pojęcia teorii automatów: klasy automatów (skończone, ze stosem, maszyny Turinga), obliczenie automatu, język akceptowany, nie determinizm automatów.	M2MCB_W08 M2MCB_W09 M2MCB_W10	Egzamin
TAJF_W02	Zna podstawowe pojęcia lingwistyki matematycznej: gramatyki i ich klasy (regularne, bezkontekstowe, kontekstowe, nieograniczone), języki formalne, hierarchia Chomsky'ego języków (regularne, bezkontekstowe, kontekstowe, rekurencyjnie przeliczalne).	M2MCB_W08 M2MCB_W09 M2MCB_W10	Egzamin
	UMIEJĘTNOŚCI		
TAJF_U01	Potrafi określić przynależność prostych języków do klas hierarchii Chomsky'ego, konstruować automaty odpowiednich klas akceptujące oraz konstruować gramatyki odpowiednich klas generujące proste języki z klas tej hierarchii.	M2MCB _U09	Kolokwium
TAJF_U02	Potrafi wskazać i uzasadnić zależności między klasami automatów, gramatyk i języków.	M2MCB _U09	Kolokwium

TAJF_U03	Potrafi stosować metody teorii automatów i lingwistyki matematycznej do opisu syntaktycznego prostych problemów i struktur wiedzy.	M2MCB _U09	Kolokwium
KOMPETENCJE SPOŁECZNE			
TAJF_KS01	Ma świadomość ograniczeń metod formalizacji syntaktycznej wiedzy, potrafi wyjaśnić różnicę złożoności między problemami i językami formalnymi odpowiednich klas oraz różnicę między językami formalnymi i naturalnymi.	M2MCB _K02	Kolokwium

TEORIA INFORMACJI I PODSTAWY BEZPIECZEŃSTWA CYFROWEGO		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	30
	Ćwiczenia	30
	Laboratorium	0
	Projekt	0
Treści kształcenia	1. Definicja i podstawowe własności entropii zmiennej losowej, entropii łącznej, entropii warunkowej, entropii względnej (odległości informacyjnej Kullbacka-Leiblera) oraz wzajemnej informacji. 2. Rozkłady prawdopodobieństwa o maksymalnej entropii w danej klasie rozkładów. 3. Intensywność entropii procesu stochastycznego z czasem dyskretnym. Wyznaczanie intensywności entropii procesów stacjonarnych. 4. Pojęcie zbioru typowego i asymptotyczna własność równomiernego rozkładu. Zagadnienie bezstratnej kompresji danych. 5. Pojęcie źródła informacji oraz kodu dla źródła informacji. Różne modele źródeł informacji. Przykłady konstruowania kodów dla źródła informacji. Nierówność Krafta. Kody optymalne. Kod Shannona i kod Huffmana. 6. Zastosowanie metod opartych na entropii w kryptografii. Twierdzenie Shannona o tajności doskonałej systemu kryptograficznego. 7. Pojęcie kanału komunikacyjnego. Różne modele kanałów komunikacyjnych. Definicja optymalnego kodu dla kanału. 8. Pojęcie przepustowości kanału komunikacyjnego. Twierdzenie Shannona o kodowaniu dyskretnego kanału oraz łącznym kodowaniu dyskretnego źródła i kanału.	
Liczba punktów ECTS	5	

TABELA 1. EFEKTY PRZEDMIOTOWE			
1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku Matematyka			
ekty uczenia się dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	
WIEDZA			
TIN_W01	zna matematyczne podstawy teorii informacji	M2_W01	Egzamin, kolokwium,
TIN_W02	zna pojęcie oraz własności entropii zmiennej losowej, intensywności entropii procesu stochastycznego, entropii względnej (odległości informacyjnej Kullbacka-Leiblera) i informacji wzajemnej oraz ich zastosowania.	M2MCB_W03 M2MCB_W07	Egzamin, kolokwium,
TIN_W03	zna zastosowania metod opartych na entropii w kryptografii, zna pojęcie tajności doskonałej systemu kryptograficznego i warunki tajności doskonałej.	M2MCB_W07	Egzamin, kolokwium,
TIN_W04	zna pojęcie źródła informacji i kanału komunikacyjnego, zna różne modele źródła i kanału, wie na czym polega kodowanie źródła i kanału.	M2MCB_W07	Egzamin, kolokwium,

TIN_W05	wie czym jest optymalny kod dla źródła i zna sposoby konstrukcji takich kodów, rozumie związek entropii źródła informacji z zagadnieniem bezstratnej kompresji danych, zna pojęcie przepustowości kanału komunikacyjnego, wie czym jest optymalny kod dla kanału, zna twierdzenie o optymalnym kodowaniu źródła i kanału.	M2MCB_W07 M2MCB_W03	Egzamin, kolokwium,
UMIEJĘTNOŚCI			
TIN_U01	umie posługiwać się podstawowymi pojęciami teorii informacji oraz je interpretować.	M2MCB_U10	Egzamin, kolokwium, aktywność
TIN_U02	potrafi wyznaczyć entropię prostych rozkładów dyskretnych i absolutnie ciągłych, wyznaczyć dla tych rozkładów entropię względną oraz informację wzajemną, umie wyznaczać rozkłady prawdopodobieństwa o maksymalnej entropii w danej klasie rozkładów, umie wyznaczyć intensywność entropii stacjonarnego procesu stochastycznego z czasem dyskretnym, w tym łańcucha Markowa.	M2MCB_U10	Egzamin, kolokwium, aktywność
TIN_U03	umie stosować metody oparte na entropii w analizie tajności systemów kryptograficznych.	M2MCB_U10	Egzamin, kolokwium, aktywność
TIN_U04	umie posługiwać się różnymi modelami źródła informacji i kanału komunikacyjnego, w zadanym modelu potrafi wyznaczyć entropię źródła oraz przepustowość kanału.	M2MCB_U09	Egzamin, kolokwium, aktywność
TIN_U05	rozumie ograniczenia bezstratnej kompresji i optymalnego kodowania kanału, potrafi skonstruować optymalny kod dla źródła, umie zbadać istnienie optymalnego kodu o zadanych parametrach, umie stosować twierdzenie o optymalnym kodowaniu źródła i kanału.	M2MCB_U10	Egzamin, kolokwium, aktywność
KOMPETENCJE SPOŁECZNE			
TIN_K01	potrafi współdziałać i pracować w zespole, przyjmując w nim różne role.	M2MCB_K01	prezentacja
TIN_K02	rozumie potrzebę uczenia się przez całe życie, potrafi inspirować i organizować proces uczenia się innych osób.	M2MCB_K02	prezentacja

TEORIA KATEGORII		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	30
	Ćwiczenia	30
	Laboratorium	0
	Projekt	0
Treści kształcenia	1. Kategorie, funktory i naturalne transformacje. 2. Diagramy. Granice i kogranice. 3. Sprzężenia i monady. Kategoria Kleisli. 4. Lemat Yonedy. Twierdzenie o funktorach sprzężonych.	
Liczba punktów ECTS	4	

TABELA 1. EFEKTY PRZEDMIOTOWE

1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*

Efekty kształcenia dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	Sposób weryfikacji
	WIEDZA		
TK_W01	Ma podstawową wiedzę dotyczącą głównych pojęć teorii kategorii (kategorie, (ko)granice, funktory, naturalne transformacje, sprzężenia, monady)	M2_W01, M2MCB_W01, M2MCB_W05	Kolokwia, aktywność
	UMIEJĘTNOŚCI		
TK_U01	Potrafi dostrzec konstrukcje kategoryjne w różnych dziedzinach matematyki i informatyki teoretycznej.	M2MCB_U02, M2MCB_U03, M2MCB_U06	Kolokwia, aktywność
	KOMPETENCJE SPOŁECZNE		
TK_KS01	Rozumie przydatność nabytej wiedzy i umiejętności do stawiania hipotez oraz z ich weryfikacji w możliwych zastosowaniach w teorii kategorii.	M2MCB_K02	Kolokwia, aktywność

TEORIA ZŁOŻONOŚCI		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	30
	Ćwiczenia	15
	Laboratorium	0
	Projekt	0
Treści kształcenia	1. Maszyna Turinga, niedeterminizm 2. Nierozstrzygalność, maszyny Turinga z i bez własności stopu 3. Klasy problemów P i NP 4. Twierdzenie Cooka-Levina, NP-zupełność 5. Redukowalność problemów obliczeniowych 6. ETH i redukcje wielomianowe 7. Inne modele obliczeniowe: RAM, rachunek lambda 8. Złożoność obliczeniowa w teorii liczb i kryptografii 9. Randomizacja 10. Złożoność pamięciowa 11. Sposoby radzenia sobie z problemami trudnymi obliczeniowo	
Liczba punktów ECTS	3	

TABELA 1. EFEKTY PRZEDMIOTOWE

1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*

Efekty uczenia się dla modułu	OPIS E.FEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	Sposób weryfikacji
	WIEDZA		
WCB_W01	Zna podstawowe modele obliczeń i klasy problemów obliczeniowych.	M2MCB_W08	Kolokwium
WCB _W02	Zna założenia teorii złożoności, na których opiera się bezpieczeństwo współczesnych protokołów kryptograficznych.	M2MCB_W08	Kolokwium
	UMIEJĘTNOŚCI		
WCB _U01	Potrafi przeprowadzić redukcję między dwoma problemami obliczeniowymi.	M2MCB_U15	Kolokwium
WCB _U02	Potrafi rozpoznać klasyczne problemy trudne obliczeniowo.	M2MCB_U15	Kolokwium
	KOMPETENCJE SPOŁECZNE		
WCB _K01	Potrafi szukać informacji w literaturze fachowej	M2MCB_K02	Kolokwium

WARSZATY Z MATEMATYCZNYCH METOD CYBERBEZPIECZEŃSTWA		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	0
	Ćwiczenia	0
	Laboratorium	30
	Projekt	15
Treści kształcenia	1. Poznanie środowiska Sage. 2. Analiza danego zagadnienia kryptograficznego, kodowego lub teorio-liczbowego oraz dobór algorytmów. 3. Przygotowanie specyfikacji algorytmu. 4. Stworzenie aplikacji. 5. Testowanie aplikacji. 6. Przygotowanie dokumentacji stworzonej aplikacji. 7. Prezentacja otrzymanych wyników oraz dyskusja.	
Liczba punktów ECTS	3	

TABELA 1. EFEKTY PRZEDMIOTOWE			
1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*			
Efekty kształcenia dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	Sposób weryfikacji
WIEDZA			
WKK_W01	Zna wybrane algorytmy kodowania i dekodowania kodów cyklicznych, oraz podstawowe algorytmy kryptograficzne.	M2_W01-4, M2MCB_W03, M2MCB_W04	Raport pisemny
WKK_W02	Zna podstawowe twierdzenia, metody badawcze oraz algorytmy związane z problemami obliczeniowymi wykorzystywanymi w kryptografii.	M2_W01-4, M2MCB_W15	Raport pisemny
UMIEJĘTNOŚCI			
WKK_U01	Potrafi zaadoptować poznane algorytmy do rozwiązania konkretnego problemu dotyczącego bezbłędnej transmisji danych.	M2_U02-03, M2MCB_U02, M2MCB_U04, M2MCB_U07 M2MCB_U09	Projekt Prezentacja
WKK_U02	Potrafi zaadoptować poznane algorytmy do rozwiązania konkretnego zagadnienia kryptograficznego.	M2_U02-03, M2MCB_U0-4, M2MCB_U07 M2MCB_U09	Projekt Prezentacja
KOMPETENCJE SPOŁECZNE			
WKK_K01	Ma umiejętność pracy w zespole, myślenia w sposób przedsiębiorczy i rozumie społeczne aspekty stosowania zdobytej wiedzy oraz potrzebę jej rozwoju.	M2_K01, M2_K03, M2MCB_K01 M2MCB_K02	Projekt

<table>
<tr><th colspan="3">WPROWADZENIE DO CYBERBEZPIECZEŃSTWA</th></tr>
<tr><td>Status przedmiotu</td><td colspan="2">Obowiązkowy</td></tr>
<tr><td rowspan="4">Formy zajęć i ich wymiar (semestralny)</td><td>Wykład</td><td>30</td></tr>
<tr><td>Ćwiczenia</td><td>0</td></tr>
<tr><td>Laboratorium</td><td>15</td></tr>
<tr><td>Projekt</td><td>0</td></tr>
<tr><td>Treści kształcenia</td><td colspan="2">1. Systemy cyber-fizyczne, cyberprzestrzeń i cyberbezpieczeństwo (2 godz.) Cyberprzestrzeń; sieci, systemy i użytkownicy; systemy cyber-fizyczne; modelowanie systemów; współczesne sieci i systemy; trendy; wprowadzenie do dziedziny cyberbezpieczeństwa; co to znaczy „zajmuję się cyberbezpieczeństwem?”, w kontekście: technicznym, naukowym, biznesowym, prawnym, ekonomicznym; model obszarów cyberbezpieczeństwa – zagadnienia, kompetencje i zawody; cyberbezpieczeństwo a bezpieczeństwo cybernetyczne.
2. Podstawowe zagadnienia z dziedziny cyberbezpieczeństwa (2 godz.) Pojęcia fundamentalne dla dziedziny – CIA (Confidentiality, Integrity, Availability); podatność, zagrożenie, skutek, ryzyko; systemowe podejście do cyberbezpieczeństwa; modelowanie zagrożeń i ocena ryzyka; podejście klasyczne do modelowania zagrożeń; nowe metodyki modelowania i testowania bezpieczeństwa w kontekście Advanced Persisent Threats; wprowadzenie do modelowania bezpieczeństwa cyberprzestrzeni metodyką Kill Chain.
3. Zagrożenia w cyberprzestrzeni – metodyka Kill Chain: Rekonesans (2 godz.) Pozyskiwanie informacji o celach – podejścia, techniki, biały wywiad; wprowadzenie do wyszukiwania podatności (Vulnerability Assesment) sieci i systemów; planowanie ataków – podejścia, techniki, wektory ataku; wpływ ataków; metody in.
4. Zagrożenia w cyberprzestrzeni – metodyka Kill Chain: Techniki przygotowywania ataków i przełamywania zabezpieczeń; dystrybucja malware (2 godz.) Złośliwe oprogramowanie (malware): rodzaje, podstawowe pojęcia, architektura; metody dystrybucji złośliwego oprogramowania, w tym odniesienie do socjotechniki; warsztat analityka malware; wprowadzenie do klasycznych technik detekcji i analizy malware; nowe techniki detekcji i analizy malware; techniki unikania detekcji i utrudniania analizy malware.
5. Zagrożenia w cyberprzestrzeni – metodyka Kill Chain: Eksploitacja systemów, utrzymywanie dostępu i sterowanie atakami (2 godz.) Podstawowe techniki przełamywania zabezpieczeń systemów operacyjnych i systemów komputerowych; przejmowanie kontroli i wykonywanie arbitralnego oprogramowania; techniki utrzymywania złośliwego oprogramowania w systemie; tylne furtki; sieci Malware, czyli botnety: podstawowe pojęcia, elementy, architektura; komunikacja i sterowanie atakami.
6. Zagrożenia w cyberprzestrzeni – metodyka Kill Chain: Ataki – case studies. (2 godz.) Cele atakujących; trendy i case study: ransomware, IoT botnets, cryptojacking, steganografia, botnet-as-a-service; Cyber Warfare; grupy APT i ich metody działania; wpływ społeczno-ekonomiczny ataków w cyberprzestrzeni; prawo a cyberprzestępstwa; etyka a cyberprzestrzępstwa.
7. Metody i środki obrony przed współczesnymi atakami na sieci, systemy i użytkowników: bezpieczeństwo systemów i oprogramowania (4 godz.) Mechanizmy bezpieczeństwa w systemach: uwierzytelnienie, kontrola dostępu; polityki bezpieczeństwa; monitorowanie, utrzymywanie i odzyskiwanie systemów; projektowanie, modelowanie, testowanie, audyt systemów i oprogramowania w kontekście cyberbezpieczeństwa; test penetracyjny, audyt bezpieczeństwa; etapy testu penetracyjnego, techniki i warsztat pentestera; tworzenie raportu z pentestów; Red Teaming, Blue Teaming, Purple Teaming; inżynieria odwrotna.</td></tr>
</table>

	8. **Metody i środki obrony przed współczesnymi atakami na sieci, systemy i użytkowników: bezpieczeństwo danych (4 godz.)** Kryptografia i kryptoanaliza; integralność i autentyczność danych; kontrola dostępu; protokoły bezpiecznej komunikacji; bezpieczeństwo przechowywania danych; prywatność; zastosowanie kryptografii w bezpieczeństwie systemów. 9. **Metody i środki obrony przed współczesnymi atakami na sieci, systemy i użytkowników: bezpieczeństwo komunikacji (2 godz.)** Dobre praktyki zabezpieczenia sieci teleinformatycznych; sprzęt i oprogramowanie dla bezpieczeństwa teleinformatycznego: IDS/IPS, firewall, secure gateways, systemy kontroli dostępu, systemy bezpiecznej łączności; monitoring komunikacji sieciowej; analiza ruchu sieciowego dla cyberbezpieczeństwa; honeypots/honeynets; aplikacje analityczne, systemy SIEM. 10. **Metody i środki obrony przed współczesnymi atakami na sieci, systemy i użytkowników: kryminalistyka cyfrowa (4 godz.)** Pojęcia podstawowe; pozyskiwanie danych śledczych z urządzeń cyfrowych: metody, zabezpieczanie materiału dowodowego, praca z materiałem dowodowym, akwizycja danych; pozyskiwanie danych śledczych jako strumieni komunikacji: kontekst sieci, systemów i użytkowników, przechwytywanie i analiza sieciowych strumieni komunikacji, przechwytywanie i analiza danych cyfrowych; techniki poszukiwań atakujących: biały wywiad, Dark Web, wywiad gospodarczy; Digital Forensics jako element zarządzania cyberbezpieczeństwem; aspekty prawne dochodzenia śledczego z dowodami cyfrowymi; metody kryminalistyki cyfrowej w kontekście prywatnym, compliance, spory prywatne. 11. **Metody i środki obrony przed współczesnymi atakami na sieci, systemy i użytkowników: bezpieczeństwo organizacyjne, społeczne i zarządzanie cyberbepieczeństwem (2 godz.)** Organizacja systemów bezpieczeństwa i zarządzanie incydentami; zarządzanie ryzykiem; strategia i planowanie polityk bezpieczeństwa organizacji; zarządzanie ryzykiem; Threat Intelligence i bezpieczeństwo oparte o analitykę danych; zarządzanie tożsamością użytkowników i systemów; inżyniera społeczna; prywatność zachowania i danych użytkowników; normy w zakresie cyberbezpieczeństwa. 12. **Podsumowanie (2 godz.)** Cyberbezpieczeństwo sieci, systemów i użytkowników jako wielowymiarowy proces; podsumowanie przedmiotu jako analizy bezpieczeństwa cyberprzestrzeni metodyką *Kill Chain*; metody zarządzania obroną przed atakiem typu APT: rodzaje reakcji na poszczególne ataki, formułowanie strategii koncentrującej się na coraz wcześniejszym przerywaniu łańcucha; orientacja rozwoju kompetencji inżyniera cyberbezpieczeństwa na kierunku Cyberbezpieczeństwo. Zakres laboratorium: 1. Podstawy systemów operacyjnych i sieci teleinformatycznych 2. Pozyskiwanie informacji: rekonesans, skanowanie, 3. Testowanie bezpieczeństwa danych, aplikacji i systemów z wykorzystaniem specjalistycznych narzędzi. 4. Podstawy bezpieczeństwa systemów i oprogramowania 5. Wykorzystanie wirtualnej sieci komputerowej do wykonania ćwiczeń związanych zapewnianiem bezpieczeństwa cyberprzestrzeni. Realizacja zadania będzie obejmowała monitorowanie sieci i systemów, implementację mechanizmów bezpieczeństwa sieci i systemów oraz modelowania i symulowania zagrożeń w celu przetestowania wprowadzonych mechanizmów i zebrania dowodów wykonania ataków.
Liczba punktów ECTS	4

TABELA 1. EFEKTY PRZEDMIOTOWE			
1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*			
Efekty uczenia się dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	Sposób weryfikacji
WIEDZA			
WCB_W01	Ma wiedzę dotyczącą fundamentalnych pojęć z zakresu cyberbezpieczeństwa.	M2MCB_W02 , M2_W04	Kolokwium pisemne
WCB_W02	Ma wiedzę z zakresu mechanizmów stosowanych w złośliwym oprogramowaniu i sieciach botnet.	M2MCB_W02	Kolokwium pisemne
WCB_W03	Ma podstawową wiedzę z zakresu testów penetracyjnych.	M2MCB_W02	Kolokwium pisemne, zajęcia laboratoryjne
WCB_W04	Ma podstawową wiedzę z zakresu kryminalistyki cyfrowej.	M2MCB_W02	Kolokwium pisemne
WCB_W05	Ma podstawową wiedzę z obszaru środków technicznych zapewniających cyberbezpieczeństwo sieci, systemów i użytkowników.	M2MCB_W02	Kolokwium pisemne, zajęcia laboratoryjne
WCB_W06	Ma podstawową wiedzę z obszaru bezpieczeństwa komunikacji w sieciach teleinformatycznych.	M2MCB_W02	Kolokwium pisemne, zajęcia laboratoryjne
WCB_W07	Ma podstawową wiedzę z zakresu modelowania zagrożeń w cyberprzestrzeni.	M2MCB_W02	Kolokwium pisemne, zajęcia laboratoryjne
WCB_W08	Ma podstawową wiedzę z zakresu zarządzania cyberbezpieczeństwem i aspektów społecznych w cyberprzestrzeni.	M2MCB_W02 , M2_W04	Kolokwium pisemne
UMIEJĘTNOŚCI			
WCB_U01	Potrafi przygotować środowisko pracy badacza cyberbezpieczeństwa systemów i sieci.	M2MCB_U05	Zajęcia laboratoryjne, sprawozdanie
WCB_U02	Potrafi przeprowadzić podstawowy test bezpieczeństwa zgodnie z przyjętą metodyką.	M2MCB_U05	Zajęcia laboratoryjne, sprawozdanie
WCB_U03	Potrafi stworzyć dokumentację z testów bezpieczeństwa zgodnie z przyjętą metodyką i wymaganiami.	M2MCB_U05	Zajęcia laboratoryjne, sprawozdanie
WCB_U04	Potrafi modelować zagrożenia w cyberprzestrzeni zgodnie z metodyką Cyber Kill Chain	M2MCB_U05	Zajęcia laboratoryjne, sprawozdanie
WCB_U05	Potrafi stosować środki techniczne zapewniające cyberbezpieczeństwo sieci, systemów i użytkowników.	M2MCB_U05	Zajęcia laboratoryjne, sprawozdanie
WCB_U06	Potrafi skonfigurować i zabezpieczyć system końcowy lub oprogramowanie przed zagrożeniami w cyberprzestrzeni.	M2MCB_U05	Zajęcia laboratoryjne, sprawozdanie

WCB_U07	Potrafi zweryfikować w podstawowym zakresie czy system końcowy lub oprogramowanie mogą być zagrożone cyberatakami.	M2MCB_U05	Zajęcia laboratoryjne, sprawozdanie
WCB_U08	Potrafi w podstawowym zakresie przeprowadzić analizę zdarzeń w sieci i systemach w kierunku odkrycia niepożądanych akcji i anomalii.	M2MCB_U05	Zajęcia laboratoryjne, sprawozdanie
WCB_U09	Potrafi rozwiązywać zadania formułowane na bieżąco, komunikować wnioski i opinie, prowadzić na ich temat dyskusję i przekonywać innych.	M2MCB_U05, M2_W04	Zajęcia laboratoryjne, sprawozdanie, prezentacja
WCB_U10	Potrafi przygotować i przeprowadzić prezentację dotyczącą zagadnień technicznych związanych z problemem rozwiązywanym na bieżąco.	M2MCB_U05, M2_W04	Zajęcia laboratoryjne, sprawozdanie, prezentacja
WCB_U11	Potrafi krytycznie analizować dostępną literaturę z zakresu domeny wiedzy.	M2MCB_U05, M2_W04	Zajęcia laboratoryjne, sprawozdanie, prezentacja
KOMPETENCJE SPOŁECZNE			
WCB_K01	Ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy.	M2MCB_K01	Zajęcia laboratoryjne, wykład
WCB_K02	Ma orientację zawodową w obszarze inżynierii cyberbezpieczeństwa i jest świadomy procesu uczenia się w kierunku zwiększania kompetencji w tym obszarze.	M2_W04, M2_K01, M2_K03	Zajęcia laboratoryjne, wykład
WCB_K03	Ma świadomość uwarunkowań etycznych i prawnych związanych z działalnością naukową, dydaktyczną, wdrożeniową i biznesową.	M2_K04	Zajęcia laboratoryjne, wykład

WPROWADZENIE DO WSPÓŁCZENEJ KRYPTOLOGII		
Status przedmiotu	Obowiązkowy	
Formy zajęć i ich wymiar (semestralny)	Wykład	30
	Ćwiczenia	15
	Laboratorium	-
	Projekt	-
Treści kształcenia	1. Systemy kryptograficzne. Podstawowe pojęcia kryptografii i kryptoanalizy. 2. Bezpieczeństwo kryptograficzne (oszacowanie, uzyskiwanie i dowodzenie bezpieczeństwa; rodzaje ataków): a. Idealne szyfrowanie - szyfry z kluczem jednorazowym. b. Generatory kluczy - podkreślenie znaczenia entropii. 3. Szyfrowanie kluczem prywatnym (symetryczne): a. Tryby szyfrowania. b. Szyfry blokowe: DES, AES (implementacje, bezpieczeństwo). c. Szyfry strumieniowe. 4. Funkcje skrótu. 5. Szyfrowanie uwierzytelnione (algorytmy chroniące poufność i autentyczność), MAC. 6. Szyfrowanie kluczem publicznym (asymetryczne). Uzgodnienie klucza (Diffie-Hellman). 7. Podpis cyfrowy (RSA i DSA). 8. Zastosowanie krzywych eliptycznych. 9. Protokół SSL/TLS. 10. Protokoły kryptograficzne: inne i weryfikacja poprawności. 11. Kryptografia postkwantowa (informacyjnie: algorytm Shora; kryptografia na kratach).	
Liczba punktów ECTS	4	

TABELA 1. EFEKTY PRZEDMIOTOWE

1. Efekty uczenia się i ich odniesienie do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji oraz efektów kształcenia kierunku *Matematyka*

Efekty uczenia się dla modułu	OPIS EFEKTÓW KSZTAŁCENIA Absolwent studiów drugiego stopnia na kierunku Matematyka	Odniesienie do efektów kształcenia dla kierunku	sposób weryfikacji
	WIEDZA		
WWK_W01	Ma wiedze o formalnych podstawach kryptologii i uwarunkowań modeli kryptologicznych.	M2_W01 M2_W02 M2_W03 M2_W04 M2MCB_W01 M2MCB_W04	Kolokwium,
WWK_W02	Ma wiedzę o aktualnych metodach oceny bezpieczeństwa algorytmów i protokołów kryptograficznych wykorzystujących modelowanie matematyczne.	M2_W01 M2_W02 M2_W03 M2_W04 M2MCB_W01 M2MCB_W04	Kolokwium

WWK_W03	Ma wiedzę w zakresie zastosowania struktur algebraicznych w konstrukcji algorytmów i protokołów kryptograficznych.	M2_W01 M2_W02 M2_W03 M2_W04 M2MCB_W01 M2MCB_W04	Kolokwium
WWK_W04	Ma wiedzę o nowoczesnych kierunkach rozwoju kryptologii.	M2_W03	Kolokwium
UMIEJĘTNOŚCI			
WWK_U01	Potrafi ocenić bezpieczeństwo podstawowych prymitywów kryptograficznych.	M2MCB_U03 M2MCB_U04	Kolokwium, Sprawozdanie
WWK_U02	Potrafi budować i stosować modele matematyczne w ocenie bezpieczeństwa algorytmów i protokołów kryptograficznych.	M2MCB_U03 M2MCB_U04	Kolokwium, Sprawozdanie
KOMPETENCJE SPOŁECZNE			
WWK_K01	Rozumie przydatność i znaczenie nabytej wiedzy w obszarze bezpieczeństwa cyfrowego oraz jego znaczenie społeczne.	M2MCB_K02	Sprawozdanie