PROGRAM STUDIÓW - Część B

1. *Nazwa kierunku: matematyka, specjalność: bezpieczeństwo informacji*
2. *Poziom kształcenia: studia pierwszego stopnia*
3. *Profil kształcenia: ogólnoakademicki*

TREŚCI PROGRAMOWE MODUŁÓW

MK_1: Ochrona własności intelektualnej i elementy BHP

Zapoznanie się z ustawą o prawie autorskim i prawach pokrewnych. Prawo autorskie w systemie własności intelektualnej. Utwór jako przedmiot prawa autorskiego. Twórca utworu i jego prawa autorskie. Obrót prawami autorskimi. Utwory naukowe. Szczególne regulacje ochrony autorskoprawnej. Prawo autorskie w technologiach cyfrowych. Prawo pokrewne, ochrona wizerunku, adresata korespondencji i tajemnicy źródeł informacji. Skutki naruszenia praw autorskich.

MK_2: Elementy historii matematyki starożytnej/nowożytnej. Do wyboru 1 przedmiot(y) spośród jak niżej.

MK_2/I - Elementy historii matematyki starożytnej: Wybrane zagadnienia z uwzględnieniem uniwersalności matematyki jako nauki (Egipt, Babilon, Grecja, Rzym, Chiny, Indie w starożytności).

MK_2/II - Elementy historii matematyki nowożytnej: Wybrane zagadnienia z uwzględnieniem uniwersalności matematyki jako nauki (Europa, Chiny, Indie, kraje islamu w średniowieczu).

MK_3: Lektorat j.obcego (bez egzaminu)

Wybrane zagadnienia z języka obcego ogólnego, które umożliwią studentom swobodne funkcjonowanie w rzeczywistości obcojęzycznej, wybrane zagadnienia z języka obcego matematycznego takie jak np. podstawowe działania matematyczne, podstawowe pojęcia z algebry, geometrii płaskiej i przestrzennej, trygonometrii.

MK_4: Lektorat j.obcego (z egzaminem)

Wybrane zagadnienia z języka obcego ogólnego, które umożliwią studentom swobodne funkcjonowanie w rzeczywistości obcojęzycznej, wybrane zagadnienia z języka obcego matematycznego takie jak np. podstawowe działania matematyczne, podstawowe pojęcia z algebry, geometrii płaskiej i przestrzennej, trygonometrii.

MK_5: Wychowanie fizyczne

Zasady BHP na zajęciach wychowania fizycznego, regulamin korzystania z obiektu sportowego. Nauka podstawowych elementów technicznych i taktycznych. Wykształcenie wśród studentów potrzeby dbałości o kondycję fizyczną oraz wsparcie rozwoju kompetencji społecznych dotyczących współpracy grupowej.

MK_6: Wstęp do matematyki

Elementarna teoria mnogości (zbiory, relacje, funkcje, zasadnicze ich typy i operacje na nich). Moce zbiorów, typy porządkowe, Twierdzenie Zermelo i lemat Kuratowskiego-Zorna.

MK_7: Algebra liniowa I

Pojęcie ciała. Ciało liczb zespolonych, postacie algebraiczna i trygonometryczna liczb zespolonych, wzór de Moivre'a, interpretacja geometryczna liczb zespolonych. Układy równań liniowych, metoda eliminacji Gaussa rozwiązywania układów równań liniowych, wzory Cramera. Wyznaczniki i ich własności, rozwinięcie Laplace'a. Algebra macierzy, operacje na macierzach, odwracanie macierzy, rząd macierzy. Przestrzenie liniowe, baza i wymiar przestrzeni liniowych, suma prosta podprzestrzeni, przestrzeń ilorazowa.

MK_8: Algebra liniowa II

Przekształcenia liniowe, macierz przekształceń liniowych, wektory i wartości własne endomorfizmów liniowych, podprzestrzenie niezmiennicze, macierz i baza Jordana, twierdzenie Jordana. Przestrzeń sprzężona, przekształcenia sprzężone. Formy kwadratowe, metoda Lagrange'a sprowadzania form kwadratowych do postaci kanonicznej, rzeczywiste formy kwadratowe. Funkcjonały dwuliniowe, przestrzenie ortogonalne, przestrzenie euklidesowe, suma prostopadła podprzestrzeni, baza prostopadła, ortogonalizacja Schmidta.

MK_9: Analiza matematyczna I

Elementy logiki i teorii mnogości. Funkcja jako relacja. Ciągi liczbowe i ich granice. Szeregi liczbowe. Zbieżność bezwzględna i warunkowa. Liczba e. Przestrzenie metryczne. Funkcje rzeczywiste jednej zmiennej i jej własności.

MK_10: Analiza matematyczna II

Rachunek różniczkowy i całkowy funkcji jednej zmiennej rzeczywistej. Badanie przebiegu zmienności funkcji. Ciągi i szeregi funkcyjne i ich własności.

MK_11: Analiza matematyczna III

Rachunek różniczkowy i całkowy funkcji wielu zmiennych. Funkcje uwikłane. Ekstrema warunkowe. Twierdzenie o odwzorowaniu odwrotnym.

MK_12: Elementarna teoria liczb

Podstawowe własności relacji podzielności liczb całkowitych. Wyznaczanie rozkładu kanonicznego liczb naturalnych, całkowitych i wymiernych. Wyznaczanie najmniejszej wspólnej wielokrotności i największego wspólnego dzielnika liczb całkowitych. Rozwiązywanie liniowych równań diofantycznych. Arytmetyka modularna i jej zastosowania. Rozwiązywanie kongruencji. Chińskie twierdzenie o resztach. Symbol Legendre'a i jego zastosowania. Przedstawianie liczb rzeczywistych w postaci ułamków łańcuchowych. Obliczanie wartości podstawowych funkcji arytmetycznych.

MK_13: Algebra I

Grupy i ich przykłady, podgrupy; grupy cykliczne; warstwy, dzielniki normalne, grupy ilorazowe; homomorfizmy grup i ich zastosowania; grupy permutacji. Pierścienie i ich przykłady, podpierścienie; elementy odwracalne i dzielniki zera; ideały (główne, pierwsze i maksymalne); pierścienie ilorazowe; homomorfizmy pierścieni i ich zastosowania; pierścienie wielomianów; dziedziny ideałów głównych; dziedziny z jednoznacznością rozkładu. Ciała i ich własności; ciało ułamków; rozszerzenia algebraiczne ciał.

MK_14: Kombinatoryka

Schematy wyboru (wariacje z i bez powtórzeń, permutacje, kombinacje bez i z powtórzeniami). Tożsamości kombinatoryczne. Zasada włączania i wyłączania. Równania rekurencyjne i funkcje tworzące. Wybory z ograniczeniami. Podziały zbiorów oraz liczby Stirlinga. Podziały liczb.

MK_15: Metody numeryczne

Teoria błędów. Zagadnienie interpolacji. Zjawisko Rungego. Obliczanie wartości wielomianu algebraicznego - schemat Hornera. Zagadnienie aproksymacji. Aproksymacja średniokwadratowa integralna i punktowa. Aproksymacja funkcjami ortogonalnymi. Różniczkowanie numeryczne. Całkowanie numeryczne. Przybliżone rozwiązywanie równań nieliniowych. Rozwiązywanie układów równań liniowych.

MK_16: Topologia

Pojęcie ogólnej przestrzeni topologicznej (zbiory otwarte i domknięte, podprzestrzeń topologiczna, operacje wnętrza i domknięcia, zbieżność ciągów, aksjomaty oddzielania). Sposoby określania topologii, topologia wyznaczana przez metrykę. Aksjomaty przeliczalności. Przekształcenia ciągłe. Zwartość. Wybrane własności przestrzeni metrycznych (całkowita ograniczoność, zupełność, twierdzenie Banacha o odwzorowaniu zwężającym, twierdzenie Baire'a, zwartość ciągowa i pokryciowa). Spójność (definicja i własności zbiorów spójnych). Przestrzenie normalne (definicja i podstawowe własności).

MK_17: Rachunek prawdopodobieństwa I

Przestrzeń probabilistyczna. Prawdopodobieństwo warunkowe. Niezależność zdarzeń. Schematy rachunku prawdopodobieństwa. Zmienne losowe i ich rozkłady oraz parametry liczbowe. Niezależność zmiennych losowych. Zbieżność ciagów zmiennych losowych. Prawa wielkich liczb. Centralne twierdzenia graniczne.

MK_18: Równania różniczkowe

Podstawowe pojęcia i twierdzenia teorii równań różniczkowych zwyczajnych oraz metody rozwiązywania różnych typów tych równań. Rozwiązanie ogólne, szczególne, osobliwe. Zagadnienie początkowe. Interpretacja geometryczna. Równania rzędu I rozwiązywalne względem pochodnej: równania o zmiennych rozdzielonych, zupełne, liniowe, Bernoulliego, Riccatiego. Podstawowe twierdzenia o istnieniu i jednoznaczności rozwiązania zagadnienia Cauchy'ego. Równania liniowe wyższych rzędów. Układy równań różniczkowych. Dowód istnienia i jednoznaczności rozwiązań zagadnienia początkowego dla normalnego układu równań różniczkowych. Układy liniowe, macierz fundamentalna rozwiązań. Wzór Liouville'a. Układy liniowe o stałych współczynnikach.

MK_19: Statystyka matematyczna

Elementy statystyki opisowej. Rozkłady wybranych statystyk z próby. Estymatory i ich własności. Metody konstrukcji estymatorów. Estymacja punktowa i przedziałowa. Weryfikacja hipotez. Testy parametryczne i nieparametryczne. Model regresji liniowej. Elementy analizy szeregów czasowych.

MK_20: Wprowadzenie do teorii grafów

Grafy. Drogi i cykle. Grafy eulerowskie. Grafy hamiltonowskie. Proste zastosowania grafów: zagadnienie najkrótszej drogi, zadanie chińskiego listonosza, problem komiwojażera. Drzewa. Zliczanie drzew oznakowanych. Problem najkrótszych połączeń.

MK_21: Teoria grafów - analiza sieci

Grafy i digrafy. Spójność, zbiory rozspajające. Drogi i cykle. Sieci i przepustowość. Przepływy w sieciach. Przekroje i ich przepustowość. Twierdzenie o maksymalnym przepływie i minimalnym przekroju.

MK_22: Elementy kryptografii i teorii kodowania

Podzielność i reprezentacja liczb całkowitych, systemy liczbowe. Rozszerzony algorytm Euklidesa. Kongruencje i elementy odwrotne w pierscieniu Z/mZ, efektywny algorytm obliczania potęg w pierscieniu Z/mZ. Układy kongruencji liniowych: metody rozwiązywania. Systemy kryptograficzne symetryczne i asymetryczne: szyfry podstawieniowe, przestawieniowe, afiniczne, Vigenera, Hilla, szyfr RSA. Szukanie błędów, poprawianie, kodowanie i dekodowanie informacji.

MK_23: Kryptografia stosowana - projektowanie szyfrów

Ogólny zarys bezpieczeństwa komputerowego. Efektywna implementacja m. in. arytmetyka liczb całkowitych wielokrotnej precyzji, arytmetyka modularna liczb wielokrotnej precyzji, algorytmy obliczania największego wspólnego dzielnika. Nowoczesne algorytmy szyfrowania symetrycznego. Szyfry blokowe: szyfr DES, kryptoanaliza różnicowa i kryptoanaliza liniowa, zasady projektowania szyfrów blokowych, szyfry Feisela, szyfr AES; Tryby operacyjne szyfrów blokowych. Efektywna implementacja m. in. arytmetyka liczb całkowitych wielokrotnej precyzji, arytmetyka modularna liczb wielokrotnej precyzji, algorytmy obliczania największego wspólnego dzielnika.

MK_24: Algebra relacyjna i relacyjne bazy danych

Algebra relacyjna jako teoretyczny model do opisu semantyki relacyjnych baz danych. Relacyjne bazy danych i język SQL. Normalizacja i denormalizacja. Implementacje i interfejsy programistyczne.

MK_25: Ryzyko procesów informacyjnych

Niepewność a ryzyko. Klasyfikacje i analiza ryzyka. Zarządzanie ryzykiem. Matematyczne miary ryzyka. Monitorowanie zmienności i korelacji. Procesy informacyjne. Ryzyko procesów informacyjnych jako część ryzyka operacyjnego. Ryzyko oszustw (wewnętrznych i zewnętrznych). Tworzenie rezerw. Ryzyko modelu. Zaburzenia, luki i błędy w przekazie informacji. Teoria wartości ekstremalnych, prawo potęgowe i rozkład Pareto. Doprecyzowanie szacunków ryzyka. Zasada "racjonalnej ignorancji" w pozyskiwaniu informacji. Modele niekompletnej informacji. Informacja probabilistyczna.

MK_26: Pracownia programowania I: wstęp do programowania

Praca z kompilatorem na przykładzie C/Pascal oraz z interpreterem na przykładzie Perl. Struktura programu w językach C/Pascal/Perl/Maxima. Typy danych: całkowite, rzeczywiste, wyliczeniowe, łańcuchy i tablice, rekordy i struktury. Wskaźniki i operacje na wskaźnikach. Instrukcje proste, warunkowe, pętle. Funkcje, przekazywanie parametrów i zwracanie wartości. Instrukcje wejścia/wyjścia, praca z plikami. Wyrażenia regularne w Perlu. Proste obliczenia symboliczne, programowanie i graficzna wizualizacja wyników w Maxima.

MK_27: Pracownia programowania II. Do wyboru 1 przedmiot(y) spośród jak niżej.

MK_27/2 - Wstęp do programowania w R: Składnia i semantyka typowych języków programowania wysokiego poziomu. Strukturalizacja zagadnień programistycznych. Obiekty, ich własności i metody.

MK_27/1 - Wstęp do programowania w php: Hipertekst, SGML, HTML i MathML. Prezentacja i CSS. Strukturalizacja danych: XML i XHTML. Skrypty Javascript. Programowalne generowanie stron internetowych i budowa aplikacji webowych. Obiektowy język programowania PHP.

MK_28: Proseminarium matematyki elementarnej

Podstawowe pojęcia rachunku zdań. Twierdzenie o rozkładzie liczby naturalnej na czynniki pierwsze. Wyrażenia algebraiczne. Wartość bezwzględna. Potęgi o wykładniku niewymiernym. Logarytmy-własności. Równania i nierówności wykładnicze i logarytmiczne. Dzielenie wielomianów. Funkcje-własności. Dwumian Newtona. Miara łukowa kąta. Funkcje trygonometryczne. Wzory redukcyjne. Ciągi. Suma szeregu geometrycznego. Przykłady przekształceń geometrycznych: obrót, odbicie. Wielościany foremne. Twierdzenie o okręgu wpisanym w czworokąt i okręgu opisanym na czworokącie. Równanie okręgu. Kombinatoryka Prawdopodobieństwo warunkowe, prawdopodobieństwo całkowite. Niezależność zdarzeń. Schemat Bernoulliego.

MK_29: Seminarium dyplomowe I

Treści zgodne z tematami przygotowywanych prac licencjackich na dany rok akademicki.

MK_30: Seminarium dyplomowe II

Treści zgodne z tematami przygotowywanych prac licencjackich na dany rok akademicki.

MK_31: Pracownia dyplomowa

Treści dostosowane do tematyki realizowanych prac licencjackich w danym roku akademickim - uzasadnienie tematu pracy, opis aktualnego stanu wiedzy, przedstawienie wyników badań.

MK_32: Wykład fakultatywny I (bez egzaminu). Do wyboru 1 przedmiot(y) spośród jak niżej.

MK_32/1 - Elementy kryptologii kwantowej: Matematyczne podstawy mechaniki kwantowej. Informacja kwantowa. Jednostka informacji kwantowej - kubit. Układy kubitów, stany mieszane, kwantowe splątanie, stany Bella. Bramki kwantowe. Kwantowa transformata Fouriera i jej zastosowania. Gęste kodowanie, teleportacja kwantowa. Algorytmy kwantowe: Shora, Grovera. Komunikacja kwantowa. Polaryzacja optyczna i jej rola w kodowaniu informacji. Protokół BB84. Protokoły kwantowej dystrybucji klucza. Prywatność i informacja koherentna. Bezpieczeństwo informacji kwantowej. Przesył informacji klasycznej poprzez kanał kwantowy. Atak kolektywny w kryptografii kwantowej.

MK_F - Inny, zgłoszony na dany semestr: treści specyficzne dla zgłaszanego i wybranego przedmiotu na dany rok akademicki.

MK_33: Wykład fakultatywny II (z egzaminem). Do wyboru 1 przedmiot(y) spośród jak niżej.

MK_33/1 - Wzorce w ciągach niezależnych zmiennych losowych: Funkcje generujące prawdopodobieństwa. Momenty stopu. Średnie czasy oczekiwania na wybrane wzorce w ciągach niezależnych zmiennych losowych w ujęciu kombinatorycznym. Zagadnienia konkurujących wzorców. Wyznaczanie prawdopodobieństw pojawień się danego wzorca przed innymi. Elementy teorii martyngałów z czasem dyskretnym. Zastosowanie teorii martyngałów do zagadnień związanych z pojawianiem się wzorców. Elementy scan statistic.

MK_F - Inny, zgłoszony na dany semestr: treści specyficzne dla zgłaszanego i wybranego przedmiotu na dany rok akademicki.

MK_34: Wykład fakultatywny III (z egzaminem). Do wyboru 1 przedmiot(y) spośród jak niżej.

MK_34/1 - Krzywe eliptyczne: Równanie Weierstrassa krzywej eliptycznej. Dodawanie punktów na krzywej eliptycznej. Przestrzenie rzutowe i punkty w nieskończoności, tw. Pascala, tw. Pappusa. Układy współrzędnych rzutowych, Jacobianowych, Edwardsa. Punkty torsyjne krzywych eliptycznych i ich parowania: Weila i Tate-Lichtenbauma. Krzywe eliptyczne nad ciałami skończonymi. Rząd grupy punktów krzywej. Algorytm Schoof'sa. Krzywe superosobliwe. Systemy kryptograficzne oparte na krzywych eliptycznych.

MK_F - Inny, zgłoszony na dany semestr: treści specyficzne dla zgłaszanego i wybranego przedmiotu na dany rok akademicki.

MK_35: Zastosowanie matematyki w nowoczesnych technologiach. Do wyboru 1 przedmiot(y) spośród jak niżej.

MK_35/1 - Matematyczne podstawy grafiki komputerowej: Reprezentacje obiektów geometrycznych. Macierzowa reprezentacja przekształceń geometrycznych. Przekształcenia afiniczne. Liczby zespolone, kwaterniony i ich zastosowanie w grafice komputerowej. Reprezentacje krzywych i powierzchni. Interpolacja.

MK_35/2 - Matematyczne podstawy kompresji danych: Kompresja stratna i bezstratna, stopnie kompresji. Kompresja w przechowywaniu i transmisji danych. Kodowanie Huffmana, arytmetyczne, słownikowe i predykcyjne. Miary jakości i zniekształceń. Zagadnienia kompresji obrazu i dźwięku.

MK_F - Inny, zgłoszony na dany semestr: treści specyficzne dla zgłaszanego i wybranego przedmiotu na dany rok akademicki.

MK_36: Wiarygodność informacji. Do wyboru 1 przedmiot(y) spośród jak niżej.

MK_36/1 - Algebraiczne aspekty teorii kodowania: Kody liniowe i ich reprezentacje macierzowe: macierze generujące i macierze kontroli parzystości; kodowanie, dekodowanie za pomocą kodów liniowych: metoda lidera warstwy i metoda syndromu, kody dualne. Kody doskonałe: kody Hamminga i Golaya. Kody wielomianowe.Kody cykliczne: wielomianowa reprezentacja kodów cyklicznych, wielomiany generujące, macierze generujące i macierze kontroli parzystości, algorytm dekodowania. Szczególne rodzaje kodów cyklicznych: np. kody BCH - kody poprawiające błędy wielokrotne: algorytm dekodowania.

MK_36/2 - Koncepcje i metody bezpiecznej komunikacji: Zastosowania kryptograficznych funkcji skrótu, wymagania stawiane funkcjom skrótu, własności funkcji skrótu wymagane w szczególnych zastosowaniach,funkcje jednokierunkowe i funkcje kompresujące, Funkcje skrótu bez klucza i z kluczem, cele bezpieczeństwa, metody ataku na funkcje skrótu m. in. metodą dnia urodzin i ataki wykorzystujące własności podstawowego szyfru. Integralność danych i uwierzytelnianie wiadomości: funkcje wykorzystywane do uwierzytelnienia komunikatów, wymagania stawiane kodom uwierzytelniania komunikatów, bezpieczeństwo kodów uwierzytelniania komunikatów.

MK_37: Ryzyko i zarządzanie informacją. Do wyboru 1 przedmiot(y) spośród jak niżej.

MK_37/1 - Modelowanie zagrożeń i zabezpieczeń systemów przetwarzania informacji: Projektowania systemów przetwarzania danych z hierarchią poziomów dostępu oraz granulacją wrażliwości informacji. Metodologia STRIDE i ASF. Ocena i kategoryzacja zagrożeń oraz ryzyka: model standardowy i DREAD. Przedstawienie zasad oraz technik identyfikacji i oceny zagrożeń systemów przetwarzania danych oraz wyznaczania przeciwdziałań i minimalizacji ryzyka.

MK_37/2 - Teoria gier w zarządzaniu ryzykiem informacyjnym: Podział i klasyfikacja gier.Gry niekooperacyjne w postaci normalnej. Gry o sumie zerowej: strategie minimaksowe i maksiminowe, poziom bezpieczeństwa. Twierdzenie o minimaksie, wartość gry. Elementy teorii użyteczności. Równowaga Nasha. Strategie stabilne ewolucyjnie. Związki teorii gier z teorią informacji. Gry z niepełną informacją. Gry Bayesa. Gry kooperacyjne w postaci normalnej i w postaci funkcji charakterystycznej. Optymalne strategie obrony (bazujące na metodach teorii gier) przed zagrożeniami związanymi z ryzykiem informacyjnym (cyberatak, detekcja intruza, działanie w warunkach utraty/braku pełnej informacji. Wykorzystanie pojęć i narzędzi teorii gier do konstrukcji modeli bezpieczeństwa i prywatności informacji. Zastosowanie teorii gier do kryptografii.

MK_38: Wybrane działy matematyki zaawansowanej. Do wyboru 1 przedmiot(y) spośród jak niżej.

MK_38/2 - Analiza matematyczna IV: Operacje na formach różniczkowych. Całkowanie form. Lemat Pioncare. Wektorowe wersje twierdzenia Stokesa. Tensor metryczny i forma objętości.

MK_38/1 - Algebra II: Grupy przekształceń, działanie grupy na zbiorze, twierdzenia Sylowa, grupy rozwiązalne, grupy proste, struktura skończenie generowanych grup abelowych; pierścienie wielomianów wielu zmiennych, pierścienie noetherowskie, twierdzenie Hilberta o bazie, zbiory algebraiczne, pierścienie szeregów potęgowych; ciała skończone, rozszerzenia algebraiczne, liczby algebraiczne i przestępne, ciało rozkładu wielomianu, równania rozwiązalne w pierwiastnikach, ciała algebraicznie domknięte, rozszerzenia konstruowalne, klasyczne konstrukcje geometryczne.

MK_39: Współczesne aspekty i zastosowania nauk społecznych: wybrane zagadnienia

Treści zgodne z dokonanym przez studenta wyborem przedmiotu z obszaru nauk społecznych w danym roku akademickim.

MK_40: Przedmiot na innym kierunku

Treści zgodne z dokonanym przez studenta wyborem przedmiotu w danym roku akademickim.

MK_41: Praktyka zawodowa

Zasady BHP obowiązujące w danej jednostce. Zasady funkcjonowania firmy i jej struktura. Zakres wykorzystania technologii informatycznych w danej jednostce. Definiowanie potrzeb w zakresie systemów i technologii informacyjnych stosowanych w firmie. Dobór oprogramowania. Obsługa (w podstawowym zakresie) systemów informacyjnych stosowanych w danej jednostce.

DZIEKAN
WYDZIAŁU MATEMATYKI I INFORMATYKI
dr hab. Krzysztof Piotr Belina-Prażmowski-Kryński
prof. UwB