ФАКУЛТЕТ ЗА ИНФОРМАТИЧКИ НАУКИ И КОМПЈУТЕРСКО ИНЖЕНЕРСТВО
Универзитет Св. Кирил и Методиј

Елаборат за втор циклус студии по

Кодирање и криптографија

Изработиле:
Проф. д-р Смиле Марковски
Проф. д-р Верица Бакева
Доц. д-р Весна Димитрова
Доц. д-р Боро Јакимовски

Скопје, 19.09.2011

I. Вовед

1. Причини за предлагање на студиската програма

Изучувањето на теоретската основа на кодирање и криптографија претставува основа за изградба на квалитетни идни научници кои ќе дадат голем придонес во кодирањето и криптографијата. Дел од членовите на Факултетот за информатички науки и компјутерско инженерство (ФИНКИ) поседуваат долгогодишно искуство во обука на идни научници во теоретските основи на информатиката.

Целта на овој елаборат е дефинирање на втор циклус студии кои претставуваат логичко продолжување на досегашните постдипломски студии. Предложената студиска програма претставува добра подлога за понатамошно продолжување на младите научници со докторски студии.

Во рамки на предложените предмети студентите ќе можат да се стекнат со теоретски познавања од областите на: криптографија и теорија на кодирање.

2. Елементи со кои се овозможува мобилност на студенти

Предложените предметни содржини, предмет на студиите од втор циклус по кодирање и криптографија, се компатибилни со соодветните студии кои се нудат на најголемиот број светски универзитети кои ја поддржуваат оваа тематика и овозможуваат мобилност на студентите.

II. Општ дел

- Назив на предлагачот – Факултетот за информатички науки и компјутерско инженерство, Универзитет „Св. Кирил и Методиј“ - Скопје
- Назив на студиската програма – Втор циклус студии по Кодирање и криптографија
- Траење на студиите – 2 семестри.
- Услови за запишување на студиите – завршени додипломски студии на компјутерските насоки кои носат минимум 240 кредити. За студиските насоки по компјутерски технологии кои носат помалку од 240 кредити, се дополагаат испити за еквиваленција.
- Академскиот или стручниот назив или степен кој се стекнува со завршување на студиите – Магистер по информатички науки – Теорија на кодирање или Магистер по информатички науки – Криптографија и сигурност на компјутерски системи

III. Студиска програма

Научно подрачје на студиската програма се теоретските основи на информатиката. Наставата по вториот циклус на студии од кодирање и криптографија ќе се одвива во два семестри. Вкупниот број на кредити кои ги носат студиите е 60.

Во наставната програма на модулите е предвидено да има по 4 задолжителни и 2 изборни предмети кои се во согласност со избраната тема за магистерска работа. Наставната содржина, предложените наставници кои ќе ја изведуваат наставата, бројот

на кредитит по предмет и пописот на литературата предложена за секој од предметите е дадена во делот V. од овој елаборат.

Проверката на знаење ќе се одвива во вид на семинари, испити, како и проектни задачи.

Студентите кои дипломирале на студиски програми по компјутерски науки или технологии, чиишто студии носат помалку од 240 кредити, а сакаат да се запишат на втор циклус на студии по кодирање и криптографија, треба да положат испити кои ќе им овозможат навлегување во основите на теоретската информатика. Во следната листа се дадени предметите кои се нудат на првиот циклус на студии на Институтот за информатика, ПМФ, и кои се потребни како предзнаење. Како влезни предмети можат да се прифатат и предмети положени на други институции за кои може да се утврди еквивалентност со подолу наведените предмети.

Предмети од прв циклус на студии потребни за упис на студиите од втор циклус по Кодирање и криптографија се:

Алгоритми

Дискретни структури 3

Веројатност и статистика

Безбедност и криптографија

IV. Образложение за реализацијата

Изведувањето на наставата ќе се одвива во просториите на Факултетот за информатички науки и компјутерско инженерство.

Опремата со која располага Факултетот за информатички науки и компјутерско инженерство е доволна за потребите за одвивање на наставата која се нуди во оваа наставна програма.

1. Кадри за реализација на студиската програма

Студиите се составени од 6 предмети, од кои 4 се задолжителни и 2 се изборни. Студиите се поддржани од следните наставници, членови на ПМФ, кои би биле главни изведувачи на наставата:

Д-р Маргита Кон-Поповска, редовен професор на ФИНКИ,

margita.kon-popovska@finki.ukim.mk

Д-р Смиле Марковски, редовен професор на ФИНКИ, smile.markovski@finki.ukim.mk

Д-р Марјан Гушев, редовен професор на ФИНКИ, marjan.gushev@finki.ukim.mk

Д-р Жанета Попеска, редовен професор на ФИНКИ, zaneta.popeska@finki.ukim.mk

Д-р Верица Бакева, вонреден професор на ФИНКИ, verica.bakeva@finki.ukim.mk

Д-р Ана Мадевска Богданова, вонреден професор на ФИНКИ,

ana.madevska.bogdanova@finki.ukim.mk

Д-р Данило Глигороски, насловен вонреден професор на ФИНКИ,

danilo.gligoroski@gmail.com

Д-р Марија Михова, доцент на ФИНКИ, marija.mihova@finki.ukim.mk

Д-р Горан Велинов, насловен доцент на ФИНКИ, goran.velinov@finki.ukim.mk

Д-р Анастас Мишев, доцент на ФИНКИ, anastas.mishev@finki.ukim.mk

Д-р Весна Димитрова, доцент на ФИНКИ, vesna.dimitrova@finki.ukim.mk

Д-р Дејан Спасов, доцент на ФИНКИ, dejan.spasov@finki.ukim.mk

V. Содржина на студиските програми

Во следните табели е даден список на предметите потребни за изучување на модулите Кодирање и Криптографија и сигурност на компјутерски системи.

1. Модул Кодирање

Име на предметот	**Семестар**		**кредити**
Напредни алгебарски структури	9		8
Случајни процеси	9		8
Теорија на кодирање	9		8
Изборен	9		6
Теорија на информации 2		10	8
Изборен		10	6
Магистерска тема		10	16

Задолжителни предмети кои го формираат модулот

зимски семестар					
	Предмет	Предавања	Аудиториски	Лабораториски	кредити
9	Напредни алгебарски структури	30	30		8
9	Случајни процеси	30	30		8
9	Теорија на кодирање	30	30	15	8
	Вкупно задолжителни				
	Вкупно	90	90	15	24

летен семестар					
	Предмет	Предавања	Аудиториски	Лабораториски	кредити
10	Теорија на информации 2	30	30		8
	Вкупно задолжителни				
	Вкупно	30	30		8

Опис на предметите

Во следните табели се дадени описите на задолжителните предмети на овој модул. Описот на изборните предмети е даден на крајот на оваа глава.

Име на предметот	**Напредни алгебарски структури**		
Наставник	Проф. д-р Смиле Марковски		
Статус	Задолжителен	**Кредити**	8
Семестар	9	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, семинари		
Цели	Воведување на алгебраските структури кои ке се користат во другите предмети од студиите		
Содржини	Изучување на структурите и својствата на: • групоидите: полугрупи, групи и квазигрупи • алгебрите со повеќе операции: прстени, полиња, булови алгебри • релационите алгебри Посебен осврт на конечните алгеарски структури од претходните видови, кои се значајни за примените.		
Основна литература	1) Ѓ. Чупона: Предавања по алгебра, УКИМ Скопје 2) A. Clark: Elements of Abstract algebra, Dover Publ. Inc., New York		

Име на предметот	**Случајни процеси**		
Наставник	Проф. Д-р Верица Бакева		
Статус	Задолжителен	**Кредити**	**7**
Семестар	9	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, семинари		
Цели	Да се оспособат студентите да моделираат случајни процеси		
Содржини	Случајни процеси: дефиниција, карактеристики, класификација, трансформации. Стационарност на случајни процеси. Процеси со независни стационарни прираснувања; Маркови процеси со дискретно и непрекинато множество состојби: процеси на раѓање и умирање; Вериги на Марков, Вгнездени вериги на Марков. Специјални случајни процеси: случајно талкање, Поасонов, Винеров процес. Разгранувачки процеси. Процеси на обнова.		
Основна литература	Papullis: *Probability, Statistics and Stochastic Processes*., D.R.Cox, H.D.Miller: *The Theory of Stochastic Process*., Jean Walrand: Lecture Notes on Probability Theory and Random Processe, Ж. Пауше: *Веројатност, статистика и случајни процеси*.		

Име на предметот	**Теорија на кодирање**		
Наставник	Проф. д-р Верица Бакева/Проф. д-р Смиле Марковски		
Статус	Задолжителен	**Кредити**	8
Семестар	9	**Неделен фонд**	2+2+1
Условеност			
Начин на реализација	Предавања, вежби, семинари		
Цели	Запознавање на студентите со основните кодови за откривање и кодовите за поправање на грешки.		
Содржини	Математички подготовки за потребите на теоријата на кодирање: теорија на групи, теорија на конечни полиња, полиноми над конечни прстени и полиња, стохастички процеси, теорија на информации и ентропија. Основни дефиниции и својства на теорија на кодови. Теореми на Шанон. Групни кодови. Кодови што откриваат грешки и CRC. Кодови што поправаат грешки. Кодови на Рид-Милер и кодови на Рид-Соломон. Алгебарски кодови. Турбо кодови. LDPC (линеарно густи проверки на парност) кодови. Случајни проточни кодови.		
Основна литература	1. Vanstone, S.A., van Ooschot, P.S. (1989) *An Introduction to Error Correcting Codes with Applications*, Kluwer Academic Publishers, Boston 2. Hill, R. (1986) *A First Course of Coding Theory*, Clarendon Press, Oxford 3. Torleiv K., (2007) *Codes for error detection*, World scientific		

Име на предметот	**Теорија на информации 2**		
Наставник	Проф. д-р Верица Бакева		
Статус	Задолжителен	**Кредити**	8
Семестар	10	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, семинари		
Цели	Воведување на математички модел на комуникациски систем.		
Содржини	Комуникациски систем. Ентропија. Информација. Компресија на податоци: Кодирање со загуби. Asymptotic Equipartition Property (AEP) за независни случајни променливи. Теорема на Shannon за кодирање на изворен сигнал. Кодирање без загуби. Симболични кодови. Проблем на единствено декодирање. Моментални кодови. Крафтово неравенство. Теорема за бесшумно кодирање. Конструкција на оптимални кодови. Комуникација преку канал со шум (Комуникациски канал. Модели на комуникациски канал. Дискретен канал без меморија. Капацитет на дискретен канал без меморија). Извори на информации: Вериги на Марков. Извор на информации. Регуларен Марков извор. Ентропија на извор. Ред на извор. Апроксимација на општ извор на информации со извор од конечен ред. Ергодичен извор. Теорема на Shannon – McMillan (Asymptotic Equipartition Property (AEP)). Дискретен канал со меморија: Модели на дискретен канал со меморија. Канал со конечно множество состојби. Капацитет на општ дискретен канал. Теорема за кодирање за регуларен канал со конечно множество состојби. Непрекинати канали: Ентропија на непрекинати случајни променливи. Ентропија на Гаусова случајна променлива. Видови непркинати канали. Гаусов канал (временски дискретен). AEP за непрекинати случајни променливи. Теорема за кодирање за Гаусов канал.		
Основна литература	a. Thomas M. Cover, Joy A. Thomas: *Elements of Information Theory*, John Wiley & Sons, Inc. b. Ž. Pauše: *Uvod u teoriju informacije*, Školska knjiga, Zagreb c. R.Ash: *Information Theory*, Dover Publication, Inc.		

2. *Модул Криптографија и сигурност на компјутерски системи*

Име на предметот	Семестар		Кредити
Напредни алгебарски структури	9		8
Напредна криптографија	9		8
Информациска сигурност	9		8
Изборен	9		6
Криптоанализа		10	8
Изборен		10	6
Магистерска тема		10	16

Задолжителни предмети кои го формираат модулот

зимски семестар					
	Предмет	Предавања	Аудиториски	Лабораториски	кредити
9	Напредни алгебарски структури	30	30		8
9	Напредна криптографија	30	30	15	8
9	Информациска сигурност	30	30		8
	Вкупно задолжителни				
	Вкупно	90	90	15	24

летен семестар					
	Предмет	Предавања	Аудиториски	Лабораториски	кредити
10	Криптоанализа	30	30		8
	Вкупно задолжителни				
	Вкупно	30	30		8

Опис на предметите

Во следните табели се дадени описите на задолжителните предмети на овој модул. Описот на изборните предмети е даден на крајот на оваа глава.

Име на предметот	**Напредни алгебарски структури**		
Наставник	Проф. д-р Смиле Марковски		
Статус	Задолжителен	**Кредити**	8
Семестар	9	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, семинари		
Цели	Воведување на алгебраските структури кои ке се користат во другите предмети од студиите		
Содржини	Изучување на структурите и својствата на • групоидите: полугрупи, групи и квазигрупи • алгебрите со повеќе операции: прстени, полиња, булови алгебри • релационите алгебри Посебен осврт на конечните алгеарски структури од претходните видови, кои се значајни за примените.		
Основна литература	1) Ѓ. Чупона: Предавања по алгебра, УКИМ Скопје 2) A. Clark: Elements of Abstract algebra, Dover Publ. Inc., New York		

Име на предметот	**Напредна криптографија**		
Наставник	Проф. д-р Смиле Марковски, доц. д-р Весна Димитрова		
Статус	Задолжителен	**Кредити**	8
Семестар	9	**Неделен фонд**	2+2+1
Условеност			
Начин на реализација	Предавања, вежби, семинари		
Цели	Оспособеност на студентите конкретно да ги реализираат посебните видови криптографски пакети		
Содржини	Алгоритми за генерирање на огромни прости броеви и заемно прости броеви; реализација на алгоритми за симетрични крипто системи; реализација на РСА и Ел Гамал системи со јавни клучеви; реализација на протоколи за размена на клучеви; разбивање на попрости крипто системи		
Основна литература	T. Baigneres, P. Junod at al.: A classiacal introduction to cryptography exercise book, Springer, 2006		

Име на предметот	**Криптоанализа**		
Наставник	Проф. д-р Смиле Марковски, доц. д-р Весна Димитрова		
Статус	Задолжителен	**Кредити**	8
Семестар	10	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, семинари		
Цели	Изучување на основните алатки за криптоанализа		
Содржини	Видови на напади со груба сила, статистички напади, диференцијална и линеарна криптоанализа, претставувања на крипто системи како булови функции и испитувања на својствата за линеарност, специјални видови напади за посебни крипто продукти (хаш функции, блок шифривуаци, со јавни клуцеви, протоколи)		
Основна литература	1) N. Smart: Introduction to cryptography, McGraw-Hill 2003 2) S. Vaudenay: A classical introduction to cryptography – Applications for comunications security, Springer, 2006		

Име на предметот	**Информациска сигурност**		
Наставник	Проф. Д-р Смиле Марковски, доц. д-р Весна Димитрова		
Статус	Задолжителен	**Кредити**	8
Семестар	9	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, семинари		
Цели	Изучување на основните сигурносни модели за контрола на пристап, на протоколи и софтвер за компјутерски конфигурации		
Содржини	Методи за автентикација, пасворди, биометрика, два-факторска автентикација, авторизација, пристап до контролна амтрицаповече степенски модели на сигурност, огнени ѕидови, детекција на напаѓачи, едноставни протоколи за автентикација,ССЛ, софтверска несигурност, вируси, црви, временски бомбифункции за сигурност на оперативни системи		
Основна литература	1) Mark Stamp: Information security principles and practice, Wiley-Interscience 2) M. Bishop: Computer security – Art and science, Addison-Wesley, 2003		

3. Изборни предмети

Во следните табели се дадени описите за изборните предмети кои важат за сите модули дефинирани во оваа насока. Студентите исто така можат да изберат како изборен предмет и предмет од листите на задолжителни и изборни предмети од останатите насоки акредитирани во Втор циклус на студии на Институтот за Информатика при Природно-математичкиот Факултет.

Изборни предмети					
	Предмет	Предавања	Аудиториски	Лабораториски	кредити
	Безбедност на компјутерски мрежи	30	15	15	7
	Грид и научно програмирање	30	15	30	8
	Динамичко програмирање и стохастичка контрола	30	15	15	8
	Доверливост (безбедност) и сигурност кај системите за управување со бази на податоци	30	30	15	8
	Извршување и оптимизација на прашалници (SQL изрази) – теоретски аспекти	30	30	15	6
	Информациска сигурност	30	30		8
	Концептуални податочни модели кај податочните складови	30	15	15	8
	Криптоанализа	30	30		8
	Математичка логика	30	30		8
	Моделирање и управување на ETL процеси кај податочните складови	30	15	15	8
	Модерни симулации и моделирање	30	15	30	8
	Напредни алгоритми	30	30	15	8
	Надежност на компјутерски системи и мрежи	30	15	15	8
	Напредни концепти на бази на податоци	30	30	15	8
	Оптимизација	30	30	15	8
	Проект	60			8
	Напредна криптографија	30	30	15	8
	Случајни процеси	30	30		8
	Теорија на информации 2	30	30		8
	Теорија на кодирање	30	30	15	8
	Теорија на програмирање	30	30		8
	Формални методи	30	30		8
	Формални јазици и автомати	30	30	15	8

Опис на предметите

Во следните табели се дадени описите на предмети (задолжителни и изборни).

Име на предметот	**Напредни алгоритми**		
Наставник	Проф. д-р Ана Мадевска-Богданова, Доц. д-р Марија Михова, доц. д-р Боро Јакимовски, доц. д-р Весна Димитрова		
Статус	Изборен	**Кредити**	8
Семестар	9	**Неделен фонд**	2+2+1
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Целта на предметот е да се обработат техники за дизајн и анализа на ефикасни алгоритми, особено на методи кои се корисни во пракса.		
Содржини	Граф алгоритми (Елементарни, Најкратко распнувачко дрво, Најкраток пат, Сите парови на најкратки патишта, Максимален проток), Сортирачки мрежи, Матрични операции, Линеарно програмирање, Работа со полиноми и FFT, Алгоритми од теорија на броеви, Споредба на стрингови, Пресметковна геометрија, NP комплетност, Приближни алгоритми		
Основна литература	Thomas H. Cormen. Charles E. Leiserson, Ronald L. Rivest, Clifford Stein: *Introduction to Algorithms, 2/e,* MIT Press.		

Име на предметот	**Формални методи**		
Наставник	Проф. д-р Смиле Марковски, доц. д-р Боро Јакимовски		
Статус	Изборен	**Кредити**	8
Семестар	9	**Неделен фонд**	2+2+1
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Предметот ќе ги запознае студентите со можностите што ги нудат формалните методи, категориите на формални методи и нивната употреба во градењето на софтверските архитектури		
Содржини	Вовед во формални методи, Спецификација на системи користејќи методи: базирани на состојби/транзиции, аксиоматски, абстрактни модели, алгебарски, темпорална логика, паралелни системи. Формална верификација.		
Основна литература	R. A. Kemmerer. **Integrating Formal Methods into the Development Process.** *IEEE Software*, 7(5):37-50, September 1990. N. Medvidovic and R. N. Taylor. **A Classification and Comparison Framework for Software Architecture Description Languages.** *IEEE Transactions on Software Engineering*, 26(1):70-93, January 2000. D. Harel. **Statecharts: A Visual Formalism for Complex Systems.** *Science of Computer Programming*, 8(1987):231-274, 1987. J. M. Atlee and J. Gannon. **State-Based Model Checking of Event-Driven System Requirements.** *IEEE Transactions on Software Engineering*, 19(1):24-40, January 1993. C. A. R. Hoare. **An Axiomatic Basis for Computer Programming.** *Communications of the ACM*, 12(10):576-583, October 1969. J. M. Spivey. **The Z Notation: A Reference Manual.** Oriel College, Oxford, England, 1998. J. A. Goguen and T. Winkler. **Introducing OBJ3.** Technical Report, SRI-CSL-88-9, SRI International, August 1988. L. Lamport. **What Good Is Temporal Logic?** *9th World Computer*		

	Congress, 657-668, Paris, France, IFIP, North Holland, 1992. U.A. Buy and R. Moll. **A Specification-Based Approach to Concurrency Analysis.** *Journal of Automated Software Engineering*, 2(2):265-309, 1995. S. Igarashi, R. L. London, and D. C. Luckham. **Automatic Program Verification I: A Logical Basis and Its Implementation.** *Acta Informatica*, 4:145-182, 1975. S. L. Hantler and J. C. King. **An Introduction to Proving the Correctness of Programs.** *ACM Computing Surveys*, 8(3):331-353, September 1976.

Име на предметот	**Оптимизација**		
Наставник	Проф д-р. Ванчо Кусакатов, Проф. д-р Маргита Кон-Поповска,		
Статус	Изборен	**Кредити**	8
Семестар	9	**Неделен фонд**	2+2+1
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Да се обезбеди знаење за проблеми на оптимизација, класификација на оптимизациски проблеми и алгоритми и методи за нивно решавање, како и примената во информатиката		
Содржини	Вовед: едно-димензионална оптимизација, потребни услови, градиентен метод, њутнов метод, барање глобален оптимим; мулти-димензионална оптимизација: услови за оптимум, проблем без ограничувања, линеарни ограничувања, нелинеарни ограничувања. линеарно програмирање, квадратно програмирање; нелинеарни ограничувања, методи на пенали и бариери, градиентно-проектни методи, проширени методи на Лагранж, други класични методи; Други проблеми на оптимизација: стохастичка оптимизација, динамичка оптимизација; хевристички методи на оптимизација: еволутивни алгоритми, генетски алгоритми, еволутивно програмирање, ant colony оптимизација, (particle swarm) оптмизација, simulated annealing, табу пребарување		
Основна литература	Tomas Weise, Global Optimization Algorithms, 2009 (electronic version) Yurii Nesterov, Introductory lectures on Convex Optimization, Kluwer Academic Publishers 2004 (google.books) Ph. E. Gill, W. Murray, M. H. Wright, Practical Optimization, Academic Press, Inc., London, New York, Toronto, 1981 M.S. Bazaraa, C. M. Shetty, Nonlinear Programming Theory and Algorithms, John Wiley and Sons, New York, Toronto, 1979		

Име на предметот	**Безбедност на компјутерски мрежи**		
Наставник	Проф. д-р Марјан Гушев, , доц. д-р Боро Јакимовски		
Статус	Изборен	**Кредити**	7
Семестар	9 или 10	**Неделен фонд**	2+1+1
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Детален и практичен преглед на мрежни и интернет сигурносни апликации и стандарди. Конкретна примена на криптографијата, покривајќи алгоритми и протоколи кои се основата на мрежните сигурни апликации, енкрипција, дигитални потписи и размена на клучеви		
Содржини	OSI сигурносен модел, сигурносни напади, сервиси и механизми,		

	модели на интернет сигурност, интернет сигурносни стандарди, протоколи автентикација и авторизација, сигурност на електронска пошта, IP сигурност, Web сигурност и менаџмент на мрежната сигурност
Основна литература	William Stallings, Network Security Essentials: Applications and Standards

Име на предметот	**Грид и научно програмирање**		
Наставник	Проф. д-р Маргита Кон-Поповска, доц. д-р Анастас Мишев, доц. д-р Боро Јакимовски		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+1+2
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Воведување во разни техники на дистрибуирано процесирање и напредни техники на големи пресметувања.		
Содржини	Изучување на техники на напредно дистрибуирано процесирање и научно програмирање		
Основна литература	Vladimir Silva, Grid Computing for Developers, Charls River Media, 2005.		

Име на предметот	**Динамичко програмирање и стохастичка контрола**		
Наставник	Доц. Д-р. Марија Михова		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+1+1
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Запознавање со повеќе проблеми кои можат да се третираат со динамичко програмирање. Да се формулираат практични модели за оптимална контрола на динамички системи со конечен и бесконечен број на состојби.		
Содржини	Алгоритми од динамичко програмирање. Детерминистички системи, временски непрекината отимална контрола. Проблеми со целосни и нецелосни информации за состојбите.		
Основна литература	Bertsekas, Dimitri. *Dynamic Programming and Optimal Control*. Vol. I and II. 3rd ed. Nashua, NH: Athena Scientific, 2007.		

Име на предметот	**Доверливост (безбедност) и сигурност кај системите за управување со бази на податоци**		
Наставник	проф. д-р Маргита Кон-Поповска, доц. д-р Горан Велинов		
Статус	Изборен	**Кредити**	6
Семестар	9 или 10	**Неделен фонд**	2+2+1
Условеност	Предмети кои студентот треба да ги има ислушано/положено за да го слуша/полага актуелниот предмет. **Напредни концепти на бази на податоци**		
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Запознавање со концептите на податочна сигурност и доверливост кај системите на бази на податоци, бекап и обновување на бази на податоци.		

Содржини	Податочна сигурност кај системите на бази на податоци Трансакциско процесирање и конкурентност кај бази на подаотоци Некомплетни бази на податоци (incomplete databases), бекап и обновување
Основна литература	Introduction to Database systems, C.J. Date, Database system concepts, Silberschatz, Korth, Sudarshan Database management system, Raghu Ramakrishnan, Johannes Gehrke, Forth Edition, 2006

Име на предметот	**Извршување и оптимизација на прашалници (SQL изрази) – теоретски аспекти**		
Наставник	проф. д-р Маргита Кон-Поповска, доц. д-р Горан Велинов		
Статус	Изборен	**Кредити**	6
Семестар	9 или 10	**Неделен фонд**	2+2+1
Условеност	Предмети кои студентот треба да ги има ислушано/положено за да го слуша/полага актуелниот предмет: **Напредни концепти на бази на податоци**		
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Да обезбеди знаење за напредните концепти на извршување на прашалници (SQL изрази) бази на податоци. Студентите ќе се запознаат со теоретските аспекти на извршувањето на прашалници што се вградени во современите системи за управување со бази на податоци.		
Содржини	Вовед во извршувањето на прашалници, Планови на извршување на прашалниците, Оптимизација на прашалници, Типови на индекси и нивната улога, Типови на поврзувања и нивната улога, Физичко складирање на податоците, Нови и алтернативни алгоритми на оптимизација на прашалниците.		
Основна литература	Fundamentals of Database Systems, R. Elmasri and S. B. Navathe. Database system concepts, Silberschatz, Korth, Sudarshan Query Optimization, Y. Ioannidis Database management system, Raghu Ramakrishnan, Johannes Gehrke, Forth Edition, 2006		

Име на предметот	**Информациска сигурност**		
Наставник	Проф. д-р Смиле Марковски, доц. д-р Весна Димитрова		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Изучување на основните сигурносни модели за контрола на пристап, на протоколи и софтвер за компјутерски конфигурации		
Содржини	Методи за автентикација, пасворди, биометрика, два-факторска автентикација, авторизација, пристап до контролна амтрицаповече степенски модели на сигурност, огнени ѕидови, детекција на напаѓачи, едноставни протоколи за автентикација,ССЛ, софтверска несигурност, вируси, црви, временски бомбифункции за сигурност на оперативни системи		

Основна литература	1) Mark Stamp: Information security principles and practice, Wiley-Interscience 2) M. Bishop: Computer security – Aet and science, Addison-Wesley, 2003

Име на предметот	**Концептуални податочни модели кај податочните складови**		
Наставник	доц. д-р Горан Велинов, проф. д-р Маргита Кон-Поповска		
Статус	Изборен	**Кредити**	6
Семестар	9 или 10	**Неделен фонд**	2+1+1
Условеност	Предмети кои студентот треба да ги има ислушано/положено за да го слуша/полага актуелниот предмет: **Напредни концепти на бази на податоци**		
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Да обезбеди теоретско знаење за постојните концептуални модели што се применуваат при моделирањето на податочните складови. Студентите ќе се запознаат со доесгашните научни достигнуваања во оваа област, ќе ги споредат различните повеќедимензионални модели, ќе оценат кои и во колкава мерка се применливи за релана имплементација.		
Содржини	Вовед во податочни складови, Концептуално моделирање и концептуален дизајн, Повеќе димензионални коцки, Логичко моделирање и логички дизајн, индекси за податочните складови, физички дизајн, OLAP, Бизнис интелигенција за податоците.		
Основна литература	Data Warehouse Design: Modern Principles and Methodologies,M. Golfarelli, S. Rizzi, Aspects of Data Modeling and Query Processing for Complex Multidimensional Data,Torben Bach Pedersen, Conceptual Multidimensional Data Model Based on MetaCube T. Nguyen, A. Min Tjoa, R. Wagner		

Име на предметот	**Криптоанализа**		
Наставник	Проф. д-р Смиле Марковски, доц. д-р Весна Димитрова		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Изучување на основните алатки за криптоанализа		
Содржини	Видови на напади со груба сила, статистички напади, диференцијална и линеарна криптоанализа, претставувања на крипто системи како булови функции и испитувања на својствата за линеарност, специјални видови напади за посебни крипто продукти (хаш функции, блок шифривуаци, со јавни клуцеви, протоколи)		
Основна литература	1) N. Smart: Introduction to cryptography, McGraw-Hill 2003 2) S. Vaudenay: A classical introduction to cryptography – Applications for comunications security, Springer, 2006		

Име на предметот	Математичка логика		
Наставник	Проф. д-р Смиле Марковски		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Оснозавање на основните поими и својства на исказното и предикатското логичко сметање и примената во информатиката		
Содржини	Исказно сметање: булови операции и интерпретации, исказни формули, логички еквиваленции и замени, семантички таблоа, дедуктивни докази, резолуции, Генценов и Хилбертов систем Предикатско сметање: релации, предикатни формули, интерпретации, логички еквиваленции и замени, семантички таблоа,дедуцтивни форми, функции и терми Резолуциско и логичко програмирање: основна резолуција, замена, унификација, општа резолуција, логичко програмирање Темпоралнa логика.		
Основна литература	M. Ben-ari: Mathematical logic for computer science, Prentice Hall, 1992		

Име на предметот	Моделирање и управување на ETL процеси кај податочните складови		
Наставник	доц. д-р Горан Велинов, проф. д-р Маргита Кон-Поповска		
Статус	Изборен	**Кредити**	6
Семестар	10	**Неделен фонд**	2+2+1
Условеност	Предмети кои студентот треба да ги има ислушано/положено за да го слуша/полага актуелниот предмет: Напредни концепти на бази на податоци		
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Да обезбеди теоретско знаење за моделирањето и управувањето на Extraction – Transformation - Loading (ETL) процесите кај податочните складови. Студентите ќе се запознаат со доесгашните научни достигнуваања во оваа област, ќе ги совлаадт предложените концептуални модели и алгоритми со кои се дефинираат овие процеси. Ќе се запонаат со техниките и алгоритмите за оптимизација на ETL процесите.		
Содржини	Вовед во податочни складови, Концептуален и логички модел на ETL процесите, алгоритми за оптимизација на ETL процесите, приод на ETL со користење на мета податоци, интеграција на податоците, калвитет на податоците.		
Основна литература	Conceptual Modeling for ETL Processes, P. Vassiliadis, A. Simitsis, S. Skiadopoulos A Metadata - Driven Approach For Data Warehouse Refreshment, A. Vavouras, Modeling and managing ETL processes, A. Simitsis		

Име на предметот	Модерни симулации и моделирање
Наставник	Проф. Д-р. Жанета Попеска, проф. Д-р Верица Бакева, доц. Д-р Марија Михова

Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+1+2
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Запознавање со принципите на моделирање како и конвенционалните и модерните методи на симулација на системи од дискретни настани (discrete-event systems – DES) коко што се компјутерско-комуникациските системи, флексибилните производствени системи, PERT мрежите и мрежите на протоци вклучувајќи ги системите на чекање.		
Предуслови	Основни предзнаења од веројатност, статистика и оптимизација		
Содржини	Конвенционална симулација: Системи, модели и симулација, генерирање на случајни броеви, случајни променливи и стохастички процеси, анализа на излез на системи со дискретни состојби преку симулации, техники за намалување на дисперзијат. Модерна симулација: анализа на сензитивност и оптимизација на статички системии од дискретни настани, анализа на сензитивност и оптимизација на динамички системи од дискретни настани, оценување на веројатности на ретки настани.		
Основна литература	Reuven Y. Rubenshtain, Benjamin Melamed, Modern Simulation and Modeling, John Wiley & Sons, 1998.		

Име на предметот	**Надежност на компјутерски системи и мрежи**		
Наставник	Проф. Д-р. Жанета Попеска, Доц. Д-р. Марија Михова		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+1+1
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Целта на предметот е да се воведат теоретски знаења од областа на надежност на системи, да се воведат техники за моделирање и пресметување на надежност, со што би се ставило акцент на надежност на софтвер, хардверско/софртверски ситеми и мрежи.		
Содржини			
Основна литература	**Hoang Pham, "System Software Reliability" ,** Springer, 2006-11-02, ISBN: 1852339500, **Modern Statistical And Mathematical Methods in Reliability** Publisher: World Scientific Publishing Company (2005-10), ISBN: 9812563563,		

Име на предметот	**Напредни концепти на бази на податоци**		
Наставник	проф. д-р Маргита Кон-Поповска, доц. д-р Горан Велинов, асист. м-р Вангел Ајановски		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2+1
Условеност	Предмети кои студентот треба да ги има ислушано/положено за да го слуша/полага актуелниот предмет. **Бази на подаотци**		
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Да обезбеди знаење за напредните концепти на бази на		

	податоци. Студентите ќе се запознаат со строгите теоретските аспекти што се вградени во современите системи за управување со бази на податоци, како и најнови трендови и отворени проблеми од теоретски и практичен аспект во развојот на бази податоци
Содржини	Релациски модел на бази на податоци (релациона алгебра, релационо предикатно сметање, функциски зависности, нормализација). Неконвенционални на бази на податоци – Многу големи бази на податоци XML бази на податоци, неструктуирани бази на податоци Обектно ориентирани бази на подаотци Semantic web и бази на податоци Фајл организирани бази на податоци
Основна литература	Relational Databases, Chao-Chin Yang, Introduction to Database systems, C.J. Date, Database system concepts, Silberschatz, Korth, Sudarshan

Име на предметот	**Проект**		
Наставник	Сите вклучени во наставата		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	4
Условеност			
Начин на реализација	Консултации		
Цели	Студентот во соработка со професорот треба да изврши истражување во област од интерес. Резултатите од истражувањето треба да резултира со научен труд кој ќе се објави на интернационална конференција		
Содржини	Отворена од областа на истражување		
Основна литература	/		

Име на предметот	**Напредна криптографија**		
Наставник	Проф. д-р Смиле Марковски, доц. д-р Весна Димитрова		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2+1
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Оспособеност на студентите конкретно да ги реализираат посебните видови криптографски пакети		
Содржини	Алгоритми за генерирање на огромни прости броеви и заемно прости броеви; реализација на алгоритми за симетрични крипто системи; реализација на РСА и Ел Гамал системи со јавни клуцеви; реализација на протоколи за размена на клучеви; разбивање на попрости крипто системи		
Основна литература	T. Baigneres, P. Junod at al.: A classiacal introduction to cryptography exercise book, Springer, 2006		

Име на предметот	**Случајни процеси**
Наставник	Проф. Д-р Верица Бакева

Статус	Изборен	**Кредити**	**7**
Семестар	9 или 10	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Да се оспособат студентите да моделираат случајни процеси		
Содржини	Случајни процеси: дефиниција, карактеристики, класификација, трансформации. Стационарност на случајни процеси. Процеси со независни стационарни прираснувања; Маркови процеси со дискретно и непрекинато множество состојби: процеси на раѓање и умирање; Вериги на Марков, Вгнездени вериги на Марков. Специјални случајни процеси: случајно талкање, Поасонов, Винеров процес. Разгранувачки процеси. Процеси на обнова.		
Основна литература	Papullis: *Probability, Statistics and Stochastic Processes*., D.R.Cox, H.D.Miller: *The Theory of Stochastic Process*., Jean Walrand: Lecture Notes on Probability Theory and Random Processe, Ж. Пауше: *Веројатност, статистика и случајни процеси*.		

Име на предметот	**Теорија на информации 2**		
Наставник	Проф. д-р Верица Бакева		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Воведување на математички модел на комуникациски систем.		
Содржини	Комуникациски систем. Ентропија. Информација. Компресија на податоци: Кодирање со загуби. Asymptotic Equipartition Property (AEP) за независни случајни променливи. Теорема на Shannon за кодирање на изворен сигнал. Кодирање без загуби. Симболични кодови. Проблем на единствено декодирање. Моментални кодови. Крафтово неравенство. Теорема за бесшумно кодирање. Конструкција на оптимални кодови. Комуникација преку канал со шум (Комуникациски канал. Модели на комуникациски канал. Дискретен канал без меморија. Капацитет на дискретен канал без меморија). Извори на информации: Вериги на Марков. Извор на информации. Регуларен Марков извор. Ентропија на извор. Ред на извор. Апроксимација на општ извор на информации со извор од конечен ред. Ергодичен извор. Теорема на Shannon – McMillan (Asymptotic Equipartition Property (AEP)). Дискретен канал со меморија: Модели на дискретен канал со меморија. Канал со конечно множество состојби. Капацитет на општ дискретен канал. Теорема за кодирање за регуларен канал со конечно множество состојби. Непрекинати канали: Ентропија на непрекинати случајни променливи. Ентропија на Гаусова случајна променлива. Видови непркинати канали. Гаусов канал (временски дискретен). AEP за непрекинати случајни променливи. Теорема за кодирање за Гаусов канал.		
Основна литература	a. Thomas M. Cover, Joy A. Thomas: *Elements of Information Theory*, John Wiley & Sons, Inc. b. Ž. Pauše: *Uvod u teoriju informacije*, Školska knjiga, Zagreb		

	c. R.Ash: *Information Theory,* Dover Publication, Inc.

Име на предметот	**Теорија на кодирање**		
Наставник	Проф. д-р Верица Бакева/Проф. д-р Смиле Марковски		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2+1
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Запознавање на студентите со основните кодови за откривање и кодовите за поправање на грешки.		
Содржини	Математички подготовки за потребите на теоријата на кодирање: теорија на групи, теорија на конечни полиња, полиноми над конечни прстени и полиња, стохастички процеси, теорија на информации и ентропија. Основни дефиниции и својства на теорија на кодови. Теореми на Шанон. Групни кодови. Кодови што откриваат грешки и CRC. Кодови што поправаат грешки. Кодови на Рид-Милер и кодови на Рид-Соломон. Алгебарски кодови. Турбо кодови. LDPC (линеарно густи проверки на парност) кодови. Случајни проточни кодови.		
Основна литература	1. Vanstone, S.A., van Ooschot, P.S. (1989) *An Introduction to Error Correcting Codes with Applications*, Kluwer Academic Publishers, Boston 2. Hill, R. (1986) *A First Course of Coding Theory*, Clarendon Press, Oxford 3. Torleiv K., (2007) *Codes for error detection*, World scientific		

Име на предметот	**Теорија на програмирање**		
Наставник	д-р Анастас Мишев, доц. д-р Боро Јакимовски		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Изучување на теоријата за верификација, валидација и докажување на програмите		
Содржини	Едноставни императивни јазици: Синтакса, Операциона семантика, Денотациска семантика, Програмска Спецификација и нивно докажување. Недетерминизам и заштитени команди: Синтакса, Операциона семантика, Програмска семантика и нивно докажување. Споделени променливи кај паралелизмот: Синтакса и семантика. Ламбда калкулус: Синтакса, семантика, програмирање кај ламбда калкулусот. Алчни фукнциски јазици: Синтакса и семантика. Системи од едноставен тип, подтипови и пресечни типови Полиморфизам: Синтакса и полиморфно програмирање.		
Основна литература	J.C. Reynolds, *Theories of Programming Languages,* Cambridge University Press, 1998. J.C. Reynolds, *The Craft of Programming*, Prentice Hall International, 1981.		

	G. Winskel, *The Formal Semantics of Programming Languages: An Introduction*, MIT Press, 1993.

Име на предметот	**Формални јазици и автомати**		
Наставник	д-р Смиле Марковски, доц. д-р Боро Јакимовски		
Статус	Изборен	**Кредити**	8
Семестар	9 или 10	**Неделен фонд**	2+2+1
Условеност			
Начин на реализација	Предавања, вежби, домашни задачи, семинарски		
Цели	Запознавање со теоријата на пресметливост, теоријата на формални јазици, нивно препознавање, трансформација и обработка.		
Содржини	Вовед во теорија на пресметливост, Конечни автомати, Регулани јазици и регуларни граматики, Својства на регуларни јазици, Контекстно слободни јазици, Поедноставување на контекстно слободни јазици и нормална форма, Пушдаун автомати, Својства на контекстно слободни јазици, Тјурингови машини, Други модели на тјурингови машини, Хиерархија на формални јазици и автомати, Граници на алгоритамското пресметување, Други модели на пресметување.		
Основна литература	Биљана Јанева: Алгоритми и автомати. УКИМ, 1999. Peter Linz: *An Introduction to Formal Languages and Automata,* Jones and Bartlett Publishers, 2006. Thomas A. Sudkamp: *Languages and Machines, 3rd Edition*, Addison-Wesley, 2005.		