1.	Наставен предмет	***СИГУРНОСНИ КОМУНИКАЦИИ***			
2.	Шифра	**ETF114Z05**			
3.	Студиска програма	***Телекомуникации***			
4.	Семестар (изборност)	***зимски (изборен)***			
5.	Цели на предметот	*Запознавање со криптографските техники, алгоритми и протоколи, историски развој, современи трендови и нивна примена во различни апликации. Запознавање со концептите за обезбедување на сигурни комуникации низ различни типови на комуникациски мрежи и системи.*			
6.	Оспособен за (компетенции)	*Разбирање на концептите за криптографија и мрежна сигурност. Теоретска анализа и софтверска имплементација на различни алгоритми и протоколи за обезбедување на сигурни комуникации. Избор на соодветни механизми во дадена мрежна архитектура.*			
7.	Услов за запишување на предметот	*Дигитални телекомуникации 2*			
8.	Основна литература (до 3 наслови)	*1. W. Stallings, Cryptography and Network Security, Principles and Practices, Prentice Hall, 2005* *2. P. Chandra, Bulletproof Wireless Security, Elsevier, 2005* *3. Интерни скрипти, слајдови, решени задачи, ...*			
9.	Број на кредити	*6*			
10.	Вкупен расположив фонд на време	*3+1+1*			
11.	Распределба на расположивото време	*6 ECTS x 30 часа = 180 часа*			
	11.1.	*П -*	*Предавања-теоретска настава*	*45*	*часа*
	11.2.	*АВ -*	*Аудиторни вежби*	*15*	*часа*
	11.3.	*ЛВ -*	*Лабораториски вежби*	*15*	*часа*
	11.4.	*ПЗ*	*Проверка на знаење* — *1. Тестови*	*0*	*часа*
			2. Парцијални испити	*3*	*часа*
			3. Испит	*3*	*часа*
			4. Домашни работи	*10*	*часа*
	11.5.	*СЗ*	*Самостојни задачи* — *1. Проектни задачи*	*0*	*часа*
			2. Самостојни работи	*89*	*часа*
12.	Оценување				
	12.1.	*Посетеност на настава (до 10 бода)*		*0*	*бода*
	12.2.	*Парцијални испити (min. 60% од вкупниот број предвидени бодови)*		*75*	*бода*
	12.3.	*Испит (min. 50% од вкупниот број предвидени бодови)*		*75*	*бода*
	12.4.	*Тестови (max. 20% од вкупниот број предвидени бодови))*		*10*	*бода*
	12.5.	*Семинарски работи (max.10% од вкупниот број предвидени бодови)*		*10*	*бода*
	12.6.	*Лабораториски вежби (max. 20% од вкупниот број предвидени бодови)*		*5*	*бода*
	12.7.	*Проектни задачи (max. 20% од вкупниот број предвидени бодови)*		*0*	*бода*

Забелешка:	Бодови:	Оценки:
Испитот се смета за положен ако студентот освои најмалку 60% од вкупниот број бодови предвидени со предметната програма. Парцијалниот испит се смета за положен ако студентот освои најмалку 30% од вкупниот број бодови.	*од 60 до 67*	*6 (шест)*
	од 68 до 75	*7 (седум)*
	од 76 до 83	*8 (осум)*
	од 84 до 91	*9 (девет)*
	од 92 до 100	*10 (десет)*

13.	Услов за потпис и формален испит	*Реализирани активности 11.1-11.3*

ПЛАНИРАЊЕ АКТИВНОСТИ ЗА НАСТАВНИОТ ПРЕДМЕТ **СИГУРНОСНИ КОМУНИКАЦИИ**

недела	Предавања - теоретска настава		Аудиторни и лабораториски вежби	
	часа	тема	часа	Тема
I.	*3*	Вовед. Потреба од сигурност во комуникациите. Историски преглед. Современи трендови. Основни концепти во криптографија/криптоанализа. Алгоритми. Клучеви. Напади.	*1*	Примери за потреба од тајност на комуникациите.
II.	*3*	Класична симетрична енкрипција. Методи на супституција и транспозиција.	*1*	Фреквенциска анализа.
III.	*3*	Блоковска енкрипција. DES.	*1*	Слаби клучеви. Напад на DES.
			2	Алгоритми за енкрипција со супституција и транспозиција.
IV.	*3*	AES. Повеќекратна енкрипција. Сигурност на симетрична енкрипција. Тест.	*1*	Примери од конечни полиња.
			2	ЕНИГМА.
V.	*3*	Несиметрична енкрипција. Јавен/таен клуч. RSA.	*1*	Примери од теорија на броеви.
			2	DES. AES.
VI.	*3*	Hash функции. Дигитални потписи.	*1*	Едноставни примери за илустрација на RSA.
			2	Генерирање на прости броеви и факторизација.
VII.	*3*	Квантна криптографија. Примена на квантни компјутери во криптоанализа.	*1*	Примери за Hash функции и автентичност на пораките
			2	RSA. Генерирање на клуч со квантна криптографија.
VIII.	*3*	Прв парцијален испит.	*1*	Консултации.
IX.	*3*	Основни концепти за мрежна сигурност. Разлики кај жични и безжични мрежи.	*1*	Примери за ранливост при напади за различни мрежи и преносни медиуми.
			2	Квантна криптографија.
X.	*3*	Сигурност во слоевита мрежна архитектура. Физичко и податочно ниво. Автентикација.	*1*	Сигурносни аспекти на жични мрежи.
XI.	*3*	Сигурност на мрежно и транспортно ниво.	*1*	Виртуални приватни мрежи.
XII.	*3*	Сигурност на интернет комуникации. Сигурност на апликациско ниво. Тест.	*1*	PGP.
			2	Генерирање на PGP клучеви.
XIII.	*3*	Сигурност во целуларни мрежи (GSM, UMTS).	*1*	Автентикација во GSM и UMTS.
XIV.	*3*	Сигурност во безжични мрежи (Wi-Fi, Wi-Max) и ад-хок мрежи (Bluetooth, сензорски мрежи).	*1*	Автентикација во безжични и ад-хок мрежи.
XV.	*3*	Стандардизација на сигурносните механизами и протоколи. Примена.	*1*	Останати примери од примена на сигурносни механизми.
			1	Проверка на елаборати од лабораториски вежби.
Збир	***45***		***30***	