

1.	Наставен предмет	Безбедност и заштита на компјутерски системи	
2.	Шифра	ETF083L03	
3.	Студиска програма	ИНФО	
4.	Семестар (изборност)	Летен (изборен)	
5.	Цели на предметот	Запознавање со постапките и механизмите за заштита кај компјутерските системи. Заштитни и безбедносни механизми кај оперативните системи. Детекција и одбрана од вируси и тројански коњи. Заштита со механизам на заштитни ѕидови (Ifirewalls)	
6.	Оспособен за (компетенции)	Познавање на заканите од безбедносен аспект, како и соодветните механизми и постапки што се применуваат кај компјутерските системи за подигање на нивото на безбедност и заштита во однос на неовластен пристап	
7.	Услов за запишување на предметот	Компјутерски мрежи, Системски софтвер	
8.	Основна литература (до 3 наслови)	<ol style="list-style-type: none"> 1. Dieter Gollman, Computer Security, John Wiley & Sons, 1998 2. Bruce Schneier, Applied Cryptography Second Edition: protocols, algorithms, and source code in C, John Wiley & Sons, 1996 3. Jan Harrington, An Introduction to Network Security, Morgan Kaufmann Publishers Inc., September 2004 Network Devices, Cisco Systems Documentation CD-ROM 	
.	Број на кредити	6	
.	Вкупен расположив фонд на време	6 ECTS x30 часа = 180 часа	
.	Распределба на расположивото време		
	11.1.	П - Предавања-теоретска настава (14 недели x 3 часа)	45 часа
	11.2.	ЛВ - Лабораториски вежби (15 недели x 1 час)	15 часа
	11.3.	АВ - Аудиторни вежби, консултации (15 недели x 1 час)	15 часа
	11.4.	СУ - Самостојно учење	83 часа
	11.5.	ПЗ - Проверка на знаење(2 x 3 часа)+(2 x 0.5 часа)	7 часа
	11.6.	СЗ - Семинарски работи, самостојни задачи	15 часа
.	Оценување		
	12.1.	Посетеност на настава до 10 бода	10 бода
	12.2.	Парцијални испити (2 x 100 бода)	200 бода
	12.3.	Тестови (2 x 25 бода)	50 бода
	12.4.	Семинарски работи и самостојни задачи	20 бода
	12.5.	Лабораториски вежби	20 бода
	Забелешка:	Оценки:	
		од 180 до 200 бода	6 (шест)
		од 201 до 225	7 (седум)
		од 226 до 250	8 (осум)
		од 251 до 275	9 (девет)
		од 276 до 300	10 (десет)
.	Услов за потпис и формален испит	Реализирани активности: од 11.1 до 11.5	

ПЛАНИРАЊЕ АКТИВНОСТИ ЗА НАСТАВНИОТ ПРЕДМЕТ БЕЗБЕДНОСТ И ЗАШТИТА НА КОМПЈУЕТРСКИ СИСТЕМИ

недела	Предавања - теоретска настава		Аудиторни и лабораториски вежби	
	часа	Тема	часа	тема
I.	3	Вовед и основни поими. Етички норми и одговорност. Структура на криптирање.	1	Вовед и основни поими. Структура на криптирање.
II.	3	Примери на протоколи за криптирање.	1	Примери на протоколи за криптирање.
III.	3	Криптирање со тајни клучеви.	1	Криптирање со тајни клучеви.
IV.	3	Криптирање со јавни клучеви. Пробивање на криптирани системи.	1	Криптирање со јавни клучеви. Пробивање на криптирани системи.
V.	3	Основни заштитни механизми кај оперативните системи.	1	Основни заштитни механизми кај оперативните системи.
VI.	3	Архитектура на системите за заштита кај оперативни системи, автентикација, контрола на пристап: листи на пристап, имплементација на контрола на пристап (Unix, Java), Bell и La Padula модели,	2	Примери на заштитни механизми
			1	Архитектура на системите за заштита кај оперативни системи, автентикација, контрола на пристап: листи на пристап, имплементација на контрола на пристап (Unix, Java)
VII.	3	Механизми на оперативни системи за поддршка на MAC политиките.	2	Имплементација на контрола на пристап (Unix, Java)
			1	Механизми на оперативни системи за поддршка на MAC политиките.
VIII.		ПАРЦИЈАЛЕН ИСПИТ	2	Механизми на оперативни системи за поддршка на MAC политиките.
			1	КОНСУЛТАЦИИ; ПАРЦИЈАЛЕН ИСПИТ
IX.	3	Безбедносни политики Clark-Wilson и Кинески сид.	1	КОНСУЛТАЦИИ; ПАРЦИЈАЛЕН ИСПИТ
			1	Безбедносни политики Clark-Wilson и Кинески сид.
X.	3	Слабости на заштитата кај оперативните системи.	1	Слабости на заштитата кај оперативните системи.
XI.	3	Безбедни јадра на оперативните системи.	1	Безбедни јадра на оперативните системи.
			2	Безбедни јадра на оперативните системи.
XII.	3	Заштитни механизми кај TCP/IP базираните мрежи.	1	Заштитни механизми кај TCP/IP базираните мрежи.
			2	Заштитни механизми кај TCP/IP базираните мрежи.
XIII.	3	Заштитни ѕидови (Firewalls).	1	Заштитни ѕидови (Firewalls).
			2	Заштитни ѕидови (Firewalls).
XIV.	3	Детекција на вируси, тројански коњи и обиди за неовластено најавување. Spam (преку e-mail подсистем).	1	Детекција на вируси, тројански коњи и обиди за неовластено најавување. Spam (преку e-mail подсистем).
			2	Детекција на вируси, тројански коњи и обиди за неовластено најавување. Spam (преку e-mail подсистем).
XV.	3	Агенти и мобилни кодови. Заштита кај smart и други видови на картички. Протоколи за безбедни електронски трансакции.	1	Агенти и мобилни кодови. Заштита кај smart и други видови на картички. Протоколи за безбедни електронски трансакции.
Збир	45		30	